Loyola University Chicago Law Journal

Volume 22
Issue 1 *Fall 1990*

Article 5

1990

Letting *Katz* Out of the Bag: Re-Evaluating Probable Cause in the Context of Electronic Eavesdropping

Elan Gerstmann Esq.
Assoc.Law Offices Lionel R. Saporta, New York, NY

Letting *Katz* Out of the Bag: Re-Evaluating Probable Cause in the Context of Electronic Eavesdropping

Elan Gerstmann, Esq. *

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.[1]

I. INTRODUCTION

Electronic interception of communications[2] serves the dual purposes of investigative utility and evidence gathering. Initiators of electronic investigations seek to discern patterns and relationships of conduct where without eavesdropping there is but limited coherence. To warrant the government's use of these devices, however, a sufficient theory of criminal conduct must be established, supported by cogent and reliable evidence.[3] Additionally, the government must show that it has no other means to obtain the needed evidence.[4]

The quantum of evidence necessary to establish probable cause in the context of electronic eavesdropping is a basic issue. The

* Associate, Law Offices of Lionel R. Saporta, New York; B.A., 1982, Columbia College, Columbia University; J.D., 1987, State University of New York at Buffalo; member of the New York, New Jersey, and District of Columbia Bars.

1. Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

2. Framed broadly, the term electronic eavesdropping is meant in this Article to include the "wiretapping" of telephone lines (i.e., the interception of telephone conversations) and the "bugging" of areas to intercept speech by the use of hidden or remote microphones, without the consent of any participant in the conversation. Eavesdropping is also intended to include the interception of certain "electronic communications" that do not contain the human voice at any point, but carry confidential data (e.g., certain computer-to-computer transmissions). Eavesdropping excludes, however, the use of pen registers (which record the telephone numbers dialed from a particular line), trap and trace devices (which trace calls placed to a given line to their origin), and personal body recorders and/or transmitters by one or more parties to a conversation ("consensual" recording).

3. *See* 18 U.S.C. § 2518 (3)(a)-(b), (d) (1988); *see also infra* note 13, discussing the statutory scheme.

4. Federal law permits an eavesdrop only if alternative investigatory methods cannot accomplish the goals and purposes of the particular investigation. *See id.* § 2518(3)(c); *see also infra* note 13, discussing the statutory scheme.

Supreme Court first conclusively established in *Katz v. United States*[5] that the fourth amendment[6] protects spoken communication within the implied meaning of "persons, houses, papers, and effects." Just six months earlier, however, in *Berger v. New York*,[7] the Court specifically declined to consider the degree of probable cause required to justify an electronic eavesdrop.[8]

Despite the Court's reluctance to decide, the issue is more criti-

5. 389 U.S. 347 (1967). The case involved federal agents placing, without a warrant, a listening and recording device on the outside of a telephone booth. Only one side of the conversation could be heard. The agents acted on the basis of a high degree of probable cause because a previous conventional investigation had established "a strong probability" that the telephone calls would be in furtherance of a gambling operation. *Id.* at 354. Although there was no physical trespass, the Court suppressed the warrantless interception. In addition to expanding the conceptual parameters of the fourth amendment, most concisely reflected in the then-novel proposition that "the Fourth Amendment protects people, not places," *Katz* reaffirmed the fundamental premise that antecedent probable cause must be established by a court. *Id.* at 351. The Court had previously announced in Berger v. New York, 388 U.S. 41 (1967), that spoken communications may reasonably be embraced by the fourth amendment independent of any concomitant, unconsented intrusion upon tangible effects, seizure of the person, or a trespass. These propositions, however, amounted to dicta because a physical trespass had occurred during the installation of recording devices. *Id.* at 45.

6. The fourth amendment to the United States Constitution states:

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

U.S. CONST. amend. IV.

7. 388 U.S. 41 (1967).

8. In *Berger*, the writing was on the wall (but not yet in the law books) that the fourth amendment would henceforth regulate interceptions. The Court struck down a New York statute governing the use of eavesdropping devices. *See* N.Y. CRIM. PROC. LAW § 813-a (McKinney 1958) (found unconstitutional in *Berger*, 388 U.S. at 54-60). Closely read, the case limited its analysis to the failure of the statute to mandate compliance with the fourth amendment's requirement that a warrant describe with particularity the place to be searched and the items to be seized. *See Berger*, 388 U.S. at 55-58; *see also infra* notes 61-62 (particularity requires prior specification of government conduct, as well as minimization of intrusion). Because it could decide the case on other grounds, the Court declined to consider whether the quantum of evidence necessitated by the New York statute was equivalent to the fourth amendment requirement of probable cause. *See Berger*, 388 U.S. at 55. Nevertheless, the New York statute required an oath stating " 'that there is reasonable ground to believe that evidence of crime may be . . . obtained [by means of the eavesdrop],' " in addition to a requirement of particularizing the person thereby targeted. *Id.* at 54 (quoting N.Y. CRIM. PROC. LAW § 813-a (McKinney 1958)). The Court stated: "It is said . . . that the 'reasonable ground' requirement of § 813-a 'is undisputedly equivalent to the probable cause requirement of the Fourth Amendment.'. . . While we have found no case on the point by New York's highest court, we need not pursue the question further because we have concluded that the statute is deficient on its face in other respects." *Id.* at 55 (citations omitted). *See generally id.* at 55-59 (confining analysis to failure of particularity). The Court's consideration in *Berger* of a deficiency in probable cause related only to the utter absence in that statutory scheme of

cal now than ever before.[9] Increasingly sophisticated technology[10]

a probable cause requirement to obtain extensions of an eavesdrop. *See* J. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 1.4(d), at 1-23 (2d ed. 1990).

9. Although some commentaries deem the issue decided, the evidence proffered therein is unconvincing; the Supreme Court has simply not spoken to the point. *See, e.g.*, Project, *Annual Review of Criminal Procedure*, 78 GEO. L.J. 699, 792 n.457 (1990) (probable cause standard same for eavesdrop as for ordinary search warrant, citing, by analogy, Dalia v. United States, 441 U.S. 238, 255-56 n.18 (1979)). Supreme Court authority is unpersuasive because the language in *Dalia*, which in any event appears to be dictum, advises only that an electronic surveillance order issued pursuant to federal law has the indicia of a warrant. *Dalia* does not state that the ordinary indicia of a warrant necessarily satisfy the fourth amendment when applied in the electronics context. The more basic question of whether a warrant is required prior to an eavesdrop is no longer at issue. Rather, what is at issue is whether the quantum of evidence required to support a conventional search warrant necessarily is identical to that necessary to support an eavesdrop order. For a discussion of the federal statutory scheme that regulates the issuance of electronic surveillance orders, see *infra* note 13.

10. Even in 1967, the Supreme Court was impressed with the array of electronic eavesdropping devices which were available to the government and permitted an increasing intrusion upon individual privacy:

> Sophisticated electronic devices have now been developed (commonly known as "bugs") which are capable of eavesdropping on anyone in almost any given situation. They are to be distinguished from "wiretaps" which are confined to the interception of telegraphic and telephonic communications. Miniature in size (3/8' x 3/8' x 1/8') — no larger than a postage stamp — these gadgets pick up whispers within a room and broadcast them half a block away to a receiver. It is said that certain types of electronic rays beamed at walls or glass windows are capable of catching voice vibrations as they are bounced off the surfaces. Since 1940 eavesdropping has become a big business. Manufacturing concerns offer complete detection systems which automatically record voices under almost any conditions by remote control. A microphone concealed in a book, a lamp, or other unsuspected place in a room, or made into a fountain pen, tie clasp, lapel button, or cuff link increases the range of these powerful wireless transmitters to a half mile. Receivers pick up the transmission with interference-free reception on a special wave frequency. And, of late, a combination mirror transmitter has been developed which permits not only sight but voice transmission up to 300 feet. Likewise, parabolic microphones, which can overhear conversations without being placed within the premises monitored, have been developed.

Berger, 388 U.S. at 46-47.

These specifications, impressive as they are, have been improved upon vastly during the nearly twenty-five years since *Berger*, with the advent of such devices as laser beams sensitive to the vibrations of objects, further improvements upon the highly directional microphone, which remains remote from the area of interception while minimizing pickup of extraneous noises, thereby permitting amplification of the targeted conversation without substantial background distortion, and ever more detection-resistant designs. Although there are undoubtedly limitations upon the intrusive capacities of eavesdropping and other surveillance devices, we have clearly entered an era in which it is largely the law, rather than science, which limits the exposure of individuals to observation and intrusion. *See* United States v. White, 401 U.S. 745, 757 (1971)(Douglas, J., dissenting) (" '[g]iven the advancing state of both the remote sensing art and the capacity of computers to handle an uninterrupted and synoptic data flow, there seem to be no physical barriers left to shield us from intrusion' ") (quoting A. MILLER, THE ASSAULT ON PRIVACY 46 (1971)).

has produced better quality monitoring,[11] and, despite its cost, it may permit access to a greater number of potential defendants. Since *Berger*, concern has emerged about periodic extensions[12] of electronic eavesdropping in the course of a given investigation. Title III of the Omnibus Crime Control and Safe Streets Act of 1968[13] permits a more extensive intrusion than does a conventional

11. One should note, nonetheless, that the use of electronic surveillance, and particularly eavesdropping, has been perceived since the 1960s as crucial to efforts by the government to combat organized crime. *See, e.g.*, *Berger*, 388 U.S. at 60-62; *see also*, J. CARR, *supra* note 8, § 2.2 (post-World War II interest in use of electronic surveillance for national security shifted to investigation of organized crime in 1960s). It is significant, however, that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 does not limit use of surveillance to organized criminal activity or even to nonorganized but violent crimes. For example, violations of such broadly applicable statutes as the federal wire and mail fraud laws may be investigated by eavesdropping. *See* 18 U.S.C. § 2516(1)(c) (1988). By comparison, the Massachusetts eavesdropping statutes limit the designated crimes for which evidence may be sought to offenses connected with organized crime. *See* MASS. GEN. L. ch. 272, § 99 A (1968). Organized crime, however, has been somewhat broadly defined as "a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services." *Id.* This definition may create workable limitations upon the use of surveillance technology, but may de-emphasize the targeting of "mobsters." *Compare* Commonwealth v. Thorpe, 384 Mass. 271, 281, 424 N.E.2d 250, 256 (Mass. 1981) (continuing conspiracy to illegally supply civil service examinations was "organized crime"), *cert. denied*, 454 U.S. 1147 (1982) *with* Commonwealth v. Jarabek, 384 Mass. 293, 296, 424 N.E.2d 491, 493 (Mass. 1981) (no evidence of "organized crime" in scheme by two municipal officials to extort a kickback from a single contractor). The court in *Thorpe* stated: "Statutory definitions of organized crime prevailing in other States similarly focus on the elements of organization, discipline, and the provision of illegal goods and services." *Thorpe*, 384 Mass. at 277-78 n.6, 424 N.E.2d 254 n.6 (citing N.H. REV. STAT. ANN. § 570-A:1, XI (1974); N.M. STAT. ANN. § 29-9-2 (1978); TENN. CODE ANN. § 38-502 (1975)). Thus, even attempts to limit the use of eavesdropping to investigation and prosecution of organized criminal activity yield definitions that are subject to a wide latitude of interpretation, readily embracing activities not ordinarily undertaken by persons typically perceived as "mobsters." *See id.* at 286-92, 424 N.E.2d at 259-62 (Liacos, J., dissenting). Analytically, the difference between *Thorpe* and *Jarabek* would seem to turn upon the continuity of a conspiracy. If so, the benchmark for determining the propriety of an eavesdrop is the persistence demonstrated by an identifiable set of criminal actors in the course of one or more conspiracies, rather than the nature and means of the criminal activity undertaken or the goals expected to be achieved thereby. Rigorous application of this definition also would appear to require fairly extensive use of conventional investigatory tools prior to the use of an eavesdrop in order to establish the extent and continuity of a given conspiracy and thereby justify the use of an eavesdrop. Such a definition therefore is amenable to the imposition of a heightened standard of probable cause, at least *ab initio*, which presumably would compel substantial conventional investigation prior to the use of an eavesdrop.

12. The statute held unconstitutional in *Berger* permitted the maintenance of an eavesdrop for a period of two months upon a single showing of probable cause. *See Berger*, 388 U.S. at 43 n.1.

13. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 Pub. L. No. 90-351, § 802, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2521 (1988)), regulates the interception of wire, oral, and electronic communications. Related legislation appears at 18 U.S.C. §§ 2701-10, 3117, 3121-3126 (1988). The Communications Act, 47

search and seizure undertaken pursuant to a search warrant or a

U.S.C. §§ 151-613 (1988), further modifies the scheme with respect to radio communications. *See generally* C. FISHMAN, WIRETAPPING AND EAVESDROPPING § 7.22 (Supp. 1990).

A "wire communication" as defined by Title III, explicitly excludes "the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," but otherwise includes most wire and cable transmissions. 18 U.S.C. § 2510(1) (1988). "Oral communication" includes human utterances to which an expectation reasonably attaches that the communication is "not subject to interception. *Id.* § 2510(2). As amended in 1986, the scheme also regulates the interception of any "electronic communication," defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce," exclusive of oral or wire communications. *Id.* § 2510(12). Title III omits reference to the use of video equipment without concomitant recording of spoken conversation. *See* J. CARR, *supra* note 8 § 3.8, at 3-114. Neither Title III nor the fourth amendment prohibits eavesdropping consented to by at least one party to a conversation. *See* United States v. White, 401 U.S. 745 (1971); Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 3 n.1 (1983). Title III regulates the use of pen registers and trap and trace devices, but effectively limits prior judicial consideration to the completeness of the application. *See* J. CARR, *supra* note 8, § 4.11, at 4-126. In addition to regulating government conduct, Title III establishes liability and provides sanctions for nonconsensual interception by private citizens. *See* 18 U.S.C. § 2511 (1988); *see also* C. FISHMAN, *supra*, § 25, at 190. The prosecutorial use of private, unlawful interceptions remains a confused topic. *See* C. FISHMAN, *supra*, § 25.8, at 207. In sum, Title III provides that:

> (1) a high level, identifiable public official who would be responsible and accountable for the eavesdropping undertaken make the decision to apply for court-authorized eavesdropping; (2) the applicant for a warrant make detailed, particularized showings in support of the warrant application; (3) the applicant exhaust normal investigative procedures; and (4) the surveillance minimize the interception of communications not otherwise subject to interception.

Goldstock and Chananie, *"Criminal" Lawyers: The Use of Electronic Surveillance and Search Warrants in the Investigation and Prosecution of Attorneys Suspected of Criminal Wrongdoing*, 136 U. PA. L. REV. 1855, 1866 (1988) (footnotes omitted). Regarding these concepts of particularization and minimization, see *infra* notes 61-62. Title III permits states to regulate surveillance more strictly, but not less strictly. *See* J. CARR, *supra* note 8, § 2.4(a), at 2-15. Although Title III attempts comprehensive regulation of electronic surveillance, it is definitely not co-extensive with the fourth amendment, insofar as it does not regulate certain technologies that do not "intercept" communications per se, but which nonetheless may infringe upon constitutionally protected privacy interests. For instance, a mobile tracking device does not intercept communications and is not regulated by Title III, but its warrantless use may violate the fourth amendment, depending upon whether its placement and operation violate the target's reasonable expectation of privacy. J. CARR, *supra* note 8, at § 3.2(c)(2)(D), at 3-30.1; *see also* United States v. Karo, 468 U.S. 705 (1984). As noted in a report by the Senate Judiciary Committee recommending passage of the Electronic Communications Privacy Act of 1986, "tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques." S. REP. NO. 541, 99th Cong., 2d Sess. 3, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3557. Consequently, the wealth of emergent technologies requires that distinctions be made between them with respect to the nature of their operation, use, and relative impact on privacy.

conventional exception to the warrant requirement.[14]

Legal theory supporting the current federal probable cause standard fails to consider the peculiar problems that electronic eavesdropping creates. This Article will show that the prevailing theory is conclusory. It provides little basis for applying the conventional warrant standards to electronic eavesdropping. Consequently, the judiciary should reconsider the legal and theoretical precedent for the probable cause standard and re-evaluate this standard in the electronic context.

This Article discusses certain constitutional search and seizure problems peculiar to electronic eavesdropping. It analyzes the derivation of the current electronic probable cause standard in the federal case law. The Article demonstrates that, at minimum, retention of the present standard requires justification and considers, without advocating, implementation of a heightened standard of probable cause in the context of an electronic eavesdrop. Most importantly, this Article calls for debate of the underlying policies and concerns surrounding the issue.

II. HISTORICAL BACKGROUND

Title III[15] is often thought of as the culmination of electronic surveillance law development.[16] Title III, however, was merely an

14. "[A] search warrant authorizes a single, overt entry and search of that premises. . . . In contrast . . . an eavesdropping warrant may authorize a series of surreptitious intrusions for up to 30 days [each]." C. FISHMAN, WIRETAPPING AND EAVESDROPPING § 6, at 7-8 (1978). The highly intrusive nature of eavesdropping was noted by Ronald Goldstock, Director of the New York State Organized Crime Task Force, and Steven Chananie, an Assistant Deputy Attorney General, who wrote that electronic "surveillance not only constituted a gross invasion of privacy but also had the potential to infringe upon basic constitutional freedom." Goldstock and Chananie, *supra* note 13, at 1866. The authors specifically cited the chilling effect of electronic surveillance upon the constitutional rights of dissent and association. *Id.* at 1866 n.62. Carr has made further distinctions between degrees of intrusiveness associated with various technologies:

> Whether placed in a private area, such as a home, office, or similarly enclosed location, or in a public location being used for private communication, a bug can be considerably more intrusive than a wiretap. It can overhear conversations involving several persons, whereas the wiretap is limited to the number of phones connected to the specific wire. A wiretap is only effective if the particular telephone is used, while the bug hears all conversations within its range.

J. CARR, *supra* note 8, § 1.1(b), at 1-3.

15. 18 U.S.C. §§ 2510-2521 (1988).

16. *See, e.g.*, 3 C. WRIGHT, FEDERAL PRACTICE AND PROCEDURE (CRIMINAL) § 665, at 616 (2d ed. 1982) (Title III "is the climax of 40 years of very tangled development of the law". The "40 years" refers to the period between Olmstead v. United States, 277 U.S. 438 (1928), in which the Court held that the fourth amendment afforded no protection against the interception of communications without some related physical tres-

initial response to the dramatic reformulation[17] of fourth amendment protections afforded by *Berger v. New York*[18] and *Katz v. United States*.[19] *Katz* recognized that "the Fourth Amendment protects people, not places,"[20] and thus granted protection against the search and seizure of communications without requiring a physical intrusion of one's property. The courts previously had excluded communications from the list of tangible interests set forth in the amendment.[21] Title III, enacted one year after *Berger* and *Katz*, was a tentative effort to afford constitutionally adequate protection to individuals' privacy interests in their communications. Advances in surveillance technology and their application by police agencies undoubtedly prompted the *Katz* decision and Title III. Further developments in the constitutionality of electronic surveillance evolved later. The resulting probable cause standard for electronic eavesdropping emerged in part due to Title III's swift enactment.[22]

An outline of electronic surveillance law prior to Title III[23] generally begins with *Olmstead v. United States*.[24] The exclusion of

---

pass (due to the interpretation that a spoken communication could not be seized within the meaning of the fourth amendment), and the enactment of Title III in 1968.

17. The formulation that has been adopted was set forth by Justice Harlan in his concurring opinion in Katz v. United States. The protections of the fourth amendment are triggered as follows: "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* 1 W. LAFAVE, SEARCH AND SEIZURE § 2.1(b), at 306 (2d ed. 1987).

18. 388 U.S. 41 (1967).

19. 389 U.S. 347 (1967).

20. *Id.* at 351; *see also supra* note 6 (text of the fourth amendment).

21. *See supra* note 16; *see also* Cranwell, *Judicial Fine-Tuning of Electronic Surveillance*, 6 SETON HALL L. REV. 225, 229-30 (1975). The Court held for many years that illegality under state law did not render the evidence inadmissible, so long as the violation was not one of a federal constitutional guarantee. Olmstead v. United States, 277 U.S. 438, 466-67 (1928). The *Olmstead* "trespass" doctrine limited fourth amendment violations to those arising from an "actual entrance" into "private quarters" or intrusion upon some other tangible, protected interest. *Id.* at 464 (citing Gouled v. United States, 255 U.S. 298 (1921)). "*Gouled* . . . carried the inhibition against unreasonable searches and seizures to the extreme limit" because it analogized an entrance by stealth to one by force. *Id.* at 463.

22. *See* 1 W. LAFAVE, *supra* note 17, § 2.1(b), at 306. The swift enactment, within a year of *Katz*, of Title III may have served to retard judicial analysis in the area.

23. The following discussion is only a brief outline of developments marked by subtle shifts in reliance on precedent by majority opinions and powerful advocacy in dissenting opinions that anticipate the demise of the "trespass" doctrine. *See* United States v. White, 401 U.S. 745, 773 (1971) (Harlan, J., dissenting) (setting forth "a full exposition of the dynamics of the decline of the trespass rationale").

24. 277 U.S. 438 (1927); *see, e.g.*, Cranwell, supra note 21, at 227-28; 3 C. WRIGHT, *supra* note 16, § 665, at 616 (all commencing with *Olmstead*); Comment, *Constitutional*

spoken communications from fourth amendment protection first was articulated in that case. *Olmstead* held that no search or seizure occurs, within the meaning of the fourth amendment, when "voluntary conversations [are] secretly overheard." The Court reasoned that "[t]he amendment itself shows that the search is to be of material things — the person, the house, his papers, or his effects"; conversation is to be contrasted with a letter, which "is a search and seizure of the sender's papers or effects" within the plain terms of the amendment.[25] *Olmstead* involved a nontrespassory wiretap conducted by federal agents in the State of Washington, where a statute prohibited wiretapping.[26] The incoherence of the constitutional doctrine in that case can be discerned from the separate development of wiretapping, wireless electronic surveillance, and the recording of conversations at which a government agent is present.[27]

In the wake of *Olmstead*, limitations upon wiretapping were created entirely by statute.[28] The courts, however, developed the remedy that evidence so obtained in violation of these statutes was not admissible in court.[29] Although the application of a statute-based suppression remedy[30] was significant to a defendant facing surveillance evidence at trial, this development is primarily a study

---

Law—Fourth Amendment Protection Against Unlawful Electronic Search and Seizure—Requirement of Judicial Authorization Extended—Katz v. United States *(United States Supreme Court, 1967)*, 32 ALB. L. REV. 455, 456 (1968).

25. *Olmstead*, 227 U.S. at 464; *see also supra* note 6 (text of the fourth amendment).

26. *Olmstead*, 277 U.S. 455-57, 468.

27. 3 C. WRIGHT, *supra* note 16, § 665, at 618.

28. *Id.*

29. Wright summarized this development as follows:

> The development with regard to wiretapping was almost entirely by statute, and by construction of that statute. Section [705, formerly section 605,] of the [Federal] Communications Act of 1934 prohibited the interception and divulgence or publication of telephone, telegraph, or radio communications. . . . The significant sanction, developed by the Court though not mentioned in the statute, was that evidence obtained by wiretapping was not admissible in court. This ban applied not only to what was heard by the wiretap, but also to other evidence to which the government was led by the information it obtained through tapping.

Id. at 618-19 (footnotes omitted).

30. Developments regarding suppression rooted in section 705 of the Federal Communications Act may be found in two related decisions. In the first, Nardone v. United States, 302 U.S. 379 (1939), the Court rejected the argument that a sovereign is not bound by a general statute unless that consequence is specifically mentioned and held that the government must heed its own prohibition of wiretapping. *Id.* at 383-84; *see also* 3 C. WRIGHT, *supra* note 16, § 665, at 618 n.11; Cranwell, supra note 21, at 231. In the second decision, Nardone v. United States, 308 U.S. 338 (1939), the Court applied the "fruit of the poisonous tree doctrine," under which derivative evidence of an unlawful wiretap, if unattenuated, also would be suppressed unless the government met its burden

in the avoidance of constitutional ramifications. As one commentator put it, "By mandating that the government must obey its own laws, the Court was able to avoid a direct analysis of the fourth and fifth amendment issues in the use of electronic surveillance."[31]

The second line of development involved "bugging," in which the government relied upon surveillance by electronic means that did not tap telephone wires or intercept radio signals.[32] Because such surveillance did not fall within the proscription of section 705 (formerly section 605) of the Federal Communications Act,[33] development in this area until 1968 was entirely in constitutional terms. For example, in *Goldman v. United States*,[34] in which federal agents overheard conversations in an adjoining office by using a device placed against a common wall, the Supreme Court held that *Olmstead* controlled and the fourth amendment was not violated because there was no physical intrusion.[35] A different result was reached, however, in *Silverman v. United States*,[36] when officers inserted a "spike mike" into a party wall that made contact with a heating duct and picked up conversations through the entire building. The Supreme Court found the evidence obtained in *Silverman* inadmissible because a part of the defendant's house was involved in the surveillance. Regardless of whether a trespass occurred, the Court found a fourth amendment violation and stated, "We find no occasion to re-examine *Goldman* here, but we decline to go beyond it, by even a fraction of an inch."[37] Although dictum in *Silverman* disavowed the "trespass" theory of *Olmstead*, that theory survived even the broader constitutional enunciations in *Berger*, only to meet its demise in *Katz*.[38]

The Court in *Berger*[39] commenced its analysis of legal precedent

---

of convincing the court that its proof derived independently. *Id.* at 341; *see also* Cranwell, *supra* note 21, at 232 n.35.

31. Cranwell, *supra* note 21, at 231.

32. *See* C. WRIGHT, *supra* note 16, § 665, at 619-20.

33. 47 U.S.C. § 605 (1988).

34. 316 U.S. 129 (1942).

35. *See id.* at 131, 135.

36. 365 U.S. 505 (1961).

37. *Id.* at 512.

38. Only brief mention is made here of the third line of case law, involving the warrantless wiring for sound of a government agent or informant as a consenting participant in a conversation, and the operation of a tape recorder either locally or following radio transmission to a remote device. This technique was upheld in On Lee v. United States, 343 U.S. 747 (1952). Both the technique and the case were sustained after *Katz* by a plurality of the Court in United States v. White, 401 U.S. 745, 750 (1971) (plurality opinion). *See generally* 3 C. WRIGHT, *supra* note 16, § 665, at 624-27 (outlining these developments).

39. Berger v. New York, 388 U.S. 41 (1967).

by noting Lord Camden's proposition in 1765, in *Entick v. Carrington*, that intrusions into individual privacy are " 'subversive of all the comforts of society.' "[40] *Berger* asserted that this principle was pivotal to the Supreme Court's decision over a century later in *Boyd v. United States*[41] that the " 'concrete form of the case' "[42] does not control the application of the Constitution as against intrusion. Thus, *Berger* re-enunciated the principle that in construing the fourth amendment, the Court would raise substance above form. Consequently, *Berger* implied that literal recitation of terms within the Constitution, together with an admonition about their "plain meaning," would no longer end the constitutional analysis. *Katz* first effectuated this analytic transformation by overruling *Olmstead* and directly holding that the nontrespassory interception of communications is within the purview of the fourth amendment.[43]

III. STANDARDS OF PROBABLE CAUSE

Probable cause sufficient to support an electronic eavesdrop order requires that the government's evidence demonstrate a likelihood that particular evidence[44] of a specified crime will be found at the particular time and location, and by means of the proposed search.[45] The issuance and supervision of an electronic eavesdrop order requires "extra vigilance" beyond that required for warrants authorizing more limited intrusions.[46] Yet the incantation of this phrase has not prompted scrupulous attention to the requirements of probable cause in the electronics context, even when measured by a conventional standard.[47] In practice, it certainly has not

40. *Id.* at 49 (quoting Entick v. Carrington, 19 Howell's State Trials 1029, 1066 (C.P. 1765)).

41. 116 U.S. 616 (1886), *discussed and quoted in* Olmstead v. United States, 277 U.S. 438, 458-59 (1927).

42. *Berger*, 388 U.S. at 49 (quoting *Boyd*, 116 U.S. at 630).

43. Katz v. United States, 389 U.S. 347, 353 (1967).

44. The requirement that detail be provided of the particular conversations to be intercepted has been limited to a statement reflecting the type of offense under investigation. *See* J. CARR, *supra* note 8, § 4.4(c)(3)(A), at 4-40.4. For example, "[t]he description [of] . . . 'conversations pertaining to violations of the laws . . . relating to dealings in dangerous drugs,' has been held to be sufficiently particular to satisfy constitutional and statutory requirements." *Id.* at 4-40.4 to.5 (quoting State v. Weedon, 425 So. 2d 125, 126 (Fla. Dist. Ct. App. 1982)).

45. *See* 18 U.S.C. § 2518(3) (1988).

46. United States v. Falcone, 505 F.2d 478, 481 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975) (citing Berger v. New York, 388 U.S. 41 (1967) and Katz v. United States, 389 U.S. 347 (1967)).

47. *See* Goldsmith, *supra* note 13, at 133. "Nevertheless, although the probable cause

amounted to the standard advocated by Justice Stewart's concurrence in *Berger* that the showing of probable cause should "match the degree of intrusion."[48] Because the "extra vigilance" demanded in the electronics context would effectively be prescribed by an enhanced probable cause standard, while remaining within the framework of the *Illinois v. Gates*[49] "totality-of-the-circumstances" approach[50] employed by the federal courts, such an enhanced standard bears discussion.

Although the Third Circuit stated that in the electronics context "[p]robable cause is not a matter of degree,"[51] the Supreme Court has made it clear that there is no general stricture against differential standards of probable cause. In fact, the Court has a differen-

---

requirement is constitutionally mandated [in the context of an electronic eavesdrop], it has not always been strictly enforced." *Id.*

48. Berger v. New York, 388 U.S. 41, 69 (Stewart, J., concurring).

49. 462 U.S. 213, 230-32 (1983), discussed *infra* note 50, and notes 119-31 and accompanying text.

50. This analysis assumes that even a heightened standard of probable cause would be entertained by the federal courts only within the overall framework of the "totality-of-the-circumstances" test. In determining the existence of probable cause, *Gates* dispensed with the *Aguilar-Spinelli* two-prong analysis of the reliability of an anonymous informant and his information in favor of the "totality-of-the-circumstances" standard, which permits the compensation of a deficiency in one prong by a strong showing in the other prong. *Id.* at 233; *see* Spinelli v. United States, 393 U.S. 410 (1969); Aguilar v. Texas, 378 U.S. 108 (1964). The Court thereby implemented "a fluid concept—turning on the assessment of probabilities in particular factual contexts . . . ." *Gates*, 462 U.S. at 232.

Not all state jurisdictions have adopted the *Gates* standard. For instance, as a matter of state constitutional law, New York continues to use the two-prong test. The first prong of this test requires evidence of the inherent credibility of an informant (e.g., past performance record) or the reliability of his information on the particular occasion. The second prong requires the presentation of sufficient facts to permit an independent judgment that evidence of a crime may be found in a certain place at a certain time or that a certain person is involved in a crime. *See* People v. Griminger, 71 N.Y.2d 635, 524 N.E.2d 409, 529 N.Y.S.2d 55 (1988) (two-prong test applied when search was conducted pursuant to a warrant); People v. Johnson, 66 N.Y.2d 398, 488 N.E.2d 439, 497 N.Y.S.2d 618 (1985) (two-prong test applied in evaluating a warrantless arrest); *see also* W. LAFAVE & J. ISRAEL, CRIMINAL PROCEDURE § 3.3(c), at 114-15 (abr. ed. 1985). New York's probable cause analysis nevertheless is cast in terms of considerations establishing the reliability of proffered information. *See* People v. P.J. Video, Inc., 68 N.Y.2d 296, 306-07, 501 N.E.2d 556, 562-64, 508 N.Y.S.2d 907, 913-15 (1986), *cert. denied*, 479 U.S. 1091 (1987). New York's statutory scheme regulating electronic surveillance is found in N.Y. CRIM. PROC. LAW §§ 700.05-700.70 (McKinney 1984 & Supp. 1990). The state scheme must be at least as restrictive of electronic interception as is Title III. People v. Shapiro, 50 N.Y.2d 747, 763, 409 N.E.2d 897, 906-07, 431 N.Y.S.2d 422, 431 (1980).

51. United States v. Falcone, 505 F.2d 478, 481 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975). *Falcone* has, in turn, influenced the case law of several other circuits. *See, e.g.*, United States v. Leisure, 844 F.2d 1347, 1354 (8th Cir.), *cert. denied*, 488 U.S. 932, 109 S.Ct. 324 (1988); United States v. Talbert, 706 F.2d 464, 467 (4th Cir. 1983); United States v. Fury, 554 F.2d 522, 530 (2d Cir. 1977), *cert. denied*, 436 U.S. 931 (1978); United States v. Scibelli, 549 F.2d 222, 226 (1st Cir. 1977), *cert. denied*, 431 U.S. 960 (1978).

tial approach to apply the fourth amendment,[52] which in turn relies upon "reasonableness" as its determinant.[53] In *Zurcher v. Stanford Daily*,[54] the Court stated that probable cause need not be so stringent when the entry is made for civil purposes, rather than to seize evidence of a crime.[55] Thus, the initial wariness of the courts toward the intrusive potential of electronic eavesdropping appeared to have ebbed for a time without much discussion. The greater intrusiveness inherent in such technology, however, continues to be acknowledged as courts note the early concerns thereby raised and consider whether there ought to be a commensurate standard of reasonableness in the decision to authorize such a search. As noted recently by one district court:

> There is . . . evidence that the probable cause standard is somewhat more rigorous in the context of electronic surveillance. In discussing Fourth Amendment limitations on such investigations, the Supreme Court observed in *Berger* that "[t]he need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping."[56]

The court went on to cite Justice Stewart's concurrence in the *Berger* decision, in which he stated:

> *The standard of reasonableness embodied in the Fourth Amendment demands that the showing of justification match the degree of intrusion*. By its very nature electronic eavesdropping for a 60-day period, even of a specified office, involves a broad invasion of a constitutionally protected area. *Only the most precise and rigorous standard of probable cause should justify an intrusion of this sort*.[57]

Justice Stewart thus concluded that although evidence might satisfy fourth amendment standards for a conventional search or arrest, it may not constitute probable cause justifying an intrusion

---

52. Professor LaFave stated, "At least on a theoretical level, it may be argued with some force that . . . probable cause is a variable rather than a fixed test and that it permits consideration of the degree of intrusion and the law enforcement need in a particular case." 1 W. LAFAVE, *supra* note 17, § 3.2(a), at 558.

53. United States v. White, 401 U.S. 745, 753 (1971) (plurality opinion).

54. 436 U.S. 547, 554-56 (1978).

55. 436 U.S. 547, 555 (discussing Camera v. Municipal Court, 387 U.S. 523 (1967) and Frank v. Maryland, 359 U.S. 360 (1959).

56. United States v. Mancari, 663 F. Supp. 1343, 1354-55 (N.D. Ill. 1987) (quoting United States v. Berger, 388 U.S. 41, 56 (1967)). It is noteworthy that Justice Stewart explicitly made the theoretical leap from the issue of particularity emphasized in the majority opinion in *Berger* to the distinct issue of probable cause and the quantum of evidence thereby required. *See supra* note 9; *see also infra* note 58.

57. Mancari, 663 F. Supp. at 135 (quoting United States v. Berger, 388 U.S. 41, 69 (1967) (Stewart, J. concurring) (emphasis added)).

of wide scope and extended duration.[58]

It would appear that the particularly intrusive nature of electronic eavesdropping never has sufficed to form a singular basis for a heightened standard of probable cause. Recognition of certain constitutional concerns apart from the intrusive character of an eavesdrop, however, suggests that reconsideration of a heightened standard is in order. The Constitution assures citizens' "secur[ity] in their persons, houses, papers, and effects."[59] Electronic eavesdropping, for the purpose of gathering evidence of criminal activity, is universally recognized as posing a serious threat to that security. Yet relatively little consideration has been given to the difficulty of demonstrating probable cause throughout the course of a lengthy eavesdrop. It would seem clear, at first glance, that a conventional showing of probable cause must be made throughout an eavesdrop to avoid its immediate termination. But an alternative should be considered. If a substandard showing of probable cause should be tolerated in the course of an eavesdrop despite the diminished probative value of current incoming data, the courts must explicitly articulate such a rationale together with a constitutionally founded justification for allowing the eavesdrop to continue. As first posed, however, a conventional probable cause showing at its commencement may not validate a lengthy surveillance, absent the continual interception of very convincing data. The courts should not espouse a theory of absolute continuity of probable cause, below which threshold the collective evidence may

58. 1 W. LAFAVE, *supra* note 17, § 3.2(a), at 560. In discussing whether "the probable cause requirement may call for a greater or a lesser quantum of evidence, depending upon the facts and circumstances of the individual case," Professor LaFave stated that "[i]t is now clear that there are certain unique investigative techniques as to which a special probable cause test, clearly different from that which is ordinarily utilized in judging arrests and searches, is applicable." *Id.* at 557. LaFave suggests that in addition to *Berger*, support for the proposition that a higher quantum of probable cause should be required in the context of unique, particularly intrusive investigative activities can be found in Justice Marshall's dissent in Gooding v. United States, 416 U.S. 430 (1974), in which Justices Douglas and Brennan joined. In his dissent, Justice Marshall noted that a nighttime search was of a particularly intrusive character and reasoned that because the Court previously had demonstrated its willingness to reduce the quantum of probable cause when reasonable, it should recognize that such a principle could not be "a one-way street to be used only to water down the requirement of probable cause when necessary to authorize governmental intrusions." *Id.* at 465 (Marshall, J., dissenting). Notably, the focus of the foregoing concerns is on the intrusive character of the search in question, rather than other characteristics peculiar to eavesdropping that distinguish it from its conventional analog. The focus in this Article is on certain eavesdrop characteristics apart from intrusiveness that tend to distinguish this type of search from a conventional one and which arguably support consideration of a heightened standard of probable cause.

59. U.S. CONST. amend. IV.

at no point drop, and then distort the significance of interceptions by lending undue import to ambiguous data. It may be observed that, as an alternative to either of the forgoing positions, the notion of a heightened standard of probable cause *ab initio* perhaps justifies such temporary shortfalls in the collective probative value of evidence as are bound to occur in the course of an extended eavesdrop.

IV. THE CONTINUITY OF PROBABLE CAUSE IN AN EAVESDROP

The statutory regulation of eavesdropping under Title III eliminates many "general warrant"[60] problems by requiring minimization,[61] particularization,[62] and other restrictions on eavesdropping in the course of an investigation.[63] Despite these limitations, the

60. *Berger* summarily described "general warrants" as allowing:

> blanket authority to conduct general searches for goods imported to the Colonies in violation of the tax laws of the Crown. The Fourth Amendment's requirement that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized," repudiated these general warrants and "makes general searches . . . 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."

United States v. Berger, 388 U.S. 41, 58 (1967) (quoting Marron v. United States, 275 U.S. 192, 196 (1927) and citing Stanford v. Texas, 379 U.S. 476, 481 (1965)).

61. "Minimization" requires that police officers executing eavesdropping warrants "seek to avoid the interception of non-authorized conversations." Goldstock and Chananie, *supra* note 13, at 1866; *see also*, J. CARR, *supra* note 8, § 5.7(a), at 5-27 n.149. Thus, an effort to minimize should result in the temporary cessation of the recording and overhearing of conversations determined, after an abbreviated, initial period of listening, to be not relevant to criminal activity.

62. Minimization may be regarded as an aspect of the "particularity" requirement of the fourth amendment, which specifies that a warrant must particularly describe "the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. "The Supreme Court has explained that '[t]he 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.' " Goldstock and Chananie, *supra* note 13, at 1873 (quoting Andresen v. Maryland, 427 U.S. 463, 480 (1976)). Given a sufficiently particularized warrant, police must execute it in a manner that minimizes undue intrusiveness, and it is this limitation of conduct to which minimization is generally understood to correspond. *See id.* at 1874. Thus, particularity requires prior specification of government conduct, as well as the minimization of an intrusion by limiting the execution of the search so as to comply with such prior specification.

63. 18 U.S.C. § 2518(1)(b) (1988) requires that an application contain details of probable cause and particularity. Section 2518(1)(d) requires detailed justification for the duration of the search. Pursuant to § 2518(5), extension applications must satisfy the requirements of § 2518(1), as for an original application, and must include a statement of the eavesdrop's results or an explanation of its failure, pursuant to § 2518(1)(f). Arguably, in addition to these requirements, the stratified governmental application procedures

opportunity to monitor the conversations of even unnamed targets and discern whether evidence of criminal activity may be found, over such lengthy periods as a year or longer,[64] continues to bear some of the traits of a general warrant.

By imposing only minimal judicial control over the government's discretion in determining precisely when a given electronic eavesdrop should cease, Title III appears to overlook any failure of particularization of the evidence sought in the course of an extended search.[65] Professor Carr advocates improvements in Title III which would require "judicial definition of the particular objective in individual surveillance applications and orders."[66] Professor Carr notes that under Title III, surveillance may continue until the objective has been achieved, so long as extensions are obtained.[67] Because the definition of the surveillance objective is en-

---

set forth in Title III, which allow only certain designated government attorneys to authorize an eavesdrop application, act to minimize unwarranted eavesdrops. The argument that these procedures alone justify a conventional standard of probable cause, however, overlooks the point that the judiciary, not the prosecution, bears the constitutional burden of determining probable cause. *See id.* § 2516; *cf.* Katz v. United States, 389 U.S. 347 (1967) (reaffirming need for antecedent judicial finding of probable cause). Nor do the "exhaustion" or "no alternative means" provisions of Title III inherently justify the use of a conventional standard. *See* 18 U.S.C. §§ 2518(1)(c),(3)(c) (1988). Although a court must review the proposition that a conventional investigation would not readily suffice as a means to accumulate sufficient evidence for a full prosecution of a conspiratorial enterprise, this review has no bearing on whether stronger evidence (derived from conventional means) regarding such activity should be required at the threshold to establish probable cause. A problem arises only when a conspiracy is so invulnerable to conventional investigation that a heightened standard of probable cause could not be satisfied. This consideration should be factored into a determination of how great an incremental increase is warranted in establishing a heightened standard, but it should not preclude such a standard altogether.

64. The continuity of probable cause is also at issue within the confines of a single authorized period of eavesdropping:

> [I]t seems apparent that once probable cause has dissipated by virtue of an unproductive or exculpatory investigation, surveillance cannot constitutionally continue. The statute, however, provides only limited means for enforcing this principle. Under section 2518(6), the issuing judge may direct that periodic reports be submitted 'showing what progress has been made toward achievement of the authorized objective and the need for continued interception.' Presumably, should these reports reveal the loss of probable cause, termination of surveillance would be required. In addition, the existence of probable cause must be reviewed whenever applications for extensions are filed.

GOLDSMITH, *supra* note 13, at 136 (footnotes omitted). It is the latter context, over the course of one or more extensions, to which the analysis in this Article primarily is directed. Professor Goldsmith concluded that "[n]either of these safeguards, however, has proven adequate." *Id.*

65. *See* J. CARR, *supra* note 8, § 2.5(c)(3), at 2-32.

66. *Id.* at 2-31.

67. *Id.*; *see also* 18 U.S.C. § 2518(5) (1988).

tirely at the executing officer's discretion, the duration of the surveillance likewise is relegated to the officer, because it is the officer, and not the court, who defines the objective and thus determines when it has been attained.[68] Without effective control over the duration of a search, a court has little ability to regulate with any precision the evidence to be obtained. Professor Carr thus argues that the strict judicial control of the surveillance period mandated by *Berger v. New York*[69] and the fourth amendment cannot be achieved under the current statutory scheme.[70]

Of course, there are limitations upon the ability of a court to define surveillance objectives in the electronics context and, consequently, to exercise control over the duration of interception. At the outset, the inchoate nature of an electronic search imposes limitations without analogy in the conventional search context. Unlike a conventional search, electronic surveillance produces evidence that is not yet in existence and is therefore peculiarly resistant to prospective description. In the conventional context, description of the evidence sought serves to provide judicial control over the extent of the search.[71] There, the seizure of predescribed evidence terminates the search, its goal having been achieved, and triggers the withdrawal of government presence. But the government necessarily lacks definitive knowledge of what will emerge in the course of an electronic search. Because the government is not limited by the "physical characteristics of the item," which would otherwise "limit the intrusiveness"[72] of a conventional search, the government cannot provide, and hence a court cannot require, a precise description of what will be seized and when the search will end.[73]

Professor Carr has discerned this inverse relationship between eavesdrop-specific limitations in defining the surveillance objective, and judicial control over the duration of the surveillance. As difficulty of description increases, judicial control decreases. The result is a potential failure to satisfy fourth amendment particularity requirements. But it is not clear that a statute-based invitation for increased judicial participation in defining surveillance objectives will adequately address the problem of an electronic search that, by

68. J. CARR, *supra* note 8, § 2.5(c)(3), at 2-31.
69. 388 U.S. 41 (1967); see discussion *supra* text accompanying notes 39-41.
70. J. CARR, *supra* note 8, § 4.4(h), at 4-80-4-81.
71. *Id.* § 2.5(c)(1)(C), at 2-25.
72. *Id.* at 2-26.
73. *Id.*

its nature, defies a predescribed terminus, even with the best intentions of both prosecutor and court.

Other limitations inherent in the use of a renewable eavesdrop order are even more resistant to reform. Once evidence is obtained by an eavesdrop, fourth amendment problems relating to its characterization do not cease. The problem touches upon the constitutional requirement of particularity, but more directly implicates the issue of the quantum of evidence constitutionally required to maintain probable cause throughout an extended search.[74] One striking distinction between conventional and electronic searches is the relative duration of each type of search. Probable cause must be re-established upon each application for an extension of the thirty-day maximum period allotted for an eavesdrop.[75] Each application must describe the conversations intercepted during the previous eavesdrop period,[76] or a reasonable explanation for the

74. " 'There is a large difference between the two things to be proved [guilt and probable cause], as well as between the tribunals which determine them, and therefore a like difference in the *quanta* and modes of proof required to establish them.' " United States v. Ventresca, 380 U.S. 102, 108 (1965) (quoting Brinegar v. United States, 338 U.S. 160, 173 (1949)). Case law is silent, however, on the percentage of probable success necessary to establish probable cause. *But see* Illinois v. Gates, 462 U.S. 213, 238 (1983) (magistrate must discern a "fair probability" that evidence will be found in a particular place). It would appear that the standard of probable cause shifts within the context in which it is applied. Based on his analysis of positions implicitly adopted in the case law, as well as construction of policy concerns, Professor LaFave has argued that the requisite probability should be (and generally is) diminished (i.e., less than 50%) in the context of arrest following a known crime, and heightened (i.e., greater than 50%) in a nonexigent search for evidence, particularly when it is not certain that a particular crime has been committed at all. *See generally* 1 W. LAFAVE, *supra* note 17, § 3.2(e). *See also* Burnett, *Evaluation of Affidavits and Issuance of Search Warrants: A Guide for Federal Magistrates*, 64 J. CRIM. L. & CRIMINOLOGY 270, 271 (1973) ("[e]mploying a mathematical concept, the magistrate must be at least fifty-one percent satisfied after reading the affidavit and considering everyday factual experiences on which reasonable and prudent men act, that the factual assertions justify the conclusion that a search of the premises will uncover the items sought"). Such a differentiated standard reflects the clear need for an arrest closely following the commission of a known crime, and a lesser need in arrest or search contexts involving uncertainty whether a crime was actually committed. Considerations in the known-crimes context relate to the need of police expeditiously to detain and identify suspects immediately following the commission of a crime, at the risk of losing the opportunity to conduct show-ups by eyewitnesses. In contrast, a search undertaken for the purpose of determining whether a crime in fact occurred is not limited to the identification of a suspect (and is consequently more intrusive), and does not so readily justify a reduced standard of probable cause, as it is not driven to the same extent by exigency. *See generally* 1 W. LAFAVE, *supra*, note 17, § 3.2(e).

75. 18 U.S.C. § 2518(5) (1988). There is no statutory limit on the number of extensions that may be obtained by the Government. *See* J. CARR, *supra* note 8, Sec. 5.10; C. FISHMAN, *supra* note 14, § 177.

76. 18 U.S.C. § 2518(1)(f) (1988).

failure to obtain pertinent conversations.[77] The presentations are intended to supplement, and should to some extent displace, the initial evidence presented to the court as probable cause. The initial showing will become remote temporally[78] and will either be enhanced or diminished by the character of the communications actually intercepted once surveillance has commenced. Consequently, probable cause is not constant, but fluctuates in the course of an eavesdrop.[79]

---

77. *Id.*; C. FISHMAN, *supra* note 14, § 179.

78. The greater the number of extensions authorized, the more remote in time (or "stale") becomes the initial evidence supporting probable cause:

> It does not satisfy the probable cause standard if the government can demonstrate only that the items to be seized could have been found at the specified location at some time in the past. Rather, the Government must reveal facts that make it likely that the items being sought are in that place when the warrant issues.

United States v. Domme, 753 F.2d 950, 953 (11th Cir. 1985) (citing U.S. v. Tehte, 722 F.2d 1114, 1119 (3d Cir. 1983), *cert. denied*, 466 U.S. 904 (1984)). "Staleness is more often a problem in the federal courts, due primarily to the stratified authorization process employed by the Department of Justice." Goldsmith, *supra* note 13, at 133.

79. "With wiretaps, however, the degree of probable cause existing during the course of the investigation may fluctuate, since the growing amalgam of information received during the tap more sharply defines the skeletal data, inferences and sophisticated suspicions with which the investigation began." United States v. Bynum, 360 F. Supp. 400, 404 (S.D.N.Y.), *aff'd*, 485 F.2d 490 (2d Cir. 1973). *Bynum* observes that the interception of data over time will cause probable cause to fluctuate. Another formulation of the issue of fluctuating probable cause states the problem as follows:

> [O]nce surveillance commenced, the best indicator of whether probable cause continued was the fruits of the actual surveillance conducted, rather than the informants' predictions of what future surveillance might uncover. Thus, as time went by, the informants' information became relatively more stale, and the results thus far obtained relatively more important.

United States v. Dorfman, 542 F. Supp. 345, 363 (N.D. Ill.), *aff'd*, 690 F.2d 1217 (7th Cir. 1982). Nevertheless, it would appear that the problem in the electronics context of the fading probative value of an original probable cause showing has not been recognized sufficiently in the case law. "[E]ven when properly issued, lengthy surveillances routinely have been allowed without regard to the possibility that intervening factors may have vitiated the original probable cause." Goldsmith, *supra* note 13, at 133. The technical issue of staleness has not been deemed particularly important, as a practical matter, when conventional search warrants have been issued with respect to a conspiracy. Likewise, because criminal activity monitored electronically by the government is usually of a protracted nature, staleness problems would appear to be diminished depending upon the types of cases in which the use of eavesdropping is sought. *See, e.g.*, *Domme*, 753 F.2d at 953; *Dorfman*, 542 F. Supp. at 363; *see also* Goldsmith, *supra* note 13, at 134 ("[t]ypically, staleness arguments have been rejected because of the continuing nature of the criminal activity under consideration").

It would seem that staleness necessarily should not receive identical treatment in the conventional and electronic contexts, because in an eavesdrop, the same item of stale information is relied upon to sustain probable cause over a continuing and more extensive period of time. The *Dorfman* formulation of fluctuating probable cause more appropriately acknowledges staleness in the electronics context, by proposing that probable cause can diminish significantly due to increasing staleness following commencement of the

Interceptions of conversations that clearly demonstrate the existence of particular criminal activity generally pose few problems of characterization. Matters are quite different in an extension application or progress report, in which a warrant court[80] is presented with intercepted data that only ambiguously implicates either the existence of criminal activity or the character of the particular activity. In these cases, the conversations must be characterized by reference to evidence presented either in the initial application or in some previous extension application or progress report. Ambiguous conversations that are seized in the course of an eavesdrop may operate to characterize, in turn, future ambiguous communications, the accuracy of which depends upon the respective accuracy of several prior characterizations. Because the total number of eavesdrop extensions is unregulated by Title III, purported showings of probable cause may be grounded on false characterizations that have been compounded many times in the course of an eavesdrop. Thus, in some cases, probable cause may drop below a constitutionally sanctionable threshold, while maintaining the appearance of integrity due to flawed characterizations at one or more junctures.

The interception of ambiguous data may be deemed corroborative of the initial evidence. But it may only be evidence of a mistaken theory of criminal activity. This possibility, which imports some degree of uncertainty into the process, should be considered. Analytic considerations, then, should not be limited to the increasing remoteness in time of the initial set of evidence[81] and the consequent diminution of its value in accurately characterizing ambiguous data as further evidence of criminal activity. Of course,

---

eavesdrop, even to the point at which the requisite quantum of evidence to support a theory of criminal activity no longer exists. Sufficient probable cause to support a particularized theory of criminal activity is, of course, a constitutional and statutory prerequisite to either an electronic or conventional warrant. *See* Goldsmith, *supra* note 13, at 52-53. But even the *Dorfman* formulation unnecessarily limits its conceptualization of diminishing probable cause to problems of staleness. It is proposed here that, although staleness relates only to the fading value of the original evidentiary showing, the interception of nonincriminating or highly ambiguous data actually contradicts, as a matter of probability, the existence of the evidence sought. It would seem logical to factor in the negative weight (in the sense that it has some counterprobative value, rather than simply no value) of intercepted data against the original probable cause showing when determining whether continuing probable cause has been demonstrated. These considerations appear to be without true analog in a conventional search.

80. The term "warrant court" is used here synonymously with a court responsible for the issuance of an eavesdrop "order" or extensions thereto.

81. *See supra* note 78; *see also* C. FISHMAN, *supra* note 14, § 181, at 275 (initial facts sustaining probable cause may become "stale . . . or discredited by the lack of fruitful interceptions").

one should consider that corroborating evidence may not be available in the target premises or from the target individuals during the anticipated period of time. Thus, ambiguous communications should not constitute merely data corroborative of probable cause, on the one hand, or be dismissed as without significance, on the other, with analytic recourse only to staleness analysis. Rather, the interception of ambiguous data introduces a negating factor that may demonstrate a lack of probable cause. Consequently, anticipating the seizure of ambiguous data, the requisite showing of probable cause should be high enough to show a fairly strong degree of certainty that the communications will actually comprise evidence of the specified criminal scheme. A higher standard would compensate for the negative impact of ambiguous or nonincriminatory data that erodes, but does not eliminate, the reasonable possibility that the theory of criminal activity supporting probable cause in fact is correct.

A brief hypothetical illustrates these issues. Assume that the government has applied to eavesdrop on communications of an alleged narcotics conspiracy which it believes operates from the basement office of a restaurant. The government also anticipates possible gambling activity in the targeted situs, but fails to include evidence of gambling in its application for an intercept.[82] Having met the conventional threshold showing of probable cause in regard to the narcotics charges, the government is granted a thirty-day intercept period and subsequently two successive thirty-day extensions.

After three months surveillance, seized communications consist primarily of references to debts and the repetitious counting of money. It is apparent that the communications intercepted during the hypothetical eavesdrop fail to implicate specifically either narcotics or gambling activity, although they may support one or both charges, and although suspicious, may even be innocent in nature.[83] On the basis of the rationale that the communications

82. For purposes of this hypothetical, assume that the government believes that it has adequate alternative means to ascertain the nature and extent of any gambling activities on the target premises and therefore declines to apply for an eavesdrop order for such purposes. An eavesdrop is permitted only if "alternative investigatory methods cannot accomplish the goals and purposes of the particular investigation." J. CARR, *supra* note 2, § 4.4 (d), at 4-52 (discussing 18 U.S.C. § 2518(3)(c) (1988)).

83. At the same time, because of the uncertain character of the evidence, it cannot be established clearly that the objective of the search was attained, thus averting the termination mandated by Title III when the objective is deemed achieved. Therefore, a separate issue arises: whether the "plain view" exception to a search warrant justifies the government's interception of conversations pertaining to unrelated criminal activity. The

might indicate narcotics, complemented by the initial showing that narcotics activity may be afoot, the intercepted data probably would be viewed by a court as justifying the government's continued presence in the targeted situs using a conventional probable cause standard. The ambiguous evidence, characterized as narcotics-related by reference to the initial showing of probable cause, not only comprises present probable cause, but will inform the character of future intercepted communications which similarly might relate to gambling or noncriminal activity. Thus is created a chain of ambiguous data. Each future link of this chain is defined less certainly as evidence of a targeted crime due to increasingly remote

---

"plain view situation refers to a post-intrusion observation in which a prior, valid intrusion has been extended to those objects in plain view from a legitimate viewing point." Comment, *"Plain View"—Anything but Plain:* Coolidge *Divides the Lower Courts*, 7 LOY. L.A.L. REV. 489, 489 n.3 (1974); *see also* 18 U.S.C. § 2517(5) (1988). In Coolidge v. New Hampshire, 403 U.S. 443 (1971), the Supreme Court held that "a seizure is justified by the plain view exception only when the police have a prior justification for an intrusion, when the incriminating nature of the object seized is immediately apparent, and when its discovery is inadvertent." Comment, *supra*, at 493 (footnotes omitted). Although most courts have accepted the "inadvertence" requirement, *id.* at 508, which seeks to prevent the warrantless seizure of evidence that the police anticipate will be found on the targeted premises, *Coolidge*, 403 U.S. at 469-71, the inadvertence requirement was "dropped" by Congress in the context of electronic eavesdropping, and an "incidental" requirement substituted, *see* SEN. R. NO. 1097, 90th Cong., 2d Sess. 12, *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2189. Although this deviation from what appears to be a still-effective constitutional requirement, *see* Comment, *supra*, at 510, has been followed by certain courts, it is not clear whether it has been followed by others, and it has been rejected by still others. *Compare* United States v. McKinnon, 721 F.2d 19, 22 (1st Cir. 1983) (distinguishing "incidental" from "inadvertent" or "unanticipated") *with* United States v. Marion, 535 F.2d 697, 700-01 (2d Cir. 1976) (equating "incidental" with "inadvertent") *and* People v. Di Stefano, 38 N.Y.2d 640, 648, 345 N.E.2d 548, 553, 382 N.Y.S.2d 5, 10 (1976) (equating "incidental" with "unanticipated"). Under the inadvertence standard, it would seem that the interception of evidence of anticipated criminal activity probably pertaining to gambling, but for which interception no prior application was made, would not qualify as a plain view seizure. This would hold true especially if the government had accumulated probable cause as to gambling and normally would be able to apply to a magistrate for a warrant. In the hypothetical, however, the government was constrained from applying to obtain gambling evidence because it had alternative investigatory means. Thus, an electronic search is not subject to a straightforward application of the otherwise constitutionally mandated inadvertence requirement. Of separate import to "plain view" considerations is the seizure of ambiguous data, which may be understood to correspond to either anticipated or unanticipated activity. Its true character is determinable at the time of interception only by ascribing to that characterization a degree of probability. Hence, the determination of whether the seizure of tangential data was anticipated, and the likelihood that the data are characterized accurately as evidence of a particular crime, collapse together as a function of the strength of the initial and subsequent showings that a particular activity is likely to occur in the targeted situs. A heightened probable cause standard, which "defines" intercepted communications with a greater degree of accuracy, clarifies the character of the intercepted data. This character must be established before inadvertence can be determined and thus incidentally affects the "plain view" doctrine.

references to the narcotics-specific evidence presented for the initial authorization. Moreover, the warrant court may overlook the converse implications of the ambiguous data: namely, the absence of specifically identifiable instances of narcotics-related activity, despite an extended intercept period and the measurable probability that the intercepted data relates to entirely nonsuspect activity.

The inherent problem of ambiguity might be compensated by a heightened probable cause standard for an electronic eavesdrop, at least *ab initio*. In light of the countervailing importance of maintaining a potentially valuable surveillance, the implementation of a heightened standard of probable cause more readily would justify the continuing intrusion of the government. The warrant court thereby could define more accurately the character of communications properly subject to seizure. Additionally, a heightened probable cause standard would support further determinations of probable cause despite periodic fluctuation; since ambiguous data more readily can be characterized as reflective of suspected criminal activity than if a lesser showing of probable cause initially had been made. Thus is justified a continued intrusion.

An interesting variation of the foregoing problem may be found in the Seventh Circuit's opinion in *United States v. Williams*.[84] That case involved evidence derived from a wiretap that had been placed on the telephone of Allen Dorfman, who ran an insurance company.[85] The evidence from this tap, which was in place for well over a year, justified the placement of "bugs" in the offices of Dorfman and another defendant.[86] The initial wiretap application, supported by an FBI agent's affidavit, stated "that there was probable cause to believe that Dorfman and others were illegally 'conspiring to establish, promote, manage, and/or receive compensation from hidden interests in one or more Reno and Las Vegas, Nevada, gambling casinos.' "[87] The affidavit relied on hearsay statements attributed to six confidential informants, one identified informant, and certain telephone toll and subscription records.[88]

Apparently, one of the confidential informants alleged that

84. 737 F.2d 594 (7th Cir. 1984), *cert. denied*, 470 U.S. 1003 (1985). Certain suppression issues considered in *Williams* were decided on the trial level in United States v. Dorfman, 542 F. Supp. 345 (N.D. Ill.), *aff'd*, 690 F.2d 1217 (7th Cir. 1982). The facts summarized in the text are derived from both the *Williams* and *Dorfman* opinions.

85. *Williams*, 737 F.2d at 600.

86. *Id.* at 600-01.

87. *Id.* at 600.

88. *Dorfman*, 542 F. Supp. at 370.

Dorfman charged inflated insurance premiums to several large Las Vegas hotel-casinos and split the proceeds with organized crime. This informant also alleged that Dorfman derived income through organized crime's hidden interest in a corporation that owned several Las Vegas hotel-casinos.[89] Another confidential informant alleged that Dorfman worked on behalf of organized crime, that money was "skimmed" from one of the casinos, and that Dorfman arranged loans from a union pension fund to those criminal interests.[90] The information provided by this informant no. 3 was deemed conclusory with respect to the Las Vegas casino allegations, but it sufficiently detailed attempts by Dorfman and others to obtain a hidden interest in a Reno casino and was amplified somewhat by a third informant.[91] All three informants alleged that the activities were carried on, in part, over Dorfman's home and office telephones in Chicago.[92] The trial court found that based on these hearsay allegations, there was probable cause to issue the initial wiretap order.[93]

The first thirty days' interceptions revealed no conversations pertinent to the allegations in the initial application.[94] Consequently, the first extension application largely reiterated the original allegations. The warrant court ruled, however, that the inclusion of certain additional allegations in the first extension application justified the issuance of an extension order. These allegations concerned a single, previously unmentioned hotel-casino, the

89. *Id.* at 371.

90. *Id.*

91. *Id.*

92. *Id.* at 371-72. The trial court held that the information cumulatively satisfied the then-followed *Aguilar-Spinelli* test, *see supra* note 50, for determining the reliability of an informant who is anonymous or part of the "criminal milieu," *see* W. LAFAVE & J. ISRAEL, *supra* note 50, § 3.3, at 114. The first prong of the test called for determination of the informant's "basis of knowledge" supporting his conclusions. This prong was deemed satisfied by the specification as to how the "skimming" operations were conducted, how Dorfman funneled casino money to organized crime, and how the purchase of the Reno casino would be financed. The court also found that the second prong of the test had been satisfied by corroboration of certain alleged details, the pattern of telephone usage as reflected in toll and subscriber records, and the rather general allegations of three other confidential informants, two of whom had provided somewhat stale information. *Dorfman*, 542 F. Supp. at 372.

93. *Dorfman*, 542 F. Supp. at 372.

94. United States v. Williams, 737 F.2d 594, 601 (7th Cir. 1984), *cert. denied*, 470 U.S. 1003 (1985); *Dorfman*, 542 F. Supp. at 374. Moreover, in its first extension application, the government entirely failed to satisfy the statutory requirement that an extension application explain a failure to obtain results corroborating the initial allegations, an omission deemed "critical" by the trial court. *Dorfman*, 542 F. Supp. at 374 (citing 18 U.S.C. § 2518(1)(f) (1988)). This failure apparently resulted from an oversight of the warrant court. *Williams*, 737 F.2d at 601.

Aladdin.[95] The extension order was predicated upon intercepted telephone conversations seized during the first thirty days, which appeared to involve discussion of a failed attempt by a corporate entity to refinance the Aladdin and another casino, together with "veiled references"[96] regarding the "handling" of a "bid" and Dorfman's efforts to get another group to "back off."[97] Eventually, it became clear that the allegations contained in both the initial application and the first extension proved to be false.[98] The conversations allegedly involving the Aladdin actually involved the defendants' efforts to influence the sale of real property by a management company[99] in a manner agreeable to a United States senator, who then might consider favorably the legislative interest of the union for which the defendants worked.[100] Allegations of this conduct were not included until the third extension application, which was filed almost three months after the electronic surveillance began.[101]

The trial court found that the first extension application was unduly terse in providing a theory of linkage between the Aladdin and the highly ambiguous references to a "bid," but held that this connection could have been inferred independently by the warrant court without guidance by the prosecution.[102] The Seventh Circuit described the allegations relating to the Aladdin as "ample" to support the findings of the warrant court, and further characterized as "surplus" the unsubstantiated allegations regarding the other casinos, which had comprised the entire initial application and most of the first extension application.[103]

It is clear from the reviewing courts' opinions that the warrant court was left entirely without assistance from the government in

95. *Dorfman*, 542 F. Supp. at 375-76.

96. *Id.* at 375. The "veiled references" appear to relate only to the identity of certain individuals. *See id.* n.28.

97. *Id.* at 375.

98. *Williams*, 737 F.2d at 602.

99. The management company controlled the real property holdings of a union pension fund to enable the fund to retain tax-exempt status. *Id.* at 598.

100. *Id.* at 598-600.

101. *Id.* at 604.

102. United States v. Dorfman, 542 F. Supp. 345, 376-78 (N.D. Ill.), *aff'd*, 690 F.2d 1217 (7th Cir. 1982). The linkage between the "bid" references and the Aladdin was ambiguous to the extent that it was characterized by negation: "[I]f there is one word which does not describe the conversations the government believed were Aladdin-related, it is 'obvious.' All the conversations are easily characterized as veiled." *Id.* at 380. Such analysis arose, however, only in the course of a hearing whereby it became significant to disprove the government's intentional or reckless representation of the evidence. *Id.*

103. *Williams*, 737 F.2d at 601.

discerning a relationship between ambiguous references to "bids" and the Aladdin casino. It is more apparent that the warrant court could have reached no conclusions about the character of the ambiguous data without the "surplus" allegations, which ultimately turned out to be false. The reviewing courts should have discussed the impact of this "surplus" information on the ambiguous data that purportedly justified a continued eavesdrop. An analysis of which information was surplus would not only have limited the later use of that data in support of probable cause, but would have recognized its negative impact on the probability that the defendants actually were engaged in the type of activity described.

The reviewing courts in *Williams*, however, did not focus upon these fundamental considerations. Instead, the courts narrowly considered whether the warrant court conceivably could have inferred a linkage between the ambiguous references and a previously unnamed hotel, as if such a linkage could have occurred without reference to the failed probable cause findings regarding all the other transactions. The warrant court must have credited the initial allegations of criminal financial relationships and imputed some of that probative force to the purported relationship between the newly alleged Aladdin scheme and the intercepted data concerning "bids." Had these courts focused upon the counter-corroborative facts, the evidence likely would have been too tenuous to sustain probable cause. But the intercept and the counter-corroborative evidence that it produced was analytically severed and treated as if it had no relevance. By holding the initial allegations to be mere surplusage, *Williams* overlooked the failure of the warrant court to identify the diminishing probable cause stemming from the failure of the intercept to yield corroborative results.

The ambiguous intercepted data related to allegations, at all stages of the eavesdrop, which were supported by evidence that satisfied only a conventional standard of probable cause. Had a greater quantum of proof been required, the government may have had to refine its theory before undertaking the lengthy series of eavesdrops. Conventional investigation might have induced the government to modify its misplaced theory of criminal activity. As a consideration of policy, the adherence to a conventional probable cause standard *ab initio* encourages the use of eavesdropping. It does not encourage the government to refine and gather evidence with respect to particularized allegations of criminal activity.

Williams also demonstrates the courts' apparent tendency to overlook the negative impact of highly ambiguous data and the

consequent dilution of the probable cause standard when fluctuating showings occur. In *Williams*, the possible failure to meet even conventional probable cause requirements was masked by terming the unsuccessful allegations mere "surplus."[104] A higher standard of probable cause at all stages would permit surveillance to continue only when probable cause is sufficiently strong to compensate for the negative impact of ambiguous data. The interception of ambiguous data, however, might severely erode probable cause, which could not be established successively if measured by a heightened standard. This erosion results from the tendency of probable cause to fluctuate downward upon interception of ambiguous data and under other circumstances. One resolution of the problem may be to require a heightened showing of probable cause only at the commencement of an eavesdrop, with reversion to the conventional standard, or even very brief substandard showings during the extension periods. Judicial or legislative acknowledgement of the issues and problems in this area undoubtedly would clarify the competing considerations.

V. Contemporary Case Law and Probable Cause Analysis in the Electronics Context

All circuit courts of appeal, as well as many other courts, have held that the standard of probable cause governing electronic eavesdropping applications is the same as for conventional warrants.[105] No court, however, appears to have identified Supreme

104. *Williams*, 737 F.2d at 604; *Dorfman*, 542 F. Supp. at 375-78.

105. *See, e.g.*, United States v. Gallo, 863 F.2d 185, 191 (2d Cir. 1988), *cert. denied*, 109 S.Ct. 1539 (1989); United States v. Leisure, 844 F.2d 1347, 1354 (8th Cir.), *cert. denied*, 488 U.S. 932 (1988); United States v. Savaiano, 843 F.2d 1280, 1286 (10th Cir.), *cert. denied*, 488 U.S. 836 (1988); United States v. Zambrana, 841 F.2d 1320, 1332 (7th Cir. 1988); United States v. Alfano, 838 F.2d 158, 161 (6th Cir.), *cert. denied*, 488 U.S. 821 (1988); United States v. Cardall, 773 F.2d 1128, 1131 (10th Cir. 1985); United States v. Brown, 761 F.2d 1272, 1275 (9th Cir. 1985); United States v. Domme, 753 F.2d 950, 953 (11th Cir. 1985); United States v. Tehfe, 722 F.2d 1114, 1118 (3d Cir. 1983), *cert. denied*, 466 U.S. 904 (1984); United States v. Talbert, 706 F.2d 464, 467 (4th Cir. 1983); *In re* De Monte, 674 F.2d 1169, 1173 (7th Cir. 1982); United States v. Martino, 664 F.2d 860, 867 (2d Cir. 1981); United States v. Weinrich, 586 F.2d 481, 487 (5th Cir. 1978), *cert. denied*, 441 U.S. 927 (1979); United States v. Hyde, 574 F.2d 856, 862 (5th Cir. 1978); United States v. Fury, 554 F.2d 522, 530 (2d Cir.), *cert. denied*, 436 U.S. 931 (1977); United States v. Ford, 553 F.2d 146, 165 (D.C. Cir. 1977); United States v. Scibelli, 549 F.2d 222, 226 (1st Cir.), *cert. denied*, 431 U.S. 960 (1977); United States v. Feldman, 535 F.2d 1175, 1179-80 (9th Cir.), *cert. denied*, 429 U.S. 940 (1976); United States v. Falcone, 505 F.2d 478, 481 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975); United States v. Paredes-Moya, 722 F. Supp. 1402, 1418 (N.D. Tex. 1989); United States v. Persico, 621 F. Supp 842, 861 (S.D.N.Y. 1985); United States v. Shipp, 578 F. Supp. 980, 985 (S.D.N.Y. 1984); United States v. Tufaro, 593 F. Supp. 476, 479 (S.D.N.Y.

Court authority that specifically upholds this position. Electronic eavesdrop decisions espousing a conventional-warrant standard of probable cause either rely upon Supreme Court authority that does not address the issue or defer without discussion to the opinions of other circuits that are similarly without substantive analysis of the pertinent constitutional and policy considerations.

A relatively old source of authority equating probable cause standards in the conventional and electronic contexts is *People v. Kaiser*.[106] This New York case and its Supreme Court affirmance simply do not supply authority for the proposition for which they are often cited. In *Kaiser*, the New York Court of Appeals wrestled with the belief that the fourth amendment should not apply to wiretapping. The court stated that at the time the warrant court issued the wiretap order, the Supreme Court was still following *Olmstead v. United States*,[107] which ruled that wiretapping made without a trespass did not violate the fourth amendment. The court observed that *Olmstead* still had not clearly been rejected by the Supreme Court.[108] The state court believed, however, that the warrant satisfied the reasonableness requirements, as previously understood, of the New York State Constitution and state laws.[109]

1983), *aff'd*, 762 F.2d 991 (2d Cir.), *cert. denied*, 474 U.S. 826 (1985); United States v. DePalma, 461 F. Supp. 800, 807 (S.D.N.Y. 1978); United States v. Baynes, 400 F. Supp. 285, 295 n.17 (E.D. Pa.), *aff'd mem.*, 517 F.2d 1399 (3d Cir. 1975); People v. Tambe, 71 N.Y.2d 492, 500, 522 N.E.2d 448, 451, 527 N.Y.S.2d 372, 375 (1988); People v. Manuli, 104 A.D.2d 386, 387, 478 N.Y.S.2d 712, 713 (1984); People v. Fusco, 75 Misc. 2d 981, 989, 348 N.Y.S.2d 858, 869 (Nassau County Ct. 1973); *see also* J. CARR, *supra* note 8, § 4.4(c), at 4-29-4-30 (citing United States v. Gonzalez, 866 F.2d 781, 786 (5th Cir. 1989); State v. Olea, 139 Ariz. 280, 290, 678 P.2d 465, 475 (Ct. App. 1983); People v. Milnes, 186 Colo. 409, 417-18, 527 P.2d 1163, 1165 (1974); and Tookes v. State, 159 Ga. App. 423, 423-24, 283 S.E.2d 642, 644 (1981), *cert. denied*, 455 U.S. 945 (1982)). These cases also generally accord deferential review to the conventionally based probable cause determinations of the warrant courts. *But see*, United States v. Washington, 782 F.2d 807, 818 n.13 (9th Cir. 1986) (conducting de novo review of search warrant challenged for failing to particularly describe the items to be seized) (citing United States v. McClintock, 748 F.2d 1278, 1282 (9th Cir. 1984), *cert. denied*, 474 U.S. 822 (1985)); United States v. McConney, 728 F.2d 1195, 1200 n.4 (9th Cir.), *cert. denied*, 469 U.S. 824 (1984).

106. 21 N.Y.2d 86, 233 N.E.2d 818, 286 N.Y.S.2d 801 (1967), *aff'd*, 394 U.S. 280 (1969). Among the New York cases relying exclusively upon *Kaiser* are People v. Tambe, 71 N.Y.2d 492, 522 N.E.2d 448 (1988) and People v. Manuli, 104 A.D.2d 386, 478 N.Y.S.2d 712 (1984), which held that "the probable cause necessary for the issuance of an [electronic] eavesdropping warrant is measured by the same standards used to determine whether probable cause exists for the issuance of a search warrant." *Tambe*, 71 N.Y.2d at 500, 522 N.E.2d at 451. They also review the issuing court's determination by an abuse of discretion standard. *See id.* at 500-01, 522 N.E.2d at 451; *Manuli*, 104 A.D.2d at 387, 478 N.Y.S.2d at 713.

107. 277 U.S. 438 (1927), discussed *supra* notes 24-27 and accompanying text.

108. *Kaiser*, 21 N.Y.2d at 95, 233 N.E.2d at 823, 286 N.Y.S.2d at 808.

109. *Id.*

The New York court also held that the search warrant at issue in *Kaiser* predated fourth amendment requirements newly established in *Berger v. New York*,[110] such as the requirement that the warrant adequately specify the precise conversations sought.[111] Moreover, the court asserted that the requirements of *Berger* had never been previously set forth or deemed mandatory by the Supreme Court.[112] The court further determined that *Berger* was prospective in effect and did not impose fourth amendment requirements upon nontrespassory wiretapping.[113]

The Supreme Court, in its narrowly crafted affirmance, held that the warrant at issue need not comply with the fourth amendment requirements, because its decision in *Berger* did not vitiate the trespass doctrine of *Olmstead*.[114] Although *Katz v. United States*[115] rejected the trespass doctrine and imposed the requirements of the fourth amendment upon wiretapping, its effect was prospective only, and therefore the warrant at issue in *Kaiser* yielded admissible evidence under the fourth and fourteenth amendments.[116] Consequently, *Kaiser v. New York*, the authority upon which the Second Circuit's opinion in *United States v. Fury*[117] partially rests, did not undertake constitutional analysis pursuant to the fourth amendment.[118] Because *Kaiser* was decided entirely without re-

110. 388 U.S. 41 (1967), discussed *supra* notes 39-43 and accompanying text.
111. *Id.* at 96-97, 233 N.E.2d at 823-24, 286 N.Y.S.2d at 808-10.
112. *Id.*
113. *Id.* at 98-101, 233 N.E.2d at 825-27, 286 N.Y.S.2d at 810-14.
114. *See* Kaiser v. New York, 394 U.S. 280, 282 (1969).
115. 389 U.S. 347 (1967), discussed *supra* note 5 and text accompanying note 43.
116. *See Kaiser*, 394 U.S. at 282-83.
117. 554 F.2d 522, 530 (2d Cir. 1977).
118. *Fury* cites, without discussion, two additional authorities: United States v. Falcone, 505 F.2d 478, 481 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975) and People v. Fusco, 75 Misc. 2d 981, 348 N.Y.S.2d 858 (Nassau County Ct. 1973). *See Fury*, 554 F.2d at 530. The sole authority cited by *Fusco* is *Kaiser*. Consequently *Fusco*, like *Kaiser*, is without roots in the fourth amendment and has no authoritative value. *See Fusco*, 75 Misc. 2d at 989, 348 N.Y.S.2d at 869. *Falcone* is a Third Circuit case which, contrary to such Supreme Court cases as Zurcher v. Stanford Daily, 436 U.S. 547, 556 (1978), flatly rejects varying degrees of "vigor" in probable cause determination. *Falcone* cites as authority Spinelli v. United States, 393 U.S. 410 (1969) and Aguilar v. Texas, 378 U.S. 108 (1964), neither of which considered electronic interception of communications. *See supra* note 50 and accompanying text; *see also Falcone*, 505 F.2d at 481. Thus, *Falcone* cites no meaningful authority and fails to account for uncontested Supreme Court authority that contradicts its postulate of nondifferential standards of probable cause.

Also relying in large part upon *Falcone* are the Courts of Appeals for the First, Fourth and Eighth Circuits. Within those circuits, alternative or supplemental authority to that of *Falcone* is inappropriate or unconvincing. For example, United States v. Talbert, 706 F.2d 464, 467 (4th Cir. 1983), cites as additional authority United States v. Baynes, 400 F. Supp. 285, 295 n.17 (E.D. Pa.), *aff'd mem.*, 519 F.2d 1399 (3d Cir. 1975), a case which cites *Falcone* and points to the absence of a "special probable cause requirement" in Title

course to the fundamental fourth amendment interpretations of *Berger* and *Katz*, its purported authority is neither determinative nor controlling. It is not even relevant.

The watershed case in federal probable cause analysis, and one of the Supreme Court authorities relied upon since 1983, is *Illinois v. Gates*.[119] In that case, the Court dispensed with a strictly bifurcated analysis of hearsay evidence and established a probable cause standard that favors a more "fluid" inquiry into the "totality-of-the circumstances."[120] There is no question that in *Gates*, the Court fully intended to satisfy the demands imposed by the fourth amendment in its assessment of a search warrant based on a partially corroborated tip by an anonymous informant.[121] The Court ruled, however, only on the application of the fourth amendment to conventional search warrants. Electronic surveillance was not at issue and was not even mentioned. Furthermore, none of the cases which cite *Gates* addresses the distinctions between an eavesdrop and a conventional search.[122] Seemingly, under *Gates*,[123] a

III. Further, United States v. Leisure, 844 F.2d 1347, 1354 (8th Cir.), *cert. denied*, 488 U.S. 932 (1988), cites as additional authority *Talbert* and *Fury*. Cases within the Fifth Circuit do not appear to cite *Falcone*, but like the Third Circuit, which crafted *Falcone* with the benefit of neither authority nor analysis, the Fifth Circuit appears to have established its precedent without discussion of pertinent distinctions. For example, United States v. Weinrich, 586 F.2d 481, 487 (5th Cir. 1978), *cert. denied*, 441 U.S. 927 (1979), cites United States v. Hyde, 574 F.2d 856, 862 (5th Cir. 1978), a case which does not appear to rest upon any pertinent authority. Yet other circuits readily rely upon these Fifth Circuit cases. *See, e.g.*, United States v. Alfano, 838 F.2d 158, 161 (6th Cir.) (citing *Weinrich*, 586 F.2d at 487), *cert. denied*, 488 U.S. 821 (1988).

119. 462 U.S. 213 (1983).

120. *See supra* note 50 for a discussion of the totality-of-the-circumstances standard.

121. *Gates*, 462 U.S. at 217.

122. Without discussion of pertinent distinctions, the Sixth, Seventh, Eighth, Ninth, and Tenth Circuits rely in significant part upon *Gates*. *See, e.g.*, United States v. Savaiano, 843 F.2d 1280, 1286 (10th Cir.) (citing Berger v. New York, 388 U.S. 41 (1967) (discussed *supra* text accompanying notes 39-41)), *cert. denied*, 488 U.S. 836 (1988); United States v. Zambrana, 841 F.2d 1320, 1332 (7th Cir.) (citing United States v. Hornick, 815 F.2d 1156 (7th Cir. 1987) (a conventional search warrant case); United States v. Alfano, 838 F.2d 158, 161 (6th Cir.) (citing United States v. Weinrich, 586 F.2d 481 (5th Cir. 1978) (discussed *supra* note 118) and United States v. Feldman, 535 F.2d 1175 (9th Cir.) (applying the *Aguilar-Spinelli* test in a purely conventional search context), *cert. denied*, 429 U.S. 940 (1976)), *cert. denied*, 488 U.S. 821 (1988); United States v. Cardall, 773 F.2d 1128, 1131 (10th Cir. 1985) (citing *Gates* and United States v. Berisford, 750 F.2d 57 (10th Cir. 1984) (a conventional search warrant case)); United States v. Brown, 761 F.2d 1272, 1275 (9th Cir. 1985) (citing United States v. Fury, 554 F.2d 522 (2d Cir. 1977) (discussed *supra* note 118)); United States v. Seybold, 726 F.2d 502, 503 (9th Cir. 1984) (a conventional search warrant case). Thus, purported authority is established not by analysis, but by cross-referencing between circuits; each strand evaporates as it is traced to its root.

123. A distinction is made here between the conventional standard of probable cause set forth in *Gates* and the general framework of flexible determination of reliability also

court might consider the particularly intrusive character of a proposed electronic search. The court might explicitly balance this factor against the evidence proffered by the government to justify that particular search. The "totality-of-the-circumstances" standard, with its inherent flexibility, would seem to authorize consideration of the degree of intrusiveness in the particular search proposed. The flexible approach of *Gates* also would appear to comprehend other distinguishing features, such as the problem of intercepting highly ambiguous data.

While the "totality-of-the- circumstances" approach is applicable to an eavesdrop as a general matter, the very presumptions upon which *Gates* is founded, and which are crucial to other portions of its holding, are largely inapplicable to the issues presented by an electronic search. In discussing the basis for its holding that the warrant-issuing authority should be accorded deference by a reviewing court in the context of a conventional warrant, the Supreme Court clearly had an overriding concern that the requisite standard of probable cause imposed upon a warrant court's review not be so great as to deter police from applying for warrants.[124] The *Gates* Court postulated that stricter scrutiny, and implicitly a stronger showing of probable cause exacted upon the initial application for a warrant, might prompt police to attempt to formulate some alternative basis within their powers that would justify a warrantless search.[125] The Court also reasoned that a warrant would mitigate that intrusion in the eyes of those subjected to the conventional search.[126] These same concerns, in *Massachusetts v. Upton*,[127] served as a basis for deference to the warrant-issuing magistrate.

It is clear that these considerations are not pertinent to the elec-

---

set forth in that case. Further, even the use in *Gates* of the term "a fair probability" connotes a flexibility which conceivably could command greater proof within the electronics context. *See supra* note 74 (discussing probable cause).

124. The Supreme Court stated in *Gates*:

> If the affidavits submitted by police officers are subjected to the type of scrutiny some courts have deemed appropriate, police might well resort to warrantless searches, with the hope of relying on consent or some other exception to the Warrant Clause that might develop at the time of the search. In addition, the possession of a warrant by officers conducting an arrest or search greatly reduces the perception of unlawful or intrusive police conduct, by assuring "the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search."

Gates, 462 U.S. at 236 (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)).

125. *Id.*

126. *Id.*

127. 466 U.S. 727, 732-33 (1984).

tronic eavesdropping situation. Therefore, it is also clear that the Court did not intend to implement fourth amendment regulation of electronic eavesdropping. First, recourse to a magistrate generally is necessary prior to electronic interception of communications by the government, and this warrant requirement is not diluted so easily by recourse to categorical exceptions as it is in a conventional context. Thus, for instance, *Gates* explicitly cited the consent exception.[128] In the electronic surveillance context, consent is not a feasible substitute for a warrant, because the nature of electronic interception requires surreptitious intrusion.[129] Therefore, the Supreme Court, which in the conventional context feared the potential recourse of police to a fabricated pretext of consented entry in lieu of a warrant, would not rely upon the *Gates* calculus to derive a standard of probable cause for an electronic search were it to consider the issue.[130]

128. *Gates*, 462 U.S at 236. The proposition that de novo review of the warrant court's probable cause determination conflicts with such policy considerations as the avoidance of consent-based intrusions and may also be limited to the conventional-warrant context, which gave rise to the deferential standard in *Gates*. The questions of what standard of probable cause should be required when police seek antecedent judicial authorization and whether this determination should be subject to the uncertainty of de novo review by a suppression or appellate court are related by their mutual concern that the police should not unduly be dissuaded from seeking a warrant and turn instead to the fabrication of some recognized exception to the warrant requirement. Although the standard of review to be applied to a probable cause determination is beyond the scope of this Article, one further observation is offered. The prospect of good faith reliance by police on a warrant, despite the eventual demonstration of some failing of the warrant, validated under the rule of United States v. Leon, 468 U.S. 897 (1984), is diminished when the eavesdrop order or extension is issued on the basis of ambiguous data. In this instance, the police have as little reason to believe that they have probable cause as the court would. In fact, a court attempting to determine whether to authorize an eavesdrop extension often may rely upon paraphrased communications whose meaning is derived from the application of police experience to the intercepted data. In attempting to find corroboration for the police interpretation, the court may reach back to previously intercepted data, which was itself characterized by reference to ambiguous data. Consequently, police necessarily should not be permitted to rely upon the court's determination under such circumstances. Thus, one might consider that the reasonableness of police "reliance" upon a court's determination of probable cause is less meaningful over the course of an extended electronic search than in the context of a conventional search.

129. *See* Dalia v. United States, 441 U.S. 238, 241 n.2 (1979). Manifestly, any "consent" obtained in the electronics context cannot be conveyed by the target of the search, thereby eliminating a significant categorical exception. Moreover, the consent required for a warrantless eavesdrop is that of a participant in the conversation, not that of a nonparticipant with some custody or control over a telephone, although the law is less clear with respect to premises. *See* C. FISHMAN, *supra* note 13, § 8, at 112, and § 22.1, at 168-69.

130. The need to minimize police abuses by providing the incentive of a warrant requirement reduced to the minimum necessary to pass constitutional muster plays a less meaningful role in the context of eavesdropping, in which the police are largely precluded from covertly intruding on the basis of pretexts such as "consent." Nevertheless, the

Nor is the other consideration articulated in *Gates* and *Upton*, a diminished perception of intrusion when a search is conducted pursuant to a warrant, applicable to the electronics context. Clearly, no government agent presents the court-issued warrant to the targets prior to an electronic search and seizure. *Katz* specified at the outset of this era of eavesdropping regulation that the categorical exceptions developed within the conventional search and seizure context have little or no application in the electronics context. The Court remarked that electronic eavesdropping could hardly be incidental to an arrest and by its very nature could never be justified on the grounds of hot pursuit or consent.[131] The Court's remarks undermine the rationale of *Gates* as applied to electronic eavesdropping because that case reasoned that the probable cause standard should be minimized in light of an anticipated recourse by police to purported categorical exceptions in order to circumvent the warrant requirement. If, after all, many of the conventional categorical exceptions to the warrant requirement justifying warrantless police intrusions do not apply in the electronics

---

incentive remains to the extent that unauthorized electronic surveillance could produce leads to other evidence, which then could be manipulated to appear independently derived. Of course, the burden upon a would-be renegade to falsify the derivation of this evidence should prevent commonplace recourse to this ploy. Moreover, renegade conduct may be less likely in the electronics context, which presumably calls for the implementation of centralized and supervised Title III operations. Although the potential for police abuse is apparently reduced under these circumstances, it cannot be gainsaid that police should be allowed to procure a warrant, whether conventional or electronic, by means of a reasonable and minimally technical process that does not encourage the unauthorized accumulation of evidence, the acquisition of which may be attributed retroactively to a conjured, "independent" lead. To dispense with the *Gates* rationale entirely would overlook the highly intrusive nature of surveillance. Nevertheless, discrepancies between electronic and conventional surveillance call for a re-evaluation of the assumptions underlying the traditional police incentive theory. Other issues include the potential tendency of police to respond to a heightened standard by increasing the number of penetrations of conspiracies by agents and informants, at increased risk to these individuals, who are free, of course, to operate consensual recording devices without a warrant. Additionally, these efforts might be pursued very vigorously, with a resulting increase in borderline entrapment situations. *See* United States v. White, 401 U.S. 745, 769-70 (1971) (Harlan, J., dissenting) (reporting frequent usage of the "consent" technique); *see also* 18 U.S.C. § 2511(2)(c), (d) (1988). Finally, there is the debatable prospect of conspiracies invulnerable to the accumulation of sufficient data to meet a heightened standard of probable cause by conventional means.

131. Katz v. United States, 389 U.S. 347, 357-58 (1967). "[w]hile the Court has permitted certain searches and seizures to stand even though a warrant had not been issued because of special surrounding circumstances, *e.g.*, 'hot pursuit,' consent or incidental to arrest, such exceptions are inappropriate in an eavesdrop situation." Comment, *supra* note 24, at 461 n.41 (citing *Katz*; United States v. Rabinowitz, 339 U.S. 56 (1950); Zap v. United States, 328 U.S. 624 (1946); and Agnello v. United States, 269 U.S. 20 (1925)).

context, then the probable cause requirement should be re-evaluated against more pertinent considerations.

For example, the observation in *Katz* that the categorical exception of "hot pursuit" is not significant in the electronics context — would appear to have been borne out by experience. Commentators have referred to the statutory provision of Title III permitting electronic interception in "an emergency situation"[132] as "never-utilized"[133] and have noted "few reported instances"[134] of its use. It is, of course, this provision which is intended to be invoked should there arise a need for electronic eavesdropping on an emergency basis akin to "hot pursuit" in the conventional context.[135] The absence of recourse to the provision is understandable. The use of electronic eavesdropping generally follows a prior, often lengthy investigation conducted by conventional means,[136] which probably explains why the exception generally is not applicable to eavesdropping.[137] In fact, the government apparently has adopted a policy against using this statutory authority to conduct emergency eavesdrops.[138]

In sum, the issuance of an eavesdrop order generally is not a function of any particular categorical exception involving an exigency of any sort.[139] Further, as *Katz* noted, conventional excep-

132. *See* 18 U.S.C. § 2518(7) (1988).

133. Cranwell, *supra* note 21, at 225 n.4.

134. J. CARR, *supra* note 8, § 3.7, at 3-107.

135. "Both Senate Report 1097 and the ABA Standards compare emergency electronic searches with warrantless searches which are allowed in conventional situations on the basis of exigent circumstances." *Id.* § 3.7(a), at 3-108 (citing S. REP. NO. 1097, 90th Cong., 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2193 and STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE 134 (Approved Draft 1971).

136. *See, e.g.*, C. FISHMAN, *supra* note 14, § 34, which describes the typical decision to seek a warrant as a consequence of and extension to the use of conventional investigative procedures that had yielded probable cause to undertake certain arrests or searches, but had not accomplished the broader goals of the investigation. It is worth noting in this context that this typical sequence of events normally should serve to provide the government with sufficient evidence to satisfy the demands of a heightened probable cause standard by the time it applies for an eavesdrop order.

137. Additional constraints upon the early or initial use in an investigation of electronic eavesdropping include the statutory requirement that the application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c) (1988); *see also supra* note 81. *See generally* J. CARR, *supra* note 8, § 4.4(d), at 4-52 (discussing the necessity requirement).

138. J. CARR, *supra* note 8, § 3.7, at 3-107.

139. *See* United States v. Ford, 553 F.2d 146, 164 (D.C. Cir. 1977) (the Supreme Court has recognized "that exigency factors will rarely, if ever, be present in instances of electronic surveillance").

tions, when the intrusion is an incidental aspect of arrest[140] or a matter of consent, also do not apply to electronic eavesdropping.[141] These distinctions, combined with the particularly intrusive nature of the search, seriously undermine the invocation of *Gates* as authority for the equivalence of probable cause standards in the conventional and electronic contexts.

Even more fundamental assumptions about the nature of probable cause-informing warrants in the conventional context have limited application to eavesdropping. Long before *Gates*, the Supreme Court observed that affidavits for search warrants "are normally drafted by nonlawyers in the midst and haste of a criminal investigation."[142] Yet it is clear that the decision to use electronic eavesdropping in most circumstances[143] is not hasty and usually follows conventional investigation.[144] Moreover, eavesdrop applications invite more precision in setting forth available justifying factors of reliability, because these applications consistently involve lawyers in both drafting and execution.[145] Therefore,

---

140. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

141. *See id.* at 358 n.22.

142. United States v. Ventresca, 380 U.S. 102, 108 (1965). "Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area." *Id.* The Court explicitly linked its concerns to the primary use of nonlawyer affidavits. *Id.*

143. The provisions of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1811 (1988), are not addressed here.

144. *See supra* note 136.

145. "Eavesdropping, more than any other pre-trial process the police are likely to be involved in, is lawyers' work. Problems arise which require an attorney's attention; events occur which only a prosecutor can effectively evaluate; decisions must be made which demand a prosecutor's input if they are to be made correctly." C. FISHMAN, *supra* note 14, § 34, at 51-52. Professor Fishman adds as a footnote to the preceding sentence the following comments:

> In addition, a prosecutor who does not actively supervise the execution of an eavesdropping warrant is abdicating a responsibility Congress clearly intended him to have. Applicants were restricted to "publicly responsible officials subject to the political process" so that "should abuses occur, the lines of responsibility [would] lead to an identifiable person. This provision [18 U.S.C. § 2516] in itself should go a long way toward guaranteeing that no abuses will happen."
>
> When a District Attorney signs an application brought to him by one of his assistants, he and his office are accepting responsibility for the manner in which the warrant is executed and the results obtained from it.

Id. at 52 n.3 (quoting S. REP. NO. 1097, 90th Cong., 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2185).

The influential if not controlling hand of the prosecutor in the conduct of investigations involving electronic surveillance was also noted by Ronald Goldstock, Director of the New York State Organized Crime Task Force. In testimony before the United States Senate Permanent Subcommittee on Investigations, Mr. Goldstock stated:

> The need to merge police and prosecutorial functions became even more acute as investigations and prosecutions became more sophisticated. Legal rules con-

traditional concerns appear misplaced or diminished in the electronics context. Discerning the policy in *Gates* that searches be regulated as closely as feasible, courts should recognize that the greater intrusiveness of electronic eavesdropping, together with the inapplicability of factors traditionally militating towards a moderated probable cause standard, require reconsideration of whether the quantum of evidence justifying an eavesdrop, either *ab initio* or at successive intervals, should be higher than for a conventional search.

VI. CONCLUSION

Cases applying the conventional context probable cause standard to an electronic eavesdrop largely have failed to consider relevant distinctions between these forms of search and seizure. This failure has been masked by invocation of authoritative sources which similarly avoid pertinent analysis. In contrast to those suspects targeted by electronic surveillance who, it is hoped, will "let the cat out of the bag," the courts themselves have withheld the inquiry and analysis necessary to the rigorous development of the fourth amendment issues in this area. Upon undertaking this analysis, the courts might commence with *Katz*, which considered not only the nature of the intrusion, but also the limited applicability of conventional categorical warrant exceptions to an electronic search. The problem of fluctuating probable cause, compounded by the interception of ambiguous data, rather than merely the intrusive nature of the search, calls for analysis of the issue, as troubling as the prospect of a heightened standard might appear. Doubtless, considerations abound, each militating toward distinct resolution of the issue. The courts should acknowledge more fully the unique character of an eavesdrop, apart from its intrusive nature, and re-evaluate probable cause accordingly. At a minimum, this effort would better justify retention of the current standard and would lead to improved clarity by reviewing courts faced with considerations peculiar to the electronic search.

> cerning search and seizure, the right to counsel, electronic surveillance and related issues are now so intricate that police must routinely rely on lawyers to determine what they can and cannot do in any type of complex investigation. Moreover, the Congress and state legislatures have formally given attorneys control over sophisticated investigative techniques used in organized crime, official corruption, and labor racketeering cases. . . . Prosecutors are also given the exclusive responsibility for applying for authorization to conduct electronic surveillance and are required to monitor and control its execution by the police.

Twenty-five Years After Valachi: *Hearings Before the Permanent Subcomm. on Investigations of the Senate Comm. on Government Affairs*, 100th Cong., 2d Sess. 28 (1988) (statement of Ronald Goldstock, Director, N.Y. State Organized Crime Task Force).