Volume 7, Number 2 Spring 1994

ELECTRONIC COMMUNICATIONS AND THE PLAIN VIEW EXCEPTION: MORE "BAD PHYSICS"

*Larry Downes**

INTRODUCTION

A federal investigative team, suspecting insider trading at the branch office of a large brokerage firm, obtains approval to intercept the communications of a particular broker, including phone communications with customers, fax transmissions, electronic mail, and computerized trades. All office communications operate off a private branch exchange (PBX), however, making it impractical to place a wiretap that would single out the suspected broker's communications. Instead, the investigators intercept and record all incoming and outgoing phone traffic of the office.[1]

Phone conversations that do not include the suspected broker are discarded immediately, but electronic communications (e.g., fax, data transfer, and electronic mail) must be processed extensively to determine not only their content but also their very nature. During this analysis investigators come across evidence of narcotics trafficking involving persons in the office who are not the subject of the securities investigation. Can this evidence be disclosed, used, and admitted at a trial

---

* Law Clerk, the Honorable Richard A. Posner, Chief Judge, United States Court of Appeals for the Seventh Circuit. B.A., Northwestern University; J.D., University of Chicago. My thanks to Professor Rochelle Dreyfuss and Mr. David R. Johnson for their suggestions on an earlier draft of this article.

1. Private branch exchanges (PBXs), which are frequently used in medium and large-sized offices, allow companies to purchase trunk lines from local and long-distance carriers and self-manage inter-office traffic using privately-owned equipment located in the office. The PBX routes calls to and from individual extensions. Intercepting the transmissions of only specified extensions would require access to the office, which would often defeat the need for secrecy in the surveillance. Interview with William T. Cook, partner, Willian Brink Olds Hofer Gilson and Lione (Jan. 15, 1992).

In 1992, the Federal Bureau of Investigation, recognizing exactly this problem, proposed amendments to the federal wiretapping law that would enhance their ability to intercept communications from PBXs. Mitch Betts, *FBI seeks right to tap all net services*, 26 COMPUTERWORLD 1, June 8, 1992; *Shades of Indifference*, 1992 THE NATION 469 (Apr. 13, 1992). In the face of opposition from the communications industry and civil liberties groups, however, the Bureau dropped this provision when it renewed its request in 1994. *Joint Hearing of the Technology and Law Subcomm. of the Senate Judiciary Comm. and the Civil and Constitutional Rights Subcomm. of the House Judiciary Comm.*, Federal News Service, Mar. 18, 1994, *available in* LEXIS, NEWS Library, FEDNEW File.

involving the narcotics operation?

While it is unlikely that investigations have yet occurred that are as complex as the one just described,[2] they are by no means the stuff of science fiction. Electronic communications[3] are expanding in both format and volume at a phenomenal pace in many information-intensive industries, and their use in high technology crimes has received considerable publicity.[4] The FBI, recognizing the technical obstacles these technologies pose to wiretapping, proposed legislation in 1992 and again in 1994 to enhance their ability to perform such investigations.[5]

As investigative technologies advance with the changing character of telecommunications, the relationship between electronic communications and the Fourth Amendment, which prohibits unreasonable searches of "persons, houses, papers, and effects,"[6] will need to be reconsidered.

---

2. According to a former Assistant United States Attorney, interception of communications other than conversations are rare and generally have the cooperation of a party who can do both screening and processing, such as a network operator whose facilities are being illegally diverted or invaded. Cook, *supra* note 1. In fact there are no reported cases of wiretaps involving anything but conversations. *See also Joint Hearing of the Technology and Law Subcomm. of the Senate Judiciary Comm. and the Civil and Constitutional Rights Subcomm. of the House Judiciary Comm.*, Federal News Service, Mar. 18, 1994, *available in* LEXIS, NEWS Library, FEDNEW File, at 14 (Sen. Leahy: "[H]ave you had any instances where you've had a court order for a wiretap that couldn't be executed because of digital telephony?" Mr. Freeh: "We've had problems just short of that."); GENERAL ACCOUNTING OFFICE, GAO/IMTEC-92-68BR FBI Wiretapping Challenges (B-249358), ADVANCED COMMUNICATIONS TECHNOLOGIES POSE WIRETAPPING CHALLENGES 2 (1992) ("[S]ince 1986, the FBI has become increasingly aware of the potential loss of wiretapping capability due to the rapid deployment of new technologies, such as cellular and integrated voice and data services.").

3. "[A] 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 . . . ." Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) [hereinafter "ECPA"]. ECPA amended Title III of the Omnibus Safe Streets and Crime Control Act, 18 U.S.C. §§ 2510-2520 (1968).

4. On the use and future of electronic communications, see Peter Coy, Jonathan B. Levine, Neil Gross, and Gail E. Schares, *Super Phones*, BUSINESS WEEK, Oct. 7, 1991, at 138. The rapid changes in the telecommunications industry can be traced partly to the breakup of AT&T and consequent entry of new providers of telecommunications products and services, and partly to the on-going advances in technology like fiber-optics, satellites, PBX, electronic mail, digitized voice mail, low-cost facsimile, and electronic data interchange (EDI). *Id.* On high technology crime, see 34 COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, Mar. 1991 (special issue on electronic publishing, constitutional rights, and hacking).

5. John Markoff, *Wiretap Technology Plan Pushed by F.B.I. Director*, N.Y. TIMES, Feb. 28, 1994, at A1, C3.

6. U.S. CONST., amend. IV. The Fourth Amendment guarantees: "[t]he 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

The Court has already addressed this issue several times,[7] and its evolving electronic seizure jurisprudence mirrors the Court's efforts to resolve a broader Fourth Amendment concern: to what extent does the Fourth Amendment provide protection from government intrusion on personal privacy?[8] For example, is an electronic communication an "effect"? Does interception constitute a seizure? And what if the interception is not of voices but of data, images, or some digital combination of all three? Does recording and analyzing the intercepted material invade some property right?[9]

In the landmark case of *Katz v. United States*,[10] the Supreme Court avoided these metaphysical questions by evaluating the Fourth Amendment in the broader context of personal privacy. Highlighting the awkwardness of the Court's narrower reading, Justice Harlan criticized the *Olmstead* decision as "bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[11]

---

searched, and the persons or things to be seized." The separate requirements of reasonableness, probable cause, approval by an impartial magistrate, and particularity, as well as the difference between a search and a seizure, are treated *infra*.

7. *See* Olmstead v. United States, 277 U.S. 438 (1928); Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1966); United States v. Kahn, 415 U.S. 143 (1974); Scott v. United States, 436 U.S. 128 (1978).

8. This concept has also been called "the right to be let alone," *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting). *Olmstead* was an early case that held wiretapping did not constitute a search and seizure and thus was not governed by the Fourth Amendment.

9. Modern telephone technology, increasingly based not on wire but on fiber optic cable, satellites, and microwave transmission, is characterized by the use of a single channel for transmission of many different kinds of signals simultaneously. *See* Coy, *supra* note 4, at 138.

A related problem, outside the scope of this article, is the evidentiary value of such recordings. Early phone technology was based on analog transmission of voice, a relatively simple concept that did not create significant issues of recording accuracy. *See* JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 7.5 at 66, 67, § 7.5(b) at 72-80 (1986). The modern approach, however, invariably includes converting the communication to a digital signal, which must be decoded by sophisticated software to be "understood" on the receiving end. Image and data are often encrypted, and in any event are never sent in forms that are meaningful without interpretation by additional software—often proprietary to the receiver or the carrier. Introduction of "wiretap" evidence may increasingly require expert witnesses to explain the government's translation processes and technologies.

10. 389 U.S. 347 (1967).

11. *Id.* at 362 (Harlan, J., concurring). *Katz*, along with Berger v. New York, 388 U.S. 41 (1966), decided six months earlier, overruled *Olmstead*. The Court has never felt obliged to articulate the nature of the property interest invaded by a wiretap.

Justice Black stuck to the old view, arguing that the Fourth Amendment could not be applied to anything as amorphous as a conversation. He derided Harlan's conclusion to the contrary: "Such an assertion simply illustrates the propensity of some members of the Court to rely on their limited understanding of modern scientific subjects in order to fit the

Since *Katz*, Fourth Amendment analysis in electronic seizure cases has focused on the defendant's privacy interest and whether it has been unlawfully invaded. The Court has thus not found it necessary to articulate the admissibility of this type of evidence, and the "physics" of electronic evidence has generally not complicated the inquiry. At the edges of criminal procedure, however, the weakness of the uneasy analogy of these seizures to those of tangible objects becomes more apparent. This article addresses one such edge, suggested by the problem posed at the beginning: does the "Plain View" exception, which approves limited seizure of physical evidence not covered by a warrant during otherwise lawful searches, apply to evidence of "other offenses" discovered during electronic surveillance?[12]

This article will argue that comparing the Supreme Court's Title III cases with its most recent Plain View jurisprudence[13] suggests the Plain View exception has minimal application in the context of electronic communications seized under Title III.[14] Lower courts that have tried to apply Plain View in Title III cases go too far, and allow evidence that has been unconstitutionally seized to be introduced in criminal proceedings.[15] These cases have dealt only with recorded telephone communications, but ultimately courts will have to consider the admissibility of electronic

---

Constitution to the times and give its language a meaning that it will not tolerate." *Katz*, 389 U.S. at 372 (Black, J., dissenting).

But there has been little argument since *Katz* that conversations and images intercepted by electronic and other recording equipment and used as evidence in criminal proceedings are appropriate subjects for Fourth Amendment analysis. *See* WAYNE R. LAFAVE & HEROLD H. ISRAEL, CRIMINAL PROCEDURE § 4.2 at 365 (1984).

12. 18 U.S.C. § 2517(5) (1988) authorizes law enforcement officers who intercept evidence concerning "other offenses" to disclose and utilize that evidence as long as it has been seized "by any means authorized" by Title III. Some courts have held this section allows the use of such evidence whenever it meets the requirements of the Plain View exception.

13. *See* Horton v. California, 496 U.S. 128 (1990); Minnesota v. Dickerson, 113 S. Ct. 2130 (1993).

14. Title III of the Omnibus Safe Streets and Crime Control Act, 18 U.S.C. §§ 2510-2520 (1968) [hereinafter "Title III"].

15. Evidence that has been seized in violation of the Fourth Amendment is generally suppressed under the exclusionary rule, *see* LAFAVE & ISRAEL, *supra* note 11, § 3.1 at 132-62. This rule should be applied to much of the evidence currently allowed under the authority of 18 U.S.C. § 2517(5). *See generally* Robert A. Morse, *Propriety, Under 18 U.S.C. § 2517(5), of Interception or Use of Communications Relating to Federal Offenses Which Were Not Specified in Original Wiretap Order*, 103 A.L.R. FED. 422 (1991). *See also* John D. LaDue, Note, *Electronic Surveillance and Conversations in Plain View: Admitting Intercepted Communications Relating to Crimes Not Specified in the Surveillance Order*, 65 NOTRE DAME L. REV. 490, 522 (1990) (summarizing cases and comments regarding the exclusionary rule and § 2517(5)).

communications such as e-mail intercepted en route to increasingly large private networks.[16] The Supreme Court's Plain View cases should apply with even more exclusionary bite to such digital communications.

This piece is organized into four sections. Section I summarizes the development of the Plain View exception from the Court's initial rejection of it in *Marron v. United States*[17] through its rebirth and most recent formulations in *Horton v. California*[18] and *Dickerson v. Minnesota*.[19] Section II traces the parallel development of electronic search and seizure doctrine in the Court before and since the passage of Title III and reviews Supreme Court cases interpreting Title III. Section III provides a framework for applying Plain View to electronic communications intercepted under a Title III wiretap using a basic understanding of the physical properties of these communications to resolve issues left open by the Supreme Court's limited interpretation of the statute. Section IV then applies the proposed tests and criticizes lower courts that have performed the analysis without regard to the unique nature of the technology. The article concludes with a summary of technological changes that have made the weakness of Plain View in searches and seizures of electronic communications more acute and recommends that courts avoid Fourth Amendment violations by giving a very narrow reading to Plain View in the context of Title III.

I. DEVELOPMENT OF THE PLAIN VIEW EXCEPTION

A. The Marron *Court's Reluctance—the Hated General Warrant*

In *Marron*, a prohibition agent searching a "speakeasy" happened upon a ledger book that showed inventories of the liquor and expense receipts of items related to the management of the business, including gifts to police officers. The warrant, however, authorized only the

16. The Internet, a loosely linked public and private network, currently has 20 million addressees and is growing rapidly. A wiretap aimed at communications on this network would be considerably more complicated than the hypothetical of the broker's office. *See* Gary Stix, *Domesticating Cyberspace*, SCIENTIFIC AMERICAN, Aug. 1993, at 100, 101.

17. 275 U.S. 192 (1927).

18. 496 U.S. 128 (1990).

19. 113 S. Ct. 2130 (1993).

seizure of "intoxicating liquors and articles for their manufacture."[20] The Supreme Court addressed two questions: Whether the ledger could be seized under the authority of the warrant, and whether the ledger could be seized as incident to the arrest of the manager.

Regarding the first question, the Court unequivocally rejected the government's contention that the seizure of the ledger did not violate the Fourth Amendment. The Fourth Amendment, the Court said, originated in the colonists' hatred for the general warrant in the form of writs of assistance, which empowered revenue officers of the Crown, "in their discretion, to search suspected places for smuggled goods."[21] To protect against a general search, the Fourth Amendment requires that police obtain particularized warrants based on probable cause which are approved by impartial magistrates. The Court held that here the requirement of particularity had been violated, stating 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. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[22] Even though the ledger was evidence of the same offense for which the warrant was issued, and even though the officer had come across it accidentally and in the course of a lawful search, the Court held that the Fourth Amendment did not permit its seizure.

Still, the Court allowed the evidence to be admitted, agreeing with the prosecution's alternate theory that it was legally seized incident to the defendant's arrest. The officers had made the arrest "for crime being committed in their presence," and therefore "had a right without a warrant contemporaneously to search the place in order to find and seize the things used to carry on the criminal enterprise."[23] Consequently, even though the Court rejected the prosecutor's implicit Plain View argument, the ledger was still lawful evidence.[24]

---

20. *Marron*, 275 U.S. at 193.
21. *Id.* at 195.
22. *Id.* at 196.
23. *Id.* at 199.
24. According to Justice White, the *Marron* Court's strict reading of the particularity requirement created a bizarre rule allowing items that could not be seized when discovered during a warranted search to be seized by an officer who had no warrant at all, as long as his search was incidental to an arrest made during the commission of a crime. An officer acting in this exceptional situation could actually perform a *more* general search than an officer who had satisfied all other Fourth Amendment requirements. *See* Coolidge v. New Hampshire, 403 U.S. 443, 515 (1971) (White, J., dissenting). This was an oddity that the

B. The Coolidge *Plurality's Uneasy Adoption*

In *Coolidge*, a plurality of the Court led by Justice Stewart reconsidered the Plain View doctrine. Since *Marron*, the Court noted, it had approved several exceptional situations where warrantless searches and seizures were allowed, such as when the police "inadvertently come across evidence while in 'hot pursuit' of a fleeing suspect," and where a police officer "is not searching for evidence against the accused, but nonetheless inadvertently comes across an incriminating object."[25]

Under similar circumstances, the plurality felt that the minor peril to the Fourth Amendment presented by the Plain View doctrine was more than offset by a "major gain" in law enforcement.[26] But, since all evidence is literally in "plain view" at the time it is seized, "circumstances in which plain view has legal significance" needed to be defined.[27] The plurality proposed the same tests for Plain View as it required for other Fourth Amendment exceptions: "that the police officer [have] a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence incriminating the accused."[28]

Justice Stewart believed both prior justification and inadvertent discovery were needed to square Plain View with the Fourth Amendment. Prior justification for the intrusion, such as a valid warrant to seize other evidence, satisfied probable cause for the search, and then only when the significance of the evidence was "immediately apparent" to the officer.[29] The second requirement, Stewart argued, was a check that kept the police from avoiding both probable cause and the impartial magistrate requirements by failing to name all the items they intended to seize at the time of an arrest. Without the inadvertence limitation, Plain View would "turn

---

Court would not remedy for over forty years, and even then without finality.

25. *Coolidge*, 403 U.S. at 465-66. The search incident to arrest had also been broadened, relaxing the requirement that the arrest occur during the commission of crime. *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE § 5.2(b) at 440-45 (2d ed. 1987).

26. *Coolidge*, 403 U.S. at 467. The requirements for Plain View exception were not met in *Coolidge* itself. *See id.* at 472. The authority of *Coolidge* was of some doubt, because the Plain View requirements were not met and Justice Stewart's opinion commanded only a plurality. Texas v Brown, 460 U.S. 730, 737 (1983) (plurality opinion) (stating that *Coolidge* while not binding should be the Court's starting point in Plain View cases). The plurality itself noted that "it would be nonsense to pretend that our decision today reduces Fourth Amendment law to complete order and harmony." *Coolidge*, 403 U.S. at 483.

27. *Coolidge*, 403 U.S. at 465.

28. *Id.* at 466.

29. *Id.* ("[T]he 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.").

an initially valid (and therefore limited) search into a 'general' one . . . ."[30]

Both Justices Black and White took exception to the second requirement. Justice Black argued that inadvertence was relevant, if at all, only when the prior justification was a warrant. Where, as in *Coolidge* itself, the search was incident to arrest, it was "independent of any power to search for such items pursuant to a warrant."[31] Justice White, on the other hand, argued that "inadvertence" was never necessary, and instead created confusion. Moreover, given that the Fourth Amendment protects "personal privacy" and "property rights," he did not see why it was even necessary. "Police with a warrant for a rifle may search only places where rifles might be and must terminate the search once the rifle is found; the inadvertence rule will in no way reduce the number of places into which they may lawfully look."[32]

C. *Subsequent development* (Brown, Hicks, Horton, Dickerson)

Since *Coolidge*, the Court has substantially extended the Plain View exception and sharpened its borders. In *Texas v. Brown*, for example, which concerned the warrantless seizure of a balloon in the front seat of the defendant's car, the Court reconsidered the *Coolidge* requirement that, to seize Plain View evidence, its value must be "immediately apparent." The plurality in *Brown* rejected this requirement as an "unhappy choice of words," and proposed instead that Plain View seizures, like any other seizure, be conditioned on probable cause.[33]

The plurality in *Brown* reasoned that the Fourth Amendment protected three interests: the defendant's privacy interest in the items searched, and his property and possessory interests in the items seized. Plain View protected the privacy interest with the requirement of a prior lawful justification for the search and protected the property and possessory interests with the requirement of probable cause for the seizure. No

---

30. *Id.* at 470.

31. *Id.* at 509 (Black, J., dissenting).

32. *Id.* at 514 (White, J., dissenting). Justice White continued to object to "inadvertence" (even in cases in which the question was reserved) until his view was ultimately adopted in *Horton*. *See* Texas v. Brown, 460 U.S. 730, 744 (1983) (White, J., concurring); Arizona v. Hicks, 480 U.S. 321, 329-30 (1987) (White, J., concurring).

33. *Brown*, 460 U.S. at 736-42. Justice Rehnquist, writing for a plurality, noted that, since *Coolidge*, additional warrantless search exceptions had been added, including limited searches of automobiles, border searches, searches with the consent of the defendant, and "stop and frisk" searches. *Id.* at 735-36.

additional Fourth Amendment interest was protected by a requirement that evidentiary value be immediately apparent. Thus, in *Brown*, even though it was not immediately apparent to the officer that the balloon was lined with narcotics, his experience with balloons of that kind gave him probable cause to believe it was. Then, even without a warrant, he could seize the balloon under Plain View since his search, incident to arrest, was justified and the seizure was supported by probable cause.[34]

A majority of the Court endorsed the requirement of probable cause to seize in *Arizona v. Hicks*.[35] Here a police officer, during a warrantless search justified under the "emergency" exception, noticed an expensive turntable in Hicks's apartment. He turned it over to jot down the serial number and determined later that the turntable had been reported stolen.

Writing for the Court, Justice Scalia held that since the officer testified to only a "reasonable suspicion" that the turntable was stolen when he moved it, his further search for the serial number was unreasonable.[36] After a review of the earlier Plain View decisions, Justice Scalia concluded that the exception could withstand Fourth Amendment attacks only if it were held to the same standards as warranted searches. Therefore, he wrote "[w]e now hold that probable cause is required."[37]

The Court in *Horton v. California* reconsidered the requirement that

---

34. *Id.* at 742. All nine justices agreed that the officer, given his prior experience, had probable cause to believe the balloon was the type frequently used to package narcotics. *Id.* at 746 (Powell, J., concurring); *id.* at 750 (Stevens, J., concurring). The Justices disagreed on whether the government needed a warrant for the subsequent search *inside* the balloon.

35. 480 U.S. 321 (1987).

36. *Id.* at 326-28, echoing Justice Stevens's concurrence in *Brown*. The following exchange underlines the importance of probable cause in Plain View search and seizure. The majority argued that "[n]o reason is apparent why an object should routinely be seizable on lesser grounds, during an unrelated search and seizure, than would have been needed to obtain a warrant for that same object if it had been known to be on the premises." *Id.* at 327.

Justice O'Connor disagreed, arguing for a lesser standard of reasonable intrusion: "'the minimal additional intrusion which results from an inspection or examination of an object in plain view is reasonable if the officer was first aware of some facts and circumstances which justify a reasonable suspicion (not probable cause in the traditional sense) that the object is or contains a fruit, instrumentality, or evidence of crime.'" 480 U.S. at 336 (O'Connor, J., dissenting) (citing LAFAVE, *supra* note 25, § 6.7(b) at 717).

The majority responded that "to treat searches more liberally would especially erode the plurality's warning in *Coolidge* that 'the "plain view" doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.'" *Id.* at 328. The explicit adoption of a probable cause standard for Plain View searches and seizures will be highly relevant to the discussion of the exception's applicability to Title III warranted wiretaps.

37. *Id.* at 326-27 ("To say otherwise would be to cut the 'plain view' doctrine loose from its theoretical and practical moorings.").

Plain View evidence be inadvertently discovered, Justice Stewart's second test. In *Horton*, the officer had tried and failed to secure a warrant for weapons used in an armed robbery, but found and seized them anyway during a search for the proceeds of the robbery (rings), for which he had obtained a warrant. Since he suspected the guns might be found, his discovery of them was not inadvertent.[38]

Reviewing the history of Plain View since *Coolidge*, the seven justices of the *Horton* majority rejected outright the inadvertence requirement.[39] The Court reiterated that the Fourth Amendment protects the defendant's privacy and argued that an inadvertence requirement did nothing to protect that interest.[40] Instead, they concluded the protection of privacy was already and more adequately protected by the Fourth Amendment's "particularity" requirement, which required that the officer restrict the scope and manner of his search to items listed on the warrant: "Scrupulous adherence to [particularity] serves the [privacy] interests in limiting the area and duration of the search that the inadvertence requirement inadequately protects. . . . If the scope of the search exceeds that permitted by the terms of a validly issued warrant . . . the subsequent seizure is unconstitutional without more."[41]

In resolving the inadvertence debate, however, the Court in *Horton* reopened a different debate about the meaning of *Coolidge*. *Horton* twice made reference to the fact that the evidentiary value of the guns seized during the officer's search was "immediately apparent,"[42] resurrecting language from *Coolidge* that had been soundly criticized by the plurality in *Brown*. Whether the immediate appearance of the value of the evidence remained a requirement for Plain View, and if so exactly what it added to the analysis was unclear until 1993, when a unanimous Court, including Chief Justice Rehnquist, who had authored *Brown*, held in *Minnesota v. Dickerson* that "immediately apparent" was indeed a requirement with teeth. In *Dickerson*, the officer, during a pat-down

38. Horton v. California, 496 U.S. 128, 131 (1990).

39. *Id.* at 130 ("We conclude that even though inadvertence is a characteristic of most legitimate 'plain view' searches, it is not a necessary condition."). The plurality in *Brown* explicitly reserved the question of inadvertence. *Brown*, 460 U.S. at 743-44.

40. *Horton*, 496 U.S. at 141 ("If the interest in privacy has been invaded, the violation must have occurred before the object came into plain view and there is no need for an inadvertence limitation on seizures to condemn it.").

41. *Id.* at 140. This had been Justice White's view all along. *See Coolidge*, 403 U.S. at 514-20 (White, J., dissenting).

42. *Horton*, 496 U.S. at 136, 142.

search of the defendant pursuant to a *Terry* stop,[43] felt a "small, hard object wrapped in plastic" which he believed to be crack cocaine.[44] But he could not be certain without "squeezing, sliding and otherwise manipulating the contents of the defendant's pocket."[45]

Affirming the Minnesota Supreme Court's decision that "plain view" could extend to situations where the officer feels rather than sees evidence, the Court also agreed with the state court that here the requirements of Plain View had not been satisfied. Relying on both *Hicks* and *Horton*, the Court noted that the "immediately apparent" requirement was the measure of probable cause in Plain View cases. "If . . . the police lack probable cause to believe that an object in plain view is contraband without conducting some further search of the object—i.e. if its 'incriminating character [is not] "immediately apparent"'—the plain view doctrine cannot support its seizure."[46] In order to establish that the police have probable cause to seize an object using Plain View, the evidentiary value of the object must be immediately apparent at the moment the object comes lawfully into view; there can be no "manipulating" or "further search" of any kind.[47]

The holding in *Horton* provides a concise summary of the current requirements for the Plain View exception that will be applied to electronic communications in Section IV. The seizure by the police officer of weapons that were not listed on his warrant was held by the Court to be constitutional because all the elements of Plain View were met: (i) the warrant provided the justification for the initial invasion of privacy, and the officer had not exceeded the scope of his search by looking somewhere other than where a ring might be found; (ii) the officer had probable cause to believe the weapons were used in criminal activity at the time of their seizure, and (iii) their evidentiary value was immediately apparent at the moment weapons were discovered.[48]

---

43. *See* Terry v. Ohio, 392 U.S. 1 (1968).

44. Minnesota v. Dickerson, 113 S. Ct. 2130, 2138 (1993).

45. *Id.*

46. *Id.* at 2137, (citing *Horton*); *see also id.* at 2139 (the turntable's stolen character was not "immediately apparent" in *Hicks*).

47. *Id.* at 2138-39.

48. *Horton*, 496 U.S. at 142 ("[T]he search was authorized by the warrant, [and] the seizure was authorized by the 'plain view' doctrine."). Justice Brennan dissented on the grounds that the inadvertence requirement protected a second and "equally important" Fourth Amendment interest, the defendant's possessory interest in the items seized, which he felt should also require the approval of a magistrate. He noted that "inadvertence" had been adopted by forty-six states and the District of Columbia. *Id.* at 142-49 (Brennan, J., dissenting).

II. JUDICIAL AND STATUTORY CONTROL OF ELECTRONIC SURVEILLANCE: THE FOURTH AMENDMENT AND TITLE III

A. Berger *and* Katz*: The Applicability of the Fourth Amendment*

During the period between the *Marron* Court's rejection of Plain View and its tentative acceptance in *Coolidge*, the Court reconsidered and redefined the law of electronic surveillance. In 1927, *Olmstead v. United States* held that wiretapping was not subject to Fourth Amendment protection, and Congress responded by making wiretapping illegal in 1934.[49] Then in 1967, the *Berger v. New York*[50] and *Katz v. United States*[51] decisions held that the Fourth Amendment did apply to wiretapping, rejecting the *Olmstead* Court's more limited view.

Berger applied the Fourth Amendment to a New York wiretapping statute and struck it down because it did not meet the requirement of particularity. Specifically, it did not condition approval of a wiretap on the ability of the police to "describe with particularity the conversations sought."[52] The *Berger* Court held that without particularity, a wiretap became "a roving commission to 'seize' any and all conversations."[53] The New York statute in effect allowed general warrants, the primary evil the Fourth Amendment was designed to cast out.[54]

The *Berger* Court recognized that electronic "searches and seizures" were different enough from those of tangible property to require special treatment, however, and specified four conditions necessary for a judge to approve a wiretap: (1) particular descriptions of the relevant crime, the information sought, the place where the interception will occur, and

---

Compare the result to *Hicks* where Plain View was not allowed to operate in a non-warrant search. There the officer's *subsequent* search of the turntable was held to be without probable cause. In *Horton* terms, the subsequent search could be considered a further invasion of privacy that was not legally justified. An invasion of privacy was not an issue in *Horton*, since the officer found the guns while looking in places he was likely to find the rings, and the search was justified by the warrant.

49. Olmstead v. United States, 277 U.S. 438 (1928); 47 U.S.C. § 605 (originally enacted as the Federal Communications Act of 1934 § 605).

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

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

52. *Berger*, 388 U.S. at 58.

53. *Id.* at 59.

54. *Id.* at 58 (citing *Marron v. United States*). The New York statute "actually permit[s] general searches by electronic devices." *Id.*

the persons whose conversations are to be seized; (2) a search designed to minimize the interception of parties unconnected to the investigation; (3) limited duration, and a new requirement of probable cause for each extension; and (4) notice to the parties searched unless there is a showing of "exigent circumstances."[55] A wiretap that did not meet these conditions would constitute a general search in violation of the Fourth Amendment.

Katz explained the general principle, implicit in *Berger*, that interception of an electronic communication constituted a "search and seizure." Katz had been convicted of transmitting wagering information by wire, a conviction based on evidence the government obtained by attaching a listening device to the *outside* of a phone booth Katz had used to make his calls. The Court reversed the conviction, holding that the government's evidence had been obtained in violation of the Fourth Amendment.

Writing for the Court, Justice Stewart rejected the argument that Fourth Amendment protection applied only to "tangible property,"[56] and made it clear that the Constitution also protects personal privacy. Since Katz had a "reasonable expectation of privacy" in his phone conversation,[57] the listening and recording "constituted a 'search and seizure' within the meaning of the fourth amendment."[58] Even though the "agents confined their surveillance to the brief periods during which [Katz] used the telephone booth and took great care to overhear only the conversations of [Katz] himself," the Court held that their interception still required a warrant.[59]

Katz established three basic principles of electronic surveillance: (1)

---

55. *Id.* at 58-60; *see also* Omnibus Crime Control and Safe Streets Act of 1968, S. REP. No. 1097, 90th Cong., 2d Sess. 74-75 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2161-62.

56. *Katz*, at 352-53. Noting that this conflicted with the *Olmstead* Court, *Katz* concluded that the "underpinnings" of the earlier case had been "so eroded by our subsequent decisions" that it could no longer be "regarded as controlling." *Id.* at 353.

Justice Black criticized this reading: "In light of . . . the fact that the Court expressly refused to re-examine *Olmstead* . . . I cannot read [the subsequent cases] as overturning the interpretation stated very plainly in *Olmstead* . . . that eavesdropping is not covered by the Fourth Amendment." *Id.* at 371 (Black, J., dissenting). Justice Black likewise criticized *Berger* as an "amorphous holding." *Id.* at 367.

57. Justice Harlan characterized the existence of this interest as a two-part test: "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*, 389 U.S. at 361 (Harlan, J., concurring).

58. *Katz*, 389 U.S. at 353.

59. *Id.* at 354-56. Obtaining one, moreover, would not have interfered with the "legitimate needs of law enforcement." *Id.* at 356 (footnotes omitted).

the Fourth Amendment protects reasonable expectations of privacy and not just "tangible objects"; (2) phone conversations are entitled to such protection; and (3) interception and recording for purposes of criminal investigation constitute a "search and seizure." *Berger* complements *Katz* by describing the specific requirements magistrates must apply in deciding whether or not to authorize such searches and seizures. Together, the two cases played an important role in the shaping of Title III, the first federal wiretapping statute, passed soon after. The drafters of Title III, in fact, made explicit their effort to meet the Court's requirements.

B. Title III

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, according to the joint House and Senate Committee Report that recommended it, "has as its dual purpose (1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."[60] To fulfill these purposes, the bill simultaneously outlawed the use of surveillance technology by private parties, and authorized its use in limited law enforcement situations.[61] In authorizing interceptions, the drafters explicitly adopted the Court's requirements from *Berger* and *Katz*.[62]

Title III's ban on private interception demonstrated Congress's

---

60. S. REP. No. 1097, *supra* note 55, at 66, *reprinted in* 1968 U.S.C.C.A.N. at 2153.

61. "Title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officials engaged in the investigation of specified types of major crimes after obtaining a court order . . . ." *Id.* at 27, *reprinted in* 1968 U.S.C.C.A.N. at 2113.

The Report of the President's Commission on Law Enforcement and Administration of Justice, "The Challenge of Crime in a Free Society" (1967), which was highly influential in the development of Title III, had concluded that the law applicable to both private and police use of electronic surveillance had become "intolerable," since it "serves neither the interests of privacy nor of law enforcement." *Id.* at 67, *reprinted in* 1968 U.S.C.C.A.N. at 2154.

62. *Id.* at 1-2, *reprinted in* 1968 U.S.C.C.A.N. at 2113 ("The proposed legislation conforms to the constitutional standards set out in [*Berger* and *Katz*]."") (citations omitted). *See also id.* at 66, 68-69, 74-75 ("[T]he Court itself has now set down the constitutional standards . . . on the use of these techniques . . . [and] the subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting title III"), 97, 101-105, *reprinted in* 1968 U.S.C.C.A.N. at 2153, 2155-56, 2161-63, 2185, 2190-94; United States v. Cox, 449 F.2d 679, 683 (10th Cir. 1971), *cert. denied*, 406 U.S. 934 (1972).

Berger and *Katz* may have even encouraged the passage of Title III, which had failed to be reported out of the Judiciary committee the year before. *Id.* at 66, *reprinted in* 1968 U.S.C.C.A.N. at 2153.

dissatisfaction with previous efforts at prohibiting electronic surveillance and provided federal protection for the privacy of wire communications. According to the Committee Report, "[t]he tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance."[63]

The limited authorization for use of wiretaps by law enforcement organizations, on the other hand, recognized that electronic surveillance could be a vital weapon in the fight against organized crime, which was particularly effective at using wire communications to obscure illegal activities.[64] Since section 605 of the Federal Communications Act, together with Supreme Court decisions including *Katz* and *Berger*, had "effectively prevented the use in both Federal and State courts of intercepted communications by wiretapping,"[65] statutory authorization was required to bring it back.

Title III created a new federal electronic surveillance scheme aimed at both the privacy and law enforcement goals. Section 2511 generally prohibits all interception and disclosure of wire or oral communications,[66] and section 2512 bans the "manufacture, distribution, sale, possession and advertising" of wiretapping and eavesdropping devices.[67] On the law enforcement side, section 2515 prohibits the use of any evidence obtained through electronic surveillance except as authorized in section 2516.[68] That section, along with sections 2517 and 2518, are Congress's attempt to meet the Fourth Amendment manner and circumstances requirements of *Berger* and *Katz*. These sections define the conditions under which a federal judge may grant an order for electronic surveillance, and specify how evidence obtained under a Title III order may be disclosed and used.[69] In accord with its specific aim of authorizing this extraordinary investigative tool only for "major crimes," section 2516 gives an

63. *Id.* at 67, *reprinted in* 1968 U.S.C.C.A.N. at 2154.

64. *Id.* at 70, *reprinted in* 1968 U.S.C.C.A.N. at 2157 ("The major purpose of Title III is to combat organized crime.").

65. *Id.* at 67-68, *reprinted in* 1968 U.S.C.C.A.N. at 2154-55.

66. 18 U.S.C. § 2511 (1988).

67. *Id.* § 2512.

68. *Id.* § 2515.

69. *Id.* §§ 2516-2518; *see also* S. REP. NO. 1097, *supra* note 55, at 96-107, *reprinted in* 1968 U.S.C.C.A.N. at 2185-96. State wiretapping statutes must likewise conform to the constitutional requirements of *Berger* and *Katz*.

exclusive list of offenses for which surveillance may be authorized, limiting electronic surveillance to illegal activities associated with organized crime.[70]

Section 2517(5), discussed in detail below, authorizes the use of evidence relating to offenses not covered by the Title III court order, so long as such evidence is gained during an otherwise compliant surveillance.[71] This paragraph has been cited by some courts as a codification of the Plain View exception,[72] but the discussion above makes clear that it is incorrect to give this reading to the law. At the time of Title III's passage, the Court had not recognized Plain View as a valid exception to the Fourth Amendment warrant requirement. *Marron*, which rejected Plain View as a violation of the Fourth Amendment, was still the law, and the Committee knew it.[73]

Despite the Committee's frequently expressed intent that Title III provide broad protection for the privacy of wire communications, several committee members criticized it for failing to do so. They also questioned whether the bill as written had succeeded in meeting the requirements of *Berger* and *Katz*.[74] Since Title III permits all the conversations of those being investigated—including conversations with completely innocent persons—to be intercepted, Senator Hart doubted whether Title III satisfied the particularity requirement. In *Katz* terms, to put the problem more generally, interception of the conversations of innocent

---

70. 18 U.S.C. § 2516 (1988).

71. This provides an exception to § 2515, which would otherwise prohibit its use.

72. *See infra* note 104 and accompanying text.

73. *See* S. REP. NO. 1097, *supra* note 55, at 100, *reprinted in* 1968 U.S.C.C.A.N. at 2189.

One commentator has argued that § 2517(5), on its face, is at odds with the particularity requirement of *Berger*, and should be held unconstitutional. Raymond R. Kepner, Comment, *Subsequent Use of Electronic Surveillance Interceptions and the Plain View Doctrine: Fourth Amendment Limitations on the Omnibus Crime Control Act*, 9 U. MICH. J.L. REF. 529, 546-53 (1976).

74. *See* S. REP. NO. 1097, *supra* note 55, at 170, *reprinted in* 1968 U.S.C.C.A.N. at 2231 (comments of Senator Hart). Senator Hart was concerned that Title III failed particularity because "it authorizes all conversations of the person named in the warrant to be intercepted over the entire period of the surveillance, with law enforcement officers authorized to sift through the many varied conversations, innocent and otherwise, that take place during the period." *Id.*

Senator Hart argued that Title III did not meet the standards set by the *Berger* Court and represented "a sweeping intrusion into private and often constitutionally protected conversations of many, and often innocent, persons," amounting to a general warrant. *Id.* at 168, *reprinted in* 1968 U.S.C.C.A.N. at 2229. *See also id.* at 178, *reprinted in* 1968 U.S.C.C.A.N. at 2238 (individual view of Sen. Burdick that Title III "was fraught with grave doubts of constitutionality").

parties would certainly violate "reasonable expectations of privacy."

The Court has never addressed a constitutional challenge to Title III, and the privacy concerns of both detractors and supporters of the bill should be kept in mind in evaluating subsequent judicial relaxation of Title III's manner and circumstances provisions.[75]

C. 1986 Amendments to Title III: "Electronic Communications"

By the 1980's, Title III had become hopelessly outdated by rapid advances in telecommunications technologies and the breakup of AT&T's monopoly as a common carrier. Title III assumed a technical environment that no longer existed, in which phone communications were transmitted as analog signals over copper phone lines operated by a single carrier. By 1986, however, those signals were being separated, repackaged, digitized and repeated, and were being transmitted over complex networks that included microwave, fiber-optic cable, radio, and a new hierarchy of international, national, regional, local, and private carriers.

The structure Congress created was no longer capable of supporting either of its "dual purposes." Title III had banned only the private interception of *wire* communications, and changing communications technology, such as wireless "cellular" phones, made private interception legally possible; the lack of authorization to intercept electronic communications, at the same time, seriously undermined Title III's effectiveness in the fight against organized crime.[76] Congress feared that courts would have trouble determining if anything still constituted a "wire communication," and identifying the rights and obligations of the new specialized players under the statute.[77]

Moreover, these new media were being used not simply to transmit conversations, but also images, data, signals, and frequently combinations of all of them.[78] Since Title III did not cover any of these new configura-

---

75. In United States v. Kahn, 415 U.S. 143 (1974), for example, Title III's requirement of particularity of person was given a broad reading, but the case did not present a constitutional challenge. *Id.* at 150.

76. *See* SENATE COMM. ON THE JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, S. REP. NO. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3355, 3555.

77. *Id.* at 11-14, *reprinted in* 1986 U.S.C.C.A.N. at 3565-68; *see, e.g.* United States v. Torres, 751 F.2d 875, 887-95 (7th Cir. 1984) (Cudahy, J., concurring in the result).

78. S. REP. NO. 541, *supra* note 76, at 2-3, *reprinted in* 1986 U.S.C.C.A.N. at 3555-57. The subsequent development of electronic communications has continued at breakneck

tions, it provided uncertain protection from interception and disclosure by private parties. There was considerable doubt about the legality of interceptions involving the new technologies, because the original statute authorized only interception of wire communications and prohibited evidentiary use of unauthorized interceptions. [79]

Congress responded with a comprehensive amendment, The Electronic Communications Privacy Act of 1986.[80] ECPA expanded Title III's coverage to include the new "electronic communications" technologies. It applies both Title III's prohibition of private interception and limited authorization for law enforcement interception to a broad and expandable range of new communications media and forms.[81] In so doing, ECPA's drafters strongly reaffirmed the primary goal of Title III:

> Most importantly, the law must advance with the technology to ensure the continued vitality of the Fourth Amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.[82]

The committee's reference to the "vitality" of the Fourth Amendment is ironic for two reasons. First, ECPA made no substantive changes to the provisions regulating the *Berger* requirements, notably the requirements of "particularity" and "minimization," which had proven controversial under the original Title III.[83] Second, between the enactment of

---

pace, and confirmed the fears expressed by the drafters of ECPA.

79. *Id.* at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559 ("The lack of clear standards may . . . endanger the admissibility of evidence.").

80. Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

81. 18 U.S.C. § 2510 (1988).

82. S. REP. NO. 541, *supra* note 76, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559. The Committee believed ECPA "represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." *Id.*

Moreover, ECPA greatly enhanced the enumerated list of federal offenses for which a Title III surveillance could be performed, recognizing the increased sophistication of organized crime. 18 U.S.C. § 2516 (1988) (notably adding offenses under the Racketeering Influenced and Corrupt Organizations Act).

83. *See* United States v. Kahn, 415 U.S. 143 (1974) (interpreting 18 U.S.C. § 2518(1)); Scott v. United States, 436 U.S. 128 (1978) (interpreting 18 U.S.C. § 2518(5)). *See infra* Section III for a discussion of *Scott* and *Kahn* and their implications for Plain View under Title III.

Title III in 1968 and ECPA in 1986, the Supreme Court had embraced the Plain View exception. ECPA did not indicate how, if at all, Congress believed this exception applied to new surveillance technologies. Given the potential for "overzealous" use of electronic surveillance by law enforcement agents, this omission was particularly unfortunate.[84]

D. The Supreme Court's Limited Interpretation of Title III

Berger and *Katz*, recall, did not explain how electronic communications—intangible objects—could qualify under the Fourth Amendment's protection of "persons, houses, papers, and effects." Instead, these cases focused on the Fourth Amendment as a protection of personal privacy. Implicit in their analysis is the understanding that it is the defendant's privacy, and not the property seized, that must not be unreasonably invaded. Subsequent cases decided under Title III have demonstrated, however, that this approach leaves important loose ends. For example, in what sense is the interception of electronic communications a search and in what sense a seizure? Is the establishment of the tap the search, and the interception the seizure? Is each communication intercepted a separate seizure? Since Plain View analysis relies on these distinctions, answers to these questions are crucial to the determination of how, if at all, Plain View applies to Title III searches.[85]

The Supreme Court has never answered these questions, but has addressed more limited questions of Title III interpretation that shed light on how the Court might apply Plain View to electronic searches and seizures. In two cases challenging Title III interceptions, the Court rejected efforts to suppress wiretap evidence, suggesting in both that the government could easily meet the "particularity" and "minimization" requirements.

In *United States v. Kahn*,[86] police obtained a Title III order to intercept calls of Kahn "and others as yet unknown" pertaining to a suspected gambling operation. In the course of the wiretap, they

---

84. *See* S. REP. NO. 541, *supra* note 76, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559 ("Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies, and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.").

85. Recall from Section I that Plain View requires a legal justification for the *search*, and probable cause of a connection to criminal activity for the *seizure* of evidence. *See supra* notes 46-48 and accompanying text.

86. 415 U.S. 143 (1974).

intercepted calls made by Kahn's wife that indicated she was also a participant.[87] Mrs. Kahn argued that since the police knew her identity when they obtained the Title III order but did not have probable cause to believe she was involved in the criminal activity, she could not be one of the parties "as yet unknown" referred to in the order. The Court rejected this argument, and held that a Title III order required only probable cause that evidence of the listed *offense* would be found on the tapped line. Identification of the persons committing the offense was optional; it didn't matter if the persons involved were known or unknown when the Title III order was approved.[88]

This interpretation of particularity in the context of electronic surveillance allowed the Court to decide the case without reference to Title III's constitutionality.[89] Moreover, the evidence against Mrs. Kahn related to the gambling offense, and was therefore seized under the warrant. There was no need to determine whether it could have been introduced under a Plain View exception.[90]

A later Title III case held that the government could likewise meet the "minimization" requirement—i.e., that the wiretap be executed in a way that minimized the interception of unrelated communications—with little difficulty. In *Scott v. United States*,[91] the defendants sought suppression of all wiretap evidence because only forty percent of the calls intercepted related to the narcotics activities specified by the order.[92] This low number, along with testimony from the investigator that he considered "minimization" to mean only that he should refrain from recording calls

87. *Id.* at 147.

88. *Id.* at 152-53. Section 2518 requires the order to identify "the person, if known," 18 U.S.C. § 2518(1)(b)(iv) (1988), whose conversations were to be intercepted. The Court held that the warrant's particularity requirement applied only to the offense, and not the persons covered.

Justice Douglas criticized this reading of Title III, arguing that "others unknown" in the order referred to the people to whom Kahn was talking, not people known to the police for whom they did not have probable cause to believe were participants. *Id.* at 160 (Douglas, J., dissenting).

89. *Id.* at 150 ("[W]e are not presented with an attack upon the constitutionality of any part of Title III . . . ."); *see also id.* at 160 (Douglas, J., dissenting).

90. *See id.* at 154 ("[N]either the statute nor the wiretap order in this case would allow the federal agents . . . total unfettered discretion. By its own terms, the wiretap order in this case conferred authority to intercept only communications 'concerning the above-described (gambling) offenses.'") This reading ignores the availability of § 2517(5), which authorizes the use of evidence of other offenses captured during an otherwise compliant Title III search.

91. 436 U.S. 128 (1978).

92. *Id.* at 132.

when he found his tap was on the wrong line,[93] failed to satisfy the Court. Minimization, the Court held, is not evaluated from the subjective state of mind of an investigator. Rather, the requirement is met when all the "circumstances, viewed objectively, justify [the] action."[94] In this case, the execution of the wiretap was satisfactory.[95]

Justice Brennan strongly criticized this reading of minimization, which he believed not only thwarted Congress's express goal of protecting personal privacy but also its effort to write a statute that would satisfy the constitutional requirements of *Berger* and *Katz*.[96] He complained that the Court had failed to read *Scott* in light of *Kahn*, which allowed evidence against Mrs. Kahn partly because, the Court noted, the minimization requirement would act as the backstop against abuse.[97] Reading the two cases together, he argued, suggested a "process of myopic, incremental denigration of Title III's safeguards" that "raises the specter that, as judicially 'enforced,' Title III may be vulnerable to constitutional attack for violation of fourth amendment standards."[98]

III. APPLYING PLAIN VIEW TO TITLE III—WARRANTED SEARCHES AND SEIZURES: A FRAMEWORK

The decisions in *Kahn* and *Scott* demonstrate that the Supreme Court has been willing to give wide latitude to the government in executing wiretaps under Title III. *Kahn* held that probable cause was required only

---

93. *Id.* at 133 n.7.

94. *Id.* at 138.

95. *Scott* was criticized by Goldsmith, *The Supreme Court and Title III: Rewriting The Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 98-111 (1983) as inconsistent with the *Berger* Court's concern that broad interceptions would amount to "general searches by electronic devices," Berger v. New York, 388 U.S. 41, 58-59 (1967). In addition to its "questionable" constitutional validity, he also argues that the "holding directly contravened basic Title III principles." Goldsmith, *supra*, at 108.

96. *See Scott*, 436 U.S. at 143-44 (Brennan, J., dissenting) ("The Court today eviscerates [the] congressionally mandated protection of individual privacy . . . [and] has disregarded or diluted congressionally established safeguards designed to prevent Government electronic surveillance from becoming the abhorred general warrant . . . .").

97. *Id.* at 147 (Brennan, J., dissenting). *See Kahn*, 415 U.S. 143, 154 (1974) ("[I]n accord with the statute the order required the agents to execute the warrant in such a manner as to minimize the interception of innocent conversations.").

98. *Scott*, 436 U.S. at 148 (Brennan, J., dissenting). Like *Kahn*, *Scott* did not present a Fourth Amendment challenge to Title III. *Id.* at 133 n.6. *See also* Goldsmith, *supra* note 95, at 111 ("Together, *Kahn* and *Scott* had made Title III safeguards against indiscriminate electronic surveillance potentially meaningless.").

as to the offenses for the which the order is issued, and *Scott* suggests that the "minimization" requirement imposes little in the way of additional checks on the execution of an authorized wiretap. Consequently, investigators may find themselves encountering evidence that other offenses are being committed by parties not named on the original order. The Court has never been asked to rule on whether such evidence may be used under a Plain View exception to the Fourth Amendment.

Some critics have argued that Plain View is inapplicable in the context of electronic communications, and one commentator has even suggested that section 2517(5), Title III's Plain View analog, is unconstitutional.[99] This article takes a less restrictive position and argues that lower courts that have tried to apply Plain View to electronic surveillance have failed to engage in the analysis required under the Supreme Court's Plain View cases. These cases have dealt only with intercepted conversations, and their weakness will only become more pronounced if they are extended to the inevitable future case where digital communications are involved. As discussed in the next section, applying section 2517(5) as it is currently understood in the federal courts to a wiretap that involves a PBX or other private communications network[100] may well lead to a challenge to Title III that plausibly questions whether it continues to meet the minimum requirements for Fourth Amendment protections outlined in *Berger* and *Katz*.

This section reviews the operative section of Title III, 18 U.S.C. § 2517(5), that has been used by lower courts as a Plain View provision for electronic surveillance, and argues that since this section can at best serve as a placeholder for the Supreme Court's evolving understanding of Plain View, a *Horton*-like analysis must be applied to challenged evidence

---

99. *See* Comment, *Subsequent Use of Electronic Surveillance Interceptions and the Plain View Doctrine: Fourth Amendment Limitations on the Omnibus Crime Control Act*, 9 U. MICH. J.L. REF. 529, 546-53 (1976); *see also* GOLDSMITH, *supra* note 95, at 141-50 (analyzing Plain View at the *Coolidge* stage of development); CARR, *supra* note 9, at § 5.9(b), at 5-63 to 5-65 (recommending that courts avoid constitutional problems by excluding all "windfall" evidence); *cf.* CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING at §§ 161-164, at 240-45 (1978).

100. PBXs are by no means the only example of a privately-operated communications server that collects and distributes both analog and digital communications for a large group of people. The ballooning number of Internet host processors storing and forwarding over a million electronic mail messages each day fits this description as well. Torsten Busse, *E-Mail Evolves into Integral Network Tool*, COMMUNICATION WEEK (Jan. 3, 1994), p.78. For that matter, a photocopy center that sends and receives faxes for its customers, or a secretarial service providing office support to a group of small businesses, would also meet this description.

offered under its authority. To highlight the limitations of these decisions, the unique nature and associated problems of digital communications are briefly described. An alternative approach to Plain View analysis is also considered and rejected.

A. Plain View and Section 2517(5)[101]

No court has literally applied Plain View to a Title III order. But some courts, faced with Fourth Amendment challenges to evidence gathered during Title III searches, have read section 2517(5) as a statutory analog for Plain View.[102] Section 2517(5) does bear superficial resemblance to the Plain View exception. It provides that evidence "relating to offenses other than those specified in the order of authorization or approval" may be used if a judge, on subsequent application, finds "that the contents were otherwise intercepted in accordance with the provisions of this chapter."[103] Despite the suggestion of at least one court, however, section 2517(5) can not *literally* codify the Plain View exception.[104] Section 2517(5) was written in 1967, when *Marron*, which had flatly rejected Plain View, was still good law. It was not until 1971 that the Supreme Court recognized Plain View, and a majority of the Court did not accept it until 1983.[105] If section 2517(5) limits the

---

101. 18 U.S.C. § 2517(5) specifies:

> When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval . . . .[s]uch contents and any evidence derived therefrom may be used [as evidence in any proceeding] when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

102. *See, e.g.*, United States v. Johnson, 539 F.2d 181 (D.C. Cir. 1976); United States v. Williams, 737 F.2d 594 (7th. Cir 1984); United States v. Sklaroff, 323 F.Supp. 296 (S.D. Fla. 1971).

103. 18 U.S.C. § 2517(5) (1988). Recall that Title III's "provisions" were drawn to conform with *Berger* and *Katz*. *See* S. REP. No. 1097, *supra* note 56, at 99-102, *reprinted in* 1968 U.S.C.C.A.N. at 2189-90.

104. *See* United States v. Masciarelli, 558 F.2d 1064, 1066-67 (2d Cir. 1977); People v. DiStefano, 382 N.Y.S.2d 5, 9 (1976) (noting that a New York statute identical to Title III "obviously intended to engraft the 'plain view' exception"); *see also* United States v. DePalma, 461 F. Supp. 300, 825 n.32 (S.D.N.Y. 1978) (noting that section 2517(5) has its "constitutional underpinnings in the 'plain view' doctrine").

105. Illinois v. Andreas, 463 U.S. 765 (1983). Note that *Horton*, decided in 1990, was the first majority opinion to deal with Plain View as an exception applicable to a search being performed under a warrant. *See also* Goldsmith, *supra* note 95, at 141.

admissibility of evidence to Fourth Amendment law as of 1968, when the Court adhered to a strict view of particularity, very little evidence could be admitted under its authority.[106]

The legislative history of section 2517(5) reinforces a narrow reading. The committee report's only commentary on this section is a citation "comparing" it to three cases, one of which is *Marron*. Like *Marron*, the other two cases allowed evidence of other offenses to be admitted based on exceptions other than Plain View.[107] Additionally, the *Katz* Court, to whom the drafters of Title III paid close attention, noted that "it is difficult to imagine how any [Fourth Amendment exception] could ever apply to the sort of search and seizure involved in [electronic surveillance]."[108]

From this discussion, it seems clear that Congress did not intend section 2517(5) to operate as a Plain View exception for Title III. But how should a court evaluate an argument that 2517(5) can be used as a Plain View exception anyway? The Supreme Court's broad interpretation of Title III in *Kahn* and *Scott* implies that the Court would likely follow lower courts in reading section 2517(5) as a Plain View analog. But the Court's uneasiness with Plain View—reflected most recently in the carefully circumscribed exceptions permitted in *Horton* and *Dickerson*—suggests that Plain View represents a *minimum* standard for Fourth Amendment challenges. Thus, section 2517(5) cannot operate unless, at

---

106. So limited, for example, § 2517(5) might apply only to evidence of other offenses when that evidence was part of intercepted communications that also contained evidence of the listed offenses.

107. S. REP. No. 1097, *supra* note 56, at 100, *reprinted in* 1968 U.S.C.C.A.N. at 2189. The three cases cited are Marron v. United States, 275 U.S. 192, 199 (1927) (allowing search when crime committed in the presence of police), United States v. Eisner, 297 F.2d 595, 597 (6th Cir. 1962) (relying on *Marron*), and State v. Hunter, 292 N.W. 609, 611 (Wis. 1940) ("the search was not unreasonable").

No senator commented specifically on this section, and it has not been substantially modified since 1968.

108. The Court's list included the exceptions relied on in the three cited cases. Katz v. United States, 389 U.S. 347, 357-58 (1967). Since *Coolidge* had not yet been decided, Plain View was not one of the exceptions noted. *Cf.* Goldsmith, *supra* note 96, at 141-42. For example, the Court did not see how electronic surveillance before or after arrest could ever be seen as "incidental" to the arrest.

This piece will not argue, as one commentator has, that the *Katz* Court's reasons for rejecting the application of other Fourth Amendment exceptions to electronic surveillance applies equally to Plain View. This argument focused on the inherently intrusive nature of wiretapping compared to search and seizure of tangible objects, and concluded that given Congress's strong words of warning in both Title III and ECPA, Plain View should be severely limited for policy reasons in the setting of electronic communications. *See* Kepner, *supra* note 73, at 553.

a minimum, the requirements of Plain View are met.[109]

At most, section 2517(5) may serve as placeholder for the evolving Plain View exception. Therefore, in evaluating the limits of Plain View to electronic searches and seizures under Title III, courts should begin by ensuring at a minimum that evidence introduced under the authority of section 2517(5) meets current Plain View requirements. As discussed in Section I, the Court's restatement of the exception in *Horton* imposes three tests:

(i) There must be a prior and limited justification for the invasion of privacy that brought the evidence into plain view;

(ii) At the time of seizure, the officer must have probable cause to believe the Plain View evidence is related to criminal activity; and

(iii) The evidentiary value of the evidence seized must be immediately apparent without any further search.

B. Search and Seizure of Digital Communications

Since Plain View analysis applies separate tests to the search and to the seizure that bring evidence into plain view, these two components must be separated before applying the tests to electronic communications.[110] The answer to this problem of "physics" is not obvious. Where a physical search involves discrete objects in discrete places, a wiretap intercepts electronic signals. When these signals are analog, courts have traditionally thought of the recording of the call as the "seizure" and the review of the call (either contemporaneously or after recording) as the

---

109. Even if Congress intended section 2517(5) to go beyond the Court's view of the Plain View exception, such an effort would not pass Fourth Amendment muster. In 1992, for example, all nine Justices signed an opinion citing *Horton* as an expression of the minimum standard for admissibility of evidence. *See* Soldal v. Cook County, 113 S. Ct. 538, 545-46 (1992) ("[F]ar from being automatically upheld, 'plain view' seizures have been scrupulously subjected to Fourth Amendment inquiry.").

110. Recall that the Court in *Katz* characterized interception of an electronic communication simply as a "search and seizure." *Katz*, 389 U.S. at 351. Since *Katz* decided the question on the basis of the newly-created privacy interest, it was not necessary for the Court to explain how the interception of an intangible object could constitute a search and seizure, and no court since has tried to identify the features of a wiretap that equate to the two components.

"search."[111] Because the seizure actually precedes the search, the minimization requirement was introduced to ensure that privacy interests are adequately protected. Under minimization, the officer must stop listening when it becomes clear a given intercepted call does not relate to the offenses listed on the Title III order.

This creative application of physical properties to the world of the intangible, however, breaks down when applied to digital communications, where there is no equivalent to listening only to the beginning of a communication and thus no effective technique for minimization. To understand why this is so requires a basic understanding of electronic communications and their transmission.

Recall the situation described at the beginning of this article. Based on probable cause to believe that insider trading is taking place in a brokerage office, impartial magistrate issues a Title III order specifying the offenses for which the police may lawfully intercept and evaluate communications. The relevant communications may include phone calls, faxes, e-an mail, and data exchanges. All traffic for the office is managed by a PBX. Thus, in order to maintain secrecy, the wiretap must be placed at a point in the network prior to the PBX equipment in the broker's office. The least intrusive point would be on the trunk line, the last link in the communications network managed by a disinterested party, i.e. the local phone carrier. Tapping the trunk line captures all communications, analog and digital, transmitted to and from the office under investigation.[112]

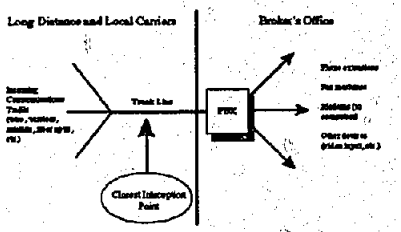

Figure 1

111. CARR, *supra* note 9, § 5.7(a), at 5-27 to 5-30; FISHMAN, *supra* note 99, § 7, at 11.

112. Figure 1 suggests a basic flaw in the F.B.I.'s 1992 proposed amendments to Title III. Direct access to the PBX would only allow investigators to identify communications directed to the phone extension of a suspect, but most electronic communications (e.g., fax, electronic mail, and computer data transmissions) are directed to interpreting devices, not the ultimate recipient of the message. See Figure 2. Most commentators in a recent debate on these amendments missed this point.. *To Tap or Not to Tap*, 36 COMM. OF THE ACM (March 1993) (quoting Ronald L. Rivest). In any event, the F.B.I. abandoned its efforts to gain undisclosed access to PBXs in its 1994 proposal. *See infra* note 151 and accompanying text.

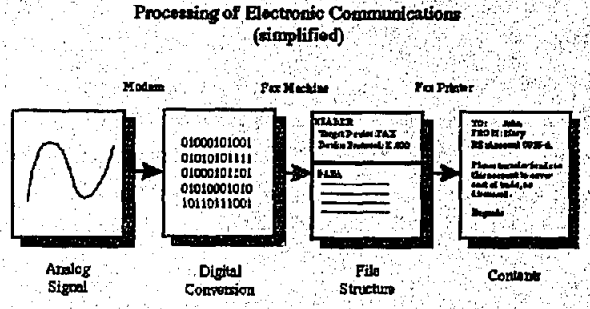

Figure 2

The scope of the interception is determined, as the Supreme Court has made clear, by the listed offenses—that is, the investigators are authorized to intercept all communications that relate to the insider trading.[113] Ideally, the investigators would only intercept these communications. For digital communications, however, it is impossible to determine the nature of the communication using the traditional minimization technique, because several layers of hardware and software must be applied to convert the intercepted signal, first to its digital format, then to a recognizable communications protocol, and finally to a format understandable to human beings.[114] The sender, receiver, and subject of a message are unknown until the last step. It is impossible to discard a digital communication that is unrelated to the subject offenses until after all of its contents are revealed to the investigators.

---

113. *Kahn v. United States*, 415 U.S. 143 (1974). Insider trading is not one of the subject offenses specified under Title III, 18 U.S.C. § 2516 (1988) (amended 1990), but insider trades could constitute predicate acts under RICO, and RICO is one of the subject offenses for which Title III orders may be authorized. *See, e.g.*, United States v. Carson, 969 F.2d 1480 (3d Cir. 1992).

114. Figure 2 is a greatly simplified model of how an incoming signal is ultimately printed by a fax machine. For details on electronic communications, see ANDREW S. TANNENBAUM, COMPUTER NETWORKS 546-58 (2d ed. 1988). Note that at the second step, the communication is understood by software in the fax machine to be in an industry standard communications format, generally the IEEE's X.400 protocol. At this point, however, the data component, which could tell the investigators, for example, to whom the message is directed, is not yet converted. X.400 or similar protocols are used for other types of electronic communications, such as data exchanges, electronic mail, and voice mail. *See* BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE, ch. 1 (1991); *See generally* TANNENBAUM, *supra*, ch. 1,9; Busse, *supra* note 100, at 78.

C. The Minimization Alternative

The difficulties of applying real-world concepts like search and seizure to electronic signals suggests an alternative approach to Plain View analysis under Title III that should be considered. This approach rejects the notion that traditional search and seizure characteristics can be applied to electronic communications at all, and proposes instead an approach to Plain View analysis tailored to the specific features of communications technology.[115]

The unique nature of electronic communications was understood by the drafters of Title III, who tried to prevent possible Fourth Amendment abuses, as *Berger* required, with the general requirement of minimization. This provision requires that investigators design their search to minimize interception of communications not covered by the order.[116] If this requirement is satisfied, the search as a whole adequately protects the privacy interests of everyone whose conversations were intercepted, and there is no need to independently satisfy the Plain View tests.

Arguably, minimization provides a Fourth Amendment check on Title III in the traditional environment of analog communications and interception by the local phone company of calls to a single phone extension.[117] But assuming for the moment that the Supreme Court would accept a minimization test as an alternative to the narrowly defined Plain View exception, the minimization approach cannot operate in the environment described in Figure 1. Minimization as it has been understood up until now can have no meaning in the increasingly digital world, where short of full translation of the message, an investigator has no meaningful basis to decide whether to continue processing.

In enacting the ECPA amendments to Title III, Congress appears to have understood that limiting scope was a difficult problem when intercepting digital communications. If minimization was to continue serving as the constitutional control on particularity, according to the Committee report, a modified minimization procedure would be required for digital messages. As the Committee properly noted, "It is impossible to 'listen' to a computer and determine when to stop listening and minimize as it is possible do so in listening to a phone conversation."

---

115. FISHMAN, *supra* note 99, § 6, at 6-6 to 6-7.

116. 18 U.S.C. § 2518(5) (1988).

117. But see criticism of minimization in the traditional environment in CARR, *supra* note 9, § 2.5(c)(1)(C), at 24.1-27; FISHMAN, *supra* note 99, § 151, at 203-10.

Thus, they concluded:

> [M]inimization for computer transmissions would require a somewhat different procedure . . . . Common sense would dictate . . . the minimization should be conducted by the initial law enforcement officials who review [the translated communication]. Those officials would delete all non-relevant material and disseminate to other officials only that information which is relevant to the investigation.[118]

This solution may satisfy "common sense," but it nonetheless suffers from two fatal problems. The first, of course, is section 2517(5). The suggestion that investigators will "delete all non-relevant material" ignores the availability of a provision in Title III to disseminate "non-relevant" material when it contains evidence of criminal activity not covered by the Title III order. Congress, like the Supreme Court in *Kahn*, proposed a solution that completely failed to address the tension between the minimization requirement and the Plain View exception. The Committee implies that it is fine for investigators to see translated digital messages because they will ignore anything not relevant, but can, under section 2517(5), take advantage of anything of evidentiary value. In effect, this modified minimization solution allows Title III to serve as a general warrant.

The second problem with the modified minimization solution is that the courts would be unlikely to apply it. The Supreme Court in *Scott* made it clear that minimization was to be evaluated based on an objective reasonableness standard, looking at the conduct of the wiretap as a whole and not the decisions made by investigators as to individual interceptions. The minimization test, according to *Scott*, is whether all the "circumstances, viewed objectively, justify [the] action."[119] The Court held that if the wiretap is conducted in a reasonable manner overall, then the entire search satisfies minimization even if some communications are seized outside the scope of the order.[120]

---

118. S. REP. No. 541, 99th Cong., 2d Sess. 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585.

119. *Scott*, 436 U.S. at 140.

120. The *Scott* Court held the evidence could be admitted because, under all the circumstances, the seizure of calls unrelated to criminal activity of any kind (which accounted for sixty percent of the intercepted calls) seemed reasonable. *See* 436 U.S. at 140-41.

Scott only dealt with conversations, and the challenge in that case was not to evidence of other offenses but of the actual offenses listed in the order. But since the clear holding is that interception of unrelated communications will not in itself dictate a finding of inadequate minimization, the Senate's "common sense" approach does not appear, absent clearer congressional direction to the contrary, a viable method for controlling what communications must be suppressed when offered under the forgotten section 2517(5). Lower courts, obediently following the *Scott* Court's direction, have not focused on details such as whether the investigator deleted non-relevant material.[121]

Moreover, since *Kahn* rejected the argument that Title III afforded any protection to persons not specifically named in the order, there would appear to be no remaining safeguard available to keep evidence of unrelated offenses by persons not named in the order from being disclosed and admitted at trial. The minimization solution proposed by the Senate, in other words, would not only lead to an expansion of Title III sharply at odds with the intention of its drafters, it would also fail to satisfy the Fourth Amendment requirements for electronic interceptions required under *Berger* and *Katz*.[122]

Since *Scott*, courts generally evaluate minimization by comparing the total number of calls intercepted to the number that did not meet the description of the order. All the cases to date involve interceptions of conversations, however, and it is unclear how other forms of electronic communication will be counted and weighed in this analysis. *See, e.g.*, United States v. Infelise, No. 90 CR 87, 1991 WL 255628, at *15 (N.D. Ill. Oct. 18, 1991) (thirteen percent unrelated conversations "does not come close to showing 'flagrant disregard' of the duty to minimize"); United States v. Moody, 762 F. Supp. 1491, 1497-98 (N.D. Ga. 1991) (evaluating minimization based on how long a conversation was listened to before making the determination of its relevancy).

121. *See, e.g.*, United States v. Homik, 964 F.2d 899, 903 (9th Cir. 1992) (following orders to listen to each conversation for only two minutes satisfies minimization); United States v. Sanchez, 961 F.2d 1169, 1178-79 (5th Cir. 1992) (use of drug "code terminology" excuses interception of innocent calls); United States v. David, 940 F.2d 772, 730 (1st Cir. 1991) (unavailability of on-the-spot Hebrew translators justified "after-the-fact minimization"); United States v. Uribe, 890 F.2d 554, 557-58 (1st Cir. 1989); United States v. Willis, 890 F.2d 1094, 1101-02 (10th Cir. 1989) (evaluating minimization by percentage of intercepted calls that were "minimized").

122. Read in this way, § 2517(5) would allow invasions of privacy that cannot be reconciled with the Court's development of either Plain View or electronic surveillance. This would be especially ironic given the insistence by the *Berger* and *Katz* Courts and the drafters of Title III that electronic surveillance ought to be held to *higher* standards of privacy protection than traditional searches.

This may have been precisely the situation Justice Brennan had in mind in his warning that *Scott* and *Kahn* taken together may have made Title III "vulnerable to constitutional attack for violation of Fourth Amendment standards . . . ." *Scott*, 436 U.S. at 148 (Brennan, J., dissenting); *see also* United States v. Kahn, 415 U.S. 143, 150, 154 (1974) (relying, pre-*Scott*, on minimization to protect the search from becoming general).

Given the technical realities involved in transmitting and translating digital communications, section 2517(5), perhaps inadvertently, creates a potentially explosive opportunity for investigators to obtain evidence of other offenses of unsuspected persons during the course of an otherwise lawful Title III order, particularly when that order relates to digital communications intercepted on their way to private communications networks. Minimization, the normal Title III control over such evidence, cannot satisfy Fourth Amendment requirements in these increasingly common environments. If courts are to apply any meaningful test in evaluating admissibility of this evidence, then the Plain View exception would appear to be the last remaining check consistent with the Court's early decisions on wiretapping and the Fourth Amendment. The next section will describe how these tests should be applied to electronic communications offered under section 2517(5).

IV. ELECTRONIC COMMUNICATIONS AND PLAIN VIEW: APPLYING THE TESTS

Since the scope of a Title III order covers only communications that relate to the offenses listed on the order, all other communications must pass the tests for Plain View of the *Horton* Court. Applying these tests, Plain View should rarely operate under Title III, particularly when the challenged evidence originates from digital communications. This section describes how the Supreme Court would be likely to evaluate the hypothetical interception at the broker's office described in Section III, and notes where lower courts that have reached different conclusions have gone astray.

A. Prior and Limited Justification for Invasion of Privacy

Plain View will not apply unless police have a legal justification (such as a warrant) for being in the place where they observe the evidence offered under the exception. The justification, however, is not a blank check to search. Police must limit their searches to prevent further invasions of the defendant's right to privacy. They must not search, in other words, in places that are unlikely to yield the items for which they have a right to look. If they do, the search is no longer legally justified, and evidence that is in plain view as a result will be suppressed.

When searching under a warrant the police must look only in places

likely to yield the items listed;[123] when searching under one of the warrantless exceptions, they cannot further invade the defendant's privacy by looking somewhere other than places justified by the nature of the exception.[124] The application of this test is not difficult in the traditional Plain View cases. Warrants must list tangible items for which the police may search, and the courts can easily determine whether police searched for them in appropriate places. If, for example, the police had a warrant to search for a car, it would be unreasonable to look for it in a dresser drawer. Any evidence found in the drawer would be inadmissible because the search was not legally justified.[125]

Under a Title III order, however, the scope of the search is defined with reference to the line (the phone number) on which the suspected communications are being transmitted and the subject offenses that the police have cause to believe are the subjects of these communications. Since this order is a form of warrant, one way to conceptualize the scope of the order in the example of the brokerage firm is by analogy to *Horton*. Recall that the police were authorized to search Horton's apartment for rings. Similarly, the Title III order may be thought to give authorization to search on the trunk line (an address, like Horton's address) for communications related to insider trading. The police may go into Horton's apartment and look in places (including closed containers) where stolen rings might reasonably be hidden; the investigators of the brokerage firm may likewise tap into the trunk line and look in communications that relate to the offenses.

This is not an entirely satisfactory analogy, however, because the trunk line, unlike Horton's street address, is a place where many people store their private communications. Additionally, it is impossible for the insider trading investigators to know (or even guess) which communications coming over the line relate to the listed offenses. Physical containers have properties such as size and shape that may be observed without opening them—so the police in *Horton* knew they could not look for the stolen rings, for example, by testing a piece of paper for a certain watermark. Digital communications do have identifying information

123. *See* Horton v. California, 496 U.S. 128, 141-42 (1990).

124. For example, once lawfully in a room under the emergency exception to search for the gun that wounded a downstairs neighbor, the officer needed—and failed to get—a separate justification for the further invasion of defendant's privacy of looking under a suspicious turntable for its serial number. Arizona v. Hicks, 480 U.S. 321, 324-25 (1987).

125. LAFAVE, *supra* note 25, § 4.9(c), at 295.

(sender, receiver, subject) that operate similarly to these physical properties, but these can only be determined by extensive processing of the communication. This processing impinges upon the privacy interests of the parties because it also exposes the content of the message.[126]

For purposes of this first test, however, there is little problem. If an electronic communication is offered under section 2517(5) as containing evidence of other offenses, the legal justification for bringing it into plain view is the Title III order itself, which authorized the police to search the trunk line for certain communications. Since communications are indistinguishable through the third step of processing shown on Figure 2, it cannot be said that the investigators exceeded their authority in looking at any communication at least to this point of processing. The difficult problem, which may be deferred to the second test, is the next step in processing, which performs the final translation. Clearly the order allows the police to intercept communications that are not covered by the terms of the order, but how much processing may be performed on such interceptions consistent with the order?[127]

B. Probable Cause to Seize

An item that is legally in Plain View but which is not covered by a warrant cannot be seized unless the officer has probable cause to believe the item is connected with criminal activity. In this sense, Plain View relaxes only trivially the Fourth Amendment's requirements. The exception allows an officer to seize without a warrant only where it is clear a subsequent application for a warrant would be a mere formality.[128]

---

126. CARR, *supra* note 9, § 2.5(c)(1)(C), at 24-27.

127. The strong language concerning scope in *Horton*, 496 U.S. at 140, suggests that only a limited amount of processing may take place. Also illuminating are cases involving closed containers in the traditional setting. *See e.g.*, United States v. Corral, 970 F.2d 719, 725 (10th Cir. 1992) ("[T]he plain view doctrine may support the warrantless seizure of a container . . . but any subsequent search of the concealed contents . . . must be accompanied by a warrant or justified by one of the exceptions."); United States v. Sylvester, 848 F.2d 520, 525 (5th Cir. 1988) ("[A] container cannot be opened unless its contents are in plain view or they can be inferred from the container's outward appearance."); United States v Johns, 707 F.2d 1093, 1095-96 (9th Cir. 1983) (opaque container that is properly seized may not be searched without a warrant).

128. In his concurrence in *Brown*, Justice Stevens argued that Plain View seizures require "strict attention" to two of the "core" requirements of the exception: "seizing the item must entail no significant additional invasion of privacy, and *at the time of the seizure* the officer must have probable cause to connect the item with criminal behavior." *Brown*, 460 U.S. 430, 748-49 (1983) (Stevens, J., concurring) (emphasis added). Otherwise, the police could seize everything in plain view when searching under a warrant and then determine later what

In *Horton*, for example, the Court noted that since the warrant did not list any guns, the officer could not seize all the guns he came across during his search. The officer could only seize the guns that he had probable cause to believe were used in criminal activity.[129]

The *Hicks* Court further broadened this theory, suggesting that probable cause to seize Plain View evidence might overcome a failure of the first test. Probable cause, in other words, might also serve *as* the justification for a search that goes beyond its initial legal scope:

> It is clear, therefore, that [an otherwise unjustified search for the serial number of the turntable would have been] valid if the "plain view" doctrine would have sustained a seizure of the equipment. There is no doubt that it would have done so if [the officer] had probable cause to believe that the equipment was stolen.[130]

Probable cause to seize, then, may be sufficient to satisfy Plain View even when the search goes beyond the justification that brought the item into plain view in the first place.

1. The Probable Cause Unit

Satisfying either version of this test with electronic communications is unlikely. Under the *Horton* standard, an officer may only seize an item that is either described by the warrant or that he has probable cause to believe is related to criminal activity. The Title III order itself will cover communications relating to the listed offenses, but what about the communications from a potentially large group of senders and receivers

---

items were of evidentiary value.

129. *Horton*, 496 U.S. at 131 (citing *Hicks*). The officer's original attempt to obtain a warrant for the challenged guns had failed, but having lawfully seen them in his search for the rings, there is no doubt the court would have found on a second application that he now did have probable cause to search for them in Horton's home. Plain View merely allowed him to skip this process in the interests of effective law enforcement. In fact during his search for the rings the officer located weapons other than those he believed were used in the robbery but did not seize these because "there was no probable cause to believe they were associated with criminal activity." *Id.* at 131 n.1.

130. *Hicks*, 480 U.S. at 326 (dicta). The officer in *Hicks* did not have probable cause to believe the turntable was stolen, and therefore his search for a serial number while lawfully in Hicks's apartment to search for a gun was an unjustified invasion of privacy. The Court is suggesting, though, that once the turntable lawfully came into Plain View, the officer could have searched for the serial number if he had probable cause to believe it was stolen (and therefore seizable).

that may be intercepted in the process? Which of these will the investigator have probable cause to associate with unrelated criminal activity at the time of their seizure?

One view is that the mere fact that these communications were being sent over a line that was the subject of the wiretap constitutes sufficient probable cause to seize and use them. Thus, there is no problem with the final stage of processing, because even though this constitutes a search and seizure, there was probable cause for it. While such an approach has a forensic appeal in its simplicity—and indeed has been adopted by several courts evaluating challenged section 2517(5) evidence—it is simply wrong.

The most obvious reason to reject such a broad view of "probable cause" is that it proves too much; it rewrites Title III (as does the minimization solution suggested by Congress noted above) in such a way at to create direct conflict with the narrow authorization of wiretapping detailed in *Berger* and *Katz*. As noted earlier, the uses of electronic communications are expanding, and there are a growing number of environments where effective methods of government surveillance potentially infringe upon the privacy interests of many innocent parties. If simply working in the suspected brokerage office, using a copy center where some unlawful activities are being communicated on a shared fax machine, or having an account on the Internet (where some illegal activity must already be going on) gives the government probable cause to seize one's electronic communications and use any evidence of wrongdoing revealed in them, it will be a very short time until no one in the electronic realm known as "cyberspace" is protected by the Fourth Amendment. There will be little point to listing the subject offenses in a Title III order. The Title III order, like the New York statute rejected by the Court in *Berger*, will lack particularity and "actually permit general searches by electronic devices."[131] Given that the Supreme Court has subjected electronic surveillance to a higher degree of scrutiny because of its "severely intrusive and indiscriminately acquisitive nature," it seems unlikely that such a wholesale rejection of the privacy interests protected by the exclusionary rule would or could be adopted.[132]

Additionally, applying the probable cause test to the entire line is

131. Berger v. New York, 388 U.S. 41, 58 (1967).

132. CARR, *supra* note 9, § 2.5(a), at 20-21; *see also* United States v. Torres, 751 F.2d 875, 884-85 (7th Cir. 1984).

inconsistent with the language of Title III itself and the Supreme Court's interpretation of this language. Recall that the scope of electronic surveillance under Title III is defined by those offenses for which the wiretap is authorized. Section 2518(1), which describes the requirements for obtaining a Title III order, requires the applicant to give "details as to the *particular offense* that has been, is being, or is about to be committed."[133] Section 2517(5) itself applies on its face to communications "relating to *offenses other than those specified in the order* of authorization or approval."[134]

Emphasizing the limiting factor of forcing the police to specify not places and things but the offenses themselves, the Supreme Court in *Kahn* held that the Fourth Amendment "particularity" requirement applied to the offenses, not the people, listed in the order.[135] If the police had probable cause to seize all communications on the line by virtue of their proximity to communications relating to the specified offenses there would arguably be no need for the additional authorization of section 2517(5) in the first place.

Lower courts facing challenges to the admissibility of "other offenses" evidence under section 2517(5) have consistently made this improper interpretation, and their efforts at rationalizing their holdings with Plain View highlights the error of testing "probable cause" with reference to the line on which the tap is placed. *United States v. Cox*,[136] an early Title III case, began by noting that the application of Plain View (then only in its *Coolidge* stage of development) to Title III was a poor analogical fit because "the quest for property is a different and less traumatic invasion than is the quest for private conversations."[137] Nevertheless, the court in *Cox* felt it would be "irrational" not to let police make use of unrelated

---

133. 18 U.S.C. § 2518(1)(b)(i) (1988) (emphasis added). Compare this to the requirement to identify the offenders themselves, which is merely to state "the identity of the person, if known, committing the offense . . . ." 18 U.S.C. § 2518(1)(b)(iv) (1988); *see also* § 18 U.S.C. 2518(4)(c) (the order "shall specify . . . a particular description of the type of communication sought to be intercepted, and a statement of the particular offenses to which it relates").

134. 18 U.S.C. § 2517(5) (1988) (emphasis added).

135. Since the conversations of Mrs. Kahn did relate to the gambling offense for which the order was issued, there was no need for the Court to go on to decide whether Plain View would have supported the use of the evidence against her. *Kahn*, 415 U.S at 152-53.

136. 449 F.2d 679 (10th Cir. 1971).

137. Id. at 686. Electronic surveillance is inherently difficult to manage given the nature of the telephone, which brings into the surveillance not only everyone using the subject phone but everyone who places a call to it, a problem that increases geometrically when the tap is on a private network and not just a single extension.

information once they had seized it.[138] Suppressing this evidence, however, is no more "irrational" than suppressing more tangible evidence seized in violation of the Fourth Amendment in traditional searches. The *Cox* court based its holding on the fact that the police had done nothing "unreasonable" in discovering the unrelated evidence, but failed to consider the important privacy protections the Supreme Court has always emphasized in Plain View cases.[139]

The court in *United States v. John*[140] also treated the Title III order as if it were a warrant to search anything transmitted along the subject communication line, holding that section 2517(5) allowed use of conversations unrelated to the offenses listed on the warrant because the section was analogous to Plain View: "Like an officer who sees contraband in plain view from a vantage point *where he has a right to be*, one properly overhearing unexpected villainy need not ignore such evidence."[141] As the Plain View cases demonstrate, however, the officer had no right to *be* in the unrelated conversation if its seizure entailed an additional invasion of privacy.[142]

The court in *United States v. Sklaroff*,[143] similarly, based its analysis of probable cause on the wiretap as a whole. In justifying this approach, the court inadvertently revealed the difficulty of reconciling its reasoning with *Katz*. The *Sklaroff* court read *Katz* to say that the "original interception" was a "seizure," and concluded that Plain View could therefore apply to anything found during a Title III search as long as Title III's technical requirements were met.[144] However, the *Sklaroff* court notably changed the language of *Katz*, which referred to the seizure of a conversation and not the original interception. This misstep allowed the

---

138. *Id.* at 687.

139. *See, e.g.*, Horton v. United States, 496 U.S. 128, 138-43 (1990).

140. 539 F.2d 181 (D.C. Cir. 1976).

141. *Id.* at 188 (emphasis added).

142. Seizure of unrelated conversations under this reading would be analogous to the search of the turntable in Hicks v. United States, 480 U.S. 321 (1987). Since this search represented a further invasion of Hicks's privacy, unjustified by the officer's initial right to be in the apartment, the court held it violated Hicks's Fourth Amendment rights. *Id.* at 327-28; *cf.* People v. DiStefano, 382 N.Y.S.2d 5, 9 (1976) ("Since eavesdropping warrants are based on substantially the same principles applicable to search warrants for physical objects . . . it seems only logical for the Legislature to have intended that intercepted communications to be treated similarly."); United States v. Escandar, 319 F. Supp. 295, 301 (S.D. Fla. 1970) assuming Title III analogous to a physical search); GOLDSMITH, *supra* note 95, at 146.

143. 323 F. Supp. 296, 307 (S.D. Fla. 1971).

144. Id. ("This is only a restatement of existing case law, adapted to fit the electronic surveillance situation.").

court to avoid the question of whether the probable cause requirement of Plain View analysis should be applied to the line as a whole or individually to the communications on the line.

In *United States v. Williams*,[145] the court rejected outright the defendant's effort to apply Plain View principles to evidence of other offenses overheard in conversations unrelated to the gambling offenses specified in the Title III order.[146] The court nonetheless upheld the use of the unrelated conversations on the ground that whatever privacy interest the parties had was trumped by the legality of the order that allowed the officers to hear them. The court, however, never addressed whether probable cause at the time of the seizure, the key component in the Court's "less sensitive" Plain View cases, was satisfied.[147]

2. *Testing Probable Cause for Each Communication*

The more appropriate application of the probable cause test in the Title III context would be to the individual communication being intercepted, rather than the entire line that was tapped. If the investigators listen to a call or decode a digital message relating to a subject offense, its seizure is justified by the order itself and there is no need to rely on Plain View to defend its use as evidence. For digital messages that do not relate to the listed offenses, however, investigators will not be able to establish that the interception and subsequent translation of the messages (the search and seizure) was justified by probable cause. Thus, like the turntable's serial number in *Hicks*, their evidentiary value must be suppressed.[148]

If transmission on the line is insufficient to satisfy probable cause,

---

145. 737 F.2d 594 (7th Cir. 1984).

146. *Id.* at 604-06 ("A more sensitive, less doctrinaire, inquiry is required.").

147. *See also* United States v. Marcy, 777 F. Supp. 1400, 1403 (N.D. Ill. 1991) ("[I]t would be absurd to suppose that the government could not seize evidence allegedly relating to 'non-enumerated' criminality because it happened to discover such evidence during the course of otherwise lawful electronic surveillance," citing *Williams*). United States v. D'Aquila, 719 F. Supp. 98, 111-14 (D. Conn. 1989), actually found that the "technical requirements" of § 2517(5) had been violated, but refused to suppress evidence of the other offenses because *defendants* failed to show that the government acted in bad faith in seeking the original order.

148. *Cf.* United States v. Cervantes, 1994 WL 91280, *2 (7th Cir. March 22, 1994). The necessary processing to determine the evidentiary value of a digital message, as described in Section III, is considerably more invasive than simply turning over the turntable by police who were lawfully in Hicks's apartment, and strains the analogy of "plain view" beyond recognition.

Plain View would rarely apply, since the investigator would have to search the communication not covered by the Title III order after intercepting it to determine if it had probative value. This subsequent search is clearly not permitted unless there was probable cause for the seizure at the time the communication was seized. Aside from its proximity to communications that were covered by the order, there is nothing about an unrelated communication that would give the investigators any reason to believe it had evidentiary value. The value of the communication does not become apparent until after the unauthorized processing takes place. Similarly, the evidentiary value of the turntable in *Hicks* did not become apparent until after the police recorded and checked its serial number. Thus, the search of the turntable was illegal because at the time the police turned it over, they had no reason to believe it had evidentiary value.

This test limits but does not nullify Plain View. Plain View could still be used for evidence of unrelated offenses found *within* communications that are covered by the order; for example, when a communication concerning insider trading also contains evidence of an unrelated gambling operation. The police have a legal justification for being inside this communication, just as the officer in *Horton* was justified in looking for rings in a drawer in which he found the guns. In this case the final processing of the communication necessary to transform it into readable form was justified because the communication was related to the insider trading specifically listed in the Title III order. Furthermore, the text of the communication relating to the illegal gambling operation is admissible because the final processing which brought this text into plain view was legally justified.

C. Evidentiary Value Immediately Apparent

The *Dickerson* Court underscored that Plain View requires not only probable cause for the seizure to connect it with criminal activity, but also that the evidentiary value of the item seized be immediately apparent to the officers. In *Dickerson*, the Court noted that the officer "determined that the lump was contraband" only after "squeezing, sliding, and otherwise manipulating the contents of the defendant's pocket."[149] This "continued exploration" constituted a "further search" not justified by any

149. Minnesota v. Dickerson, 113 S. Ct. 2130, 2138 (1993).

exception to the warrant requirement, and was thus "constitutionally invalid."[150]

This language suggests that the fast-and-loose analysis applied by courts regarding the admissibility of section 2517(5) evidence, demonstrated in the *Williams* case, is simply incompatible with the Supreme Court's continued emphasis on protecting privacy interests when considering Plain View. While Title III may give the investigators the right to intercept unrelated digital communications, the intensive "manipulation" required to bring their evidentiary value into view cannot be squared with *Dickerson*. It is quite clear from Section III that the evidentiary value of an unrelated digital communication can never be "immediately apparent" at the time it is seized.

CONCLUSION

Given the continued acceleration of change in telecommunications technology, federal courts are likely to be called upon to supervise increasingly complicated electronic surveillance under Title III. One largely undefined aspect of this supervision concerns the admissibility of evidence from electronic communications that is obtained outside the particulars of a Title III order. Some courts have attempted to resolve this issue by grafting the Plain View exception onto section 2517(5) of Title III. This article argues that in doing so these courts chose the right tool, but applied it improperly.

An analytical framework has been provided that resolves important questions about the nature of electronic searches and seizures in a manner that is faithful to the intentions of Congress and the underlying Fourth Amendment cases decided by the Supreme Court. This analysis suggests that the minimization requirement, originally designed to ensure searches met the "particularity" requirement of the Fourth Amendment, can no longer satisfy that purpose because digital electronic communications cannot be understood without extensive processing. Applying Plain View analysis leads to a conclusion that this Fourth Amendment exception will rarely apply to these interceptions. The basis that has been given by several lower courts for admitting evidence of "other offenses" is in fact insufficient under what would likely be the Supreme Court's view.

Ironically, a more generous reading of the applicability of Plain View

150. *Id.* at 2138-39.

could actually reduce Title III to a historical oddity or subject it to powerful constitutional challenges. Due to rapid expansion of electronic communications in both business and private life and the explosive growth of the number of people served by private communications equipment, Title III orders can now give law enforcement officers access to vast quantities of private communications including phone calls, electronic mail, faxes, and all manner of computer data transfers. The technical infeasibility of seizing communications covered by the order without actually processing extraneous communications in detail reveals section 2517(5) to be an unexploded land mine, which, absent careful application of the Plain View tests articulated by the Supreme Court, will turn Title III into an authorization of general warrants.

Faced with the prospect of authorizing a wiretap through which all evidence of any criminal activity by persons unrelated to the original investigation may be searched and seized, a neutral magistrate would find it difficult to approve such an order in the growing number of electronic network environments discussed in this article. Alternatively, if such an order is approved, all evidence seized (including evidence related to the original investigation) may be subject to a successful exclusionary challenge. Organized crime, the original target of Title III and ECPA, will have tremendous incentives to structure criminal communications through large private networks precisely because they are too diffuse to support a wiretapping order.

It is no response, finally, to suggest that Congress can simply amend Title III to ensure that the government can get more carefully targeted access to private networks without having to expose the investigation. As recently as March 1994, FBI Director Louis Freeh candidly admitted to a joint House and Senate committee considering amendments to Title III that the Bureau had abandoned its earlier calls for even limited access to private networks, recognizing the impracticability of getting consensus or cooperation from all the parties who would need to be involved. Acknowledging that PBXs and data exchanges constitute a "big hole" in Title III, Freeh told the committee "that's a concession we're willing to make to narrow the package."[151] But applying Title III as it is currently understood to environments that include this "big hole" might drag the

151. *Joint Hearing of the Technology and Law Subcomm. and Law Subcomm. of the Senate Judiciary Comm. and the Civil and Constitutional Rights Subcomm. of the House Judiciary Comm.*, Federal News Service, Mar. 18, 1994, at 20, *available in* LEXIS, NEWS Library, FEDNEW File.

entire statute in with it.