Pen Registers and Privacy: Risk, Expectations, and the Nullification of Congressional Intent

Clifford S. Fishman
PEN REGISTERS AND PRIVACY: RISKS, EXPECTATIONS, AND THE NULLIFICATION OF CONGRESSIONAL INTENT

Clifford S. Fishman*

CONTENTS

I. OVERVIEW ................................................... 558

II. THE EXCLUSIONARY RULE, ELECTRONIC SURVEILLANCE, AND FEDERAL LEGISLATION ................................ 561

III. SMITH V. MARYLAND ....................................... 565

A. Subjective Expectations of Privacy ....................... 566
B. Reasonable Expectations; Assumption of Risk ............ 568

IV. STATUTORY REGULATION OF ELECTRONIC SURVEILLANCE .......................................................... 574

A. Title III ...................................................... 575
B. The Foreign Intelligence Surveillance Act ............... 578

V. SMITH V. MARYLAND AND THE NULLIFICATION OF CONGRESSIONAL INTENT ........................................... 581

A. Pen Register Surveillance in General .................... 582
   1. FISA’s Civil and Criminal Liability Provisions ....... 582
   2. The “Exclusive Means” Provision ...................... 584
B. The “Directed Assistance” Provision ..................... 584
C. The Gap in FISA ........................................... 587

VI. IMMEDIATE IMPLICATIONS .................................. 589

A. Federal Implications ....................................... 589
   1. The FISA “Court Order” Requirement ................. 589
   2. The New York Telephone Dictum: Rule 57(b) and the All Writs Act .............................................. 592
B. State Implications ......................................... 594

VII. CONCLUSION .................................................. 596

* Associate Professor, The Catholic University School of Law. A.B., University of Rochester, 1966; J.D., Columbia University, 1969. Professor Fishman was formerly Executive Assistant District Attorney, Special Narcotics Prosecutor’s Office, New York City.
I. OVERVIEW

When a person makes a long distance telephone call, telephone company equipment automatically makes a record of the numbers dialed. If law enforcement officials want to know what long distance calls were completed from a particular telephone, such information can be obtained by subpoenaing the telephone company's records. On the other hand, except under unusual circumstances, no automatic record is made of the local calls dialed from a telephone. Information concerning local calls, therefore, is normally not available to law enforcement officials, either by request or subpoena, because for all practical purposes such information never existed. A special device, generally known as a pen register or touch-tone decoder, is required to record the local numbers dialed from a particular telephone.

Telephone companies use pen registers in a variety of situations unrelated to criminal investigations. For example, if a subscriber claims that he is being billed for long distance calls that were never made, the telephone company might use a pen register to check the accuracy of its automatic recording equipment. Conversely, if the telephone company suspects that a subscriber is using an illegal device to avoid being billed for long distance calls, the telephone company might use a pen register to determine whether this is being done. Additionally, if a subscriber is receiving obscene or harassing calls and suspects that a particular person is the caller, the telephone company might install a pen register on the suspect's telephone to ascertain whether such calls are being made from that telephone.

Indeed, federal law expressly permits a telephone company, upon its

1. This is common knowledge to anyone who has ever received a long distance telephone bill.
2. See Fed. R. Crim. P. 17(c).
3. A pen register is a mechanical device, usually installed at a central telephone company facility, that records on paper the numbers dialed from a particular telephone by monitoring the electronic impulses caused when the dial is rotated. Such a device reveals only the numbers that have been dialed. It does not enable anyone to hear any of the communications transmitted. Thus, a pen register discloses neither the subject of a communication between the caller and the recipient, their identities, nor whether the call was even completed. A touch-tone decoder accomplishes the same results, with the same limitations, on a touch-tone telephone. See United States v. New York Tel. Co., 434 U.S. 159, 161, 167 (1977); United States v. Caplan, 255 F. Supp. 805, 807 (E.D. Mich. 1966). See generally Claerhout, The Pen Register, 20 Drake L. Rev. 108, 109-10 (1970).
own initiative, to use pen registers for legitimate business purposes. If the telephone company's use of a pen register or other detection device uncovers evidence of criminal conduct, that evidence is admissible at the defendant's trial. Moreover, the person whose telephone was subjected to such surveillance has no fourth amendment grounds upon which to suppress the evidence; only searches and seizures conducted by state or federal officials are subject to constitutional limitations. Different legal issues arise, however, when law enforcement officials conduct pen register surveillance or when a telephone company conducts such surveillance at the behest of the police. The Supreme Court has squarely confronted these issues on two occasions.

The first case presented the question whether law enforcement use of a pen register constituted wiretapping, which is permissible only when conducted pursuant to a special and difficult-to-obtain eavesdropping order.

6. Under 18 U.S.C. § 2511(2)(a)(i) (1976), a communications common carrier may "intercept, disclose, or use" a communication carried over its facilities if such activity is a necessary incident to the service the carrier provides or is necessary to protect "the rights or property" of the carrier.


8. The fourth amendment provides: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. U.S. CONST. amend. IV.


10. When a private individual or entity acts at the request of the government, he is considered a government agent for fourth amendment purposes. His conduct, therefore, is subject to fourth amendment standards and restrictions. See, e.g., United States v. Ogden, 485 F.2d 536 (9th Cir. 1973); Corngold v. United States, 367 F.2d 1 (9th Cir. 1966); Stapleton v. Superior Court, 70 Cal. 2d 97, 447 P.2d 967, 73 Cal. Rptr. 575 (1968); State v. Scrotsky, 39 N.J. 410, 189 A.2d 23 (1963). See also Lustig v. United States, 338 U.S. 74 (1949). See generally 1 W. LAFAVE, SEARCH AND SEIZURE 114 (1978).

In *United States v. New York Telephone Co.*, the Court first ruled that an ordinary search warrant sufficed to authorize law enforcement use of a pen register. Additionally, the Court ruled that a federal district judge possessed the authority to include within the search warrant an order compelling a telephone company to assist the government by installing a pen register on the targeted telephone.

In *Smith v. Maryland*, the Court considered the legality of pen register surveillance conducted by a telephone company pursuant to an informal police request, that is, without a warrant or other court order. In holding

When government officials obtain a Title III order authorizing them to conduct a wiretap, it is common practice for the agents to use a pen register in conjunction with the tap. Several courts have held that such use of a pen register is lawful even if the Title III order does not contain an express provision authorizing its use. See *United States v. Falcone*, 505 F.2d 478, 481-83 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975); *Commonwealth v. Vitello*, 367 Mass. 224, 327 N.E.2d 819, 850 (1975); *State v. Murphy*, 137 N.J. Super. 404, 349 A.2d 122, 138-39 (1975).

12. 434 U.S. 159 (1977). The government was investigating whether two telephones were being used to conduct illegal gambling operations and obtained a search warrant pursuant to rule 41 of the Federal Rules of Criminal Procedure. The court order authorized the use of pen registers on the telephones and directed the company to furnish the F.B.I. with "all information, facilities and technical assistance" necessary to employ the devices. 434 U.S. at 161. The telephone company moved to vacate the order, arguing that only an order issued pursuant to Title III could authorize governmental use of pen registers or direct the company to provide information or assistance. *Id.* at 163.

13. 434 U.S. at 165-68. The Court found support for this conclusion in rule 57(b) of the Federal Rules of Criminal Procedure, which provides: "If no procedure is specifically prescribed by rule, the court may proceed in any manner not inconsistent with these rules or with any applicable statute." The Court then commented: "We need not and do not decide whether Rule 57(b) by itself would authorize the issuance of pen register orders." 434 U.S. at 170.

14. *Id.* at 171-78. The Court concluded that the district judge's authority to compel the telephone company to provide assistance is derived from the All Writs Act, 28 U.S.C. § 1651(a) (1976), which provides: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 434 U.S. at 172. Although the Court acknowledged that the All Writs Act did not authorize federal district courts to impose "unreasonable burdens" upon third parties, the district judge's order in *New York Tel. Co.* was in no way burdensome and even required the government to compensate the telephone company at the prevailing rates. *Id.* at 175.

The Court's reliance on the All Writs Act and its discussion of rule 57(b) of the Federal Rules of Criminal Procedure, see note 13 supra, have assumed additional significance in light of subsequent developments. See notes 175-83 and accompanying text infra.


16. The Court granted certiorari "in order to resolve indications of conflict in the decided cases as to the restrictions imposed by the Fourth Amendment on the use of pen registers." *Id.* at 2579. Prior to *Smith*, federal and state courts were divided as to whether the fourth amendment required law enforcement officials to obtain a search warrant before conducting pen register surveillance with telephone company cooperation. For cases holding or indicating in dicta that a search warrant must be obtained, see, e.g., *Application of the
such pen register use lawful and the evidence obtained admissible against
the defendant at his robbery trial, the Court held that no "search" had
occurred and thus no right to privacy protected by the fourth amendment
was invaded.17

Although the result in Smith is supportable under the particular facts of
the case, the Court's reasoning poses significant problems of both statutory
and constitutional dimensions. As will be demonstrated below, the major-
ity opinion relied on unsupportable factual assumptions, effectively nulli-
fied congressional intent, and introduced an absurd anomaly into federal
law. Ironically, however, while the Smith decision has unsettling implica-
tions for the right to privacy, it is likely to have little if any impact upon
law enforcement use of pen registers.

II. THE EXCLUSIONARY RULE, ELECTRONIC SURVEILLANCE, AND
FEDERAL LEGISLATION

To place the Supreme Court's decision in Smith in historical context,
this section will briefly examine the exclusionary rule, trace its application
electronic surveillance, and highlight legislation governing electronic
surveillance by federal officials.

Although the fourth amendment ensures that persons will not be subject
to "unreasonable" searches and seizures and requires that warrants be
based on probable cause and "particularly describe the place to be
searched and the persons or things to be seized,"18 it does not contain an
express remedy for persons whose security has been violated. In 1914,
however, in Weeks v. United States,19 the Supreme Court espoused a prin-
ciple that has come to be known as the "exclusionary rule": if law enforce-
ment officials conduct searches or seize evidence in a manner that violates
a defendant's fourth amendment rights,20 such evidence cannot be used

17. 99 S. Ct. at 2581-83. See notes 55-78 and accompanying text infra.
18. See note 8 supra.
20. Defining the exact parameters of standing to object to an illegal search and seizure
is a matter of great controversy. See, e.g., 3 W. LaFave, supra note 10, at 543-612; Grove,
against the defendant in a criminal prosecution.\textsuperscript{21}

Initially, the exclusionary rule had little impact upon electronic surveillance. In \textit{Olmstead v. United States},\textsuperscript{22} the Court held that the fourth amendment was inapplicable to wiretapping unless government officials had physically invaded the defendant’s premises. The Court interpreted the fourth amendment’s prohibition against “unreasonable searches and seizures” as meaning an unreasonable physical invasion.\textsuperscript{23} Since wiretapping did not involve a physical trespass, the Court reasoned that no “search” had occurred.\textsuperscript{24} A decade later in \textit{Nardone v. United States},\textsuperscript{25} the Court construed section 605 of the Federal Communications Act of 1934\textsuperscript{26} as creating a \textit{statutory} prohibition against unauthorized wiretapping by either government officials or private citizens.\textsuperscript{27} Thus, evidence obtained in


21. 232 U.S. at 398. The rule enunciated in \textit{Weeks} applied only to evidence seized by a federal agent that was used by a federal prosecutor; the \textit{Weeks} Court concluded that the fourth amendment’s limitations were inapplicable to evidence seized by state officials. \textit{Id.} at 398. Not until 1949, in \textit{Wolf v. Colorado}, 338 U.S. 25 (1949), did the Court hold that the fourth amendment was enforceable against the states through the due process clause of the fourteenth amendment. Moreover, it was not until 1961, in \textit{Mapp v. Ohio}, 367 U.S. 643 (1961), that the Supreme Court held that the exclusionary rule was enforceable against the states.

Proponents of the exclusionary rule have justified it as a necessity to give meaning to the fourth amendment right of privacy, to deter police misconduct by removing the incentive for illegal searches and seizures, and to preserve the integrity of the judicial system. \textit{See, e.g.}, \textit{Mapp v. Ohio}, 367 U.S. at 654-59; \textit{Weeks v. United States}, 232 U.S. at 392-93. Opponents of the rule argue that it is based on an unrealistic concept of the criminal justice system, that the rule has not and cannot have any significant deterrent effect on police misconduct, and that the cost to society — suppression of probative evidence of guilt and the resultant freeing of thousands of “guilty” criminals — far outweighs whatever minimal benefits the rule otherwise provides. \textit{See, e.g.}, \textit{Bivens v. Six Unknown Named Agents}, 403 U.S. 388, 412-24 (1971) (Burger, C.J., dissenting), and sources cited therein. For a concise history of the exclusionary rule, see Miles, \textit{Decline of the Fourth Amendment: Time to Overrule Mapp v. Ohio}, 27 CATH. U.L. REV. 9, 29-52 (1977).

22. 277 U.S. 438 (1928).

23. \textit{Olmstead} had been convicted of violating the National Prohibition Act by transporting and selling intoxicating liquor. The government had obtained its evidence against \textit{Olmstead} through wiretapping. \textit{Id.} at 455-57.


27. 302 U.S. at 382.
violation of the Act was inadmissible in federal prosecutions. Subsequ-
ently, in Goldman v. United States, the Court reiterated its Olmstead
ruling that the electronic overhearing of conversations without a physical
trespass onto the defendant's premises did not constitute a search within
the meaning of the fourth amendment.

Not until 1961, in Silverman v. United States, did the Court for the first
time suppress the fruits of electronic surveillance on constitutional
grounds. In Silverman, the Court held that by driving a "spike mike" sev-
eral inches into a party wall of the suspects' house, the agents had commit-
ted an illegal trespass that constituted an illegal search. A similar result
was reached in Clinton v. Virginia, involving a listening device that pene-
trated no more than a thumbtack deep.

The Court finally abolished the physical trespass requirement in Katz v.
United States. Government agents, acting with probable cause but with-
out a warrant, placed a listening device on the outside of a public tele-
phone booth. The agents overheard what Katz said during two telephone
conversations and so testified at Katz's gambling trial. The litigants had
approached the case in terms of whether a telephone booth was a "consti-
tutionally protected area" and whether physical penetration into such an
area had to occur before a defendant could invoke the fourth amendment's
proscription against unreasonable searches and seizures. The Court, how-
ever, "decline[d] to adopt this formulation of the issues." Justice
Stewart, writing for the majority, stressed that the interests protected by

28. In the second Nardone case, the Court held that evidence derived from wiretapping
in violation of the Federal Communications Act must be suppressed. Nardone v. United
render evidence obtained in violation of the Act inadmissible in state courts). See also
Rathburn v. United States, 355 U.S. 107 (1957) (no statutory violation when agent listening
to conversation had the consent of one party).

29. 316 U.S. 129 (1942).

30. Id. at 133-36. In Goldman, federal agents overheard conversations between defend-
ants Goldman and Shulman by pressing a listening device against the wall of an office ad-
joining Shulman's. Since there had been no physical trespass into Shulman's premises, the
Court reasoned that no search had occurred. Id.


32. Id. at 509-10.


Katz v. United States, a Postscriptum, 9 Ind. L. Rev. 468 (1976); Note, From Private Places
to Personal Privacy: A Post-Katz Study of Fourth Amendment Protections, 43 N.Y.U.L. Rev.
968 (1968).

35. 389 U.S. at 349-50.

36. Id. at 350.
the fourth amendment were not limited to those of property and freedom from physical trespass. The Court emphasized:

[The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.]

Katz, therefore, eliminated constitutional distinctions based solely on the existence of a physical intrusion and freed the fourth amendment from the constraints of property law. But while "the fourth amendment protects people, not places," the real question, as Justice Harlan pointed out in his concurring opinion, is "what protection [the fourth amendment] affords to those people."

Before a fourth amendment search and seizure can be said to have occurred, someone seeking to suppress evidence must satisfy a two-fold requirement: "first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"

Since Katz, fourth amendment litigation has often focused on whether a particular defendant had a reasonable, "legitimate," or "justifiable" expectation of privacy. In particular, the Court has frequently held that when a person reveals information to a second party, he assumes the risk that the second party will disclose that information to government officials; no constitutionally recognized expectation of privacy is violated if the second party in fact discloses what has been revealed.

Two federal statutes govern the use of electronic surveillance. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 regulates wiretapping and eavesdropping by law enforcement officials. The For-

37. Id. at 351 (citations omitted). Although the agents had probable cause to believe that Katz's conversations would be incriminating and acted with restraint by listening only when Katz was in the booth, the Court suppressed the agents' testimony as to what Katz said because the agents had failed to obtain a warrant authorizing the use of the listening device. Id. at 356-57.


39. 389 U.S. at 361 (Harlan, J., concurring).

40. Id.


42. See note 63 and accompanying text infra.


44. Title III authorized states to enact similar legislation which could be more restrictive but not more permissive than Title III. 18 U.S.C. § 2516(2) (1976). See S. REP. No.
eign Intelligence Surveillance Act of 1978\(^4^5\) regulates the use of electronic surveillance by federal officials for national security purposes. The aspects of these statutes relating to pen registers will be discussed in detail below.

III. Smith v. Maryland

The pertinent facts in Smith are readily stated. A robbery victim who had provided the police with a description and other information concerning the perpetrator began receiving threatening and obscene telephone calls from a man claiming to have committed the robbery. Because the investigation focused suspicion on Smith, the police requested that the telephone company employ a pen register to record the numbers dialed from Smith’s home telephone.\(^4^6\) The telephone company complied, installing the pen register at its central offices. The police did not seek a search warrant or other court order authorizing the use of the pen register.\(^4^7\) The day after its installation, the register revealed that a call was placed from Smith’s home telephone to the victim’s home telephone.\(^4^8\) Relying on this fact and the other information provided by the victim, the police obtained a search warrant for Smith’s home. The search revealed that a page in Smith’s telephone book was turned down to the victim’s name and number. The book was seized, Smith was arrested, a lineup was held, and the victim identified Smith as the robber.\(^4^9\)

Prior to trial, Smith moved to suppress all evidence derived from the use of the pen register on the ground that the failure of the police to obtain a warrant prior to the register’s installation rendered its use an illegal search and seizure.\(^5^0\) The trial court denied the suppression motion, and the Ma-

---

1097, 90th Cong., 2d Sess. 89, reprinted in [1968] U.S. CODE CONG. & AD. NEWS 2112, 2177. For a listing of such state laws, see C. Fishman, supra note 11, at 6.


46. 99 S. Ct. at 2578. The police may have had probable cause for a search warrant authorizing the use of the pen register on Smith's telephone. The victim had given the police a description of the robber and his automobile. In one of the calls, the self-proclaimed robber asked the victim to step out on her front porch; she did so and saw the same car that she had previously described to the police moving slowly past her home. A few days later, a police officer observed a man fitting the victim's description of the robber driving a car of the same year and make in the victim's neighborhood. By tracing the license plate number, the police learned that the car was registered to Smith. Id. Although the telephone company had traced some of the calls to a public telephone booth, the victim indicated that at least one of the calls seemed to have been made from a private residence. See Smith v. State, 283 Md. 156, 158, 389 A.2d 858, 859 (1978).

47. 99 S. Ct. at 2578.

48. Id. at 2578-79.

49. Id. at 2579.

50. Id.
ryland Court of Appeals affirmed, holding that, because no "search" had occurred, no warrant was required.\footnote{51}

As noted earlier, {\it Katz}\footnote{52} established that official conduct\footnote{53} constitutes a search and seizure subject to fourth amendment restrictions only if that conduct intrudes upon a person's expectation of privacy. And an expectation of privacy qualifies for fourth amendment protection only if two requirements are met: first, the individual by his conduct must have exhibited an actual (subjective) expectation of privacy and, second, such expectation must be one that society recognizes as reasonable.\footnote{54}

As an initial matter, the {\it Smith} Court ruled that pen register surveillance did not intrude upon a property right of Smith's because the register was installed at a central telephone company facility, not in his home, and the contents of Smith's conversations were not overheard.\footnote{55} Thus, the Court defined the issue as whether Smith had a "legitimate expectation of privacy" regarding the numbers he dialed on his home telephone. After examining the facts, the Court held that he did not.

\textbf{A. Subjective Expectations of Privacy}

In reaching its decision, the Court first questioned whether Smith actually harbored a subjective expectation of privacy concerning the numbers he dialed from his home telephone. People generally do not entertain such expectations, the Court reasoned, since the public "knows" that the telephone company has equipment capable of recording such numbers and does so for a variety of legitimate business purposes.\footnote{56} In particular, "most people . . . presumably have some awareness of one common use [of pen registers]: to aid in the identification of persons making annoying or ob-

\footnote{51. {\it Id.}; see Smith v. State, 283 Md. 156, 173-74, 389 A.2d 858, 867-68 (1978).}
\footnote{52. 389 U.S. 347 (1967).}
\footnote{53. The {\it Smith} Court noted that the pen register was installed at the request of the police, and the State apparently conceded that the telephone company was acting as a police agent rendering use of the register "state action" under the fourth and fourteenth amendments. The Court, therefore, assumed that "state action" was, in fact, present. 99 S. Ct. at 2579-80 n.4. Nevertheless, it is not altogether clear that the state's concession or the Court's acceptance of the existence of state action was truly necessary. See note 76 infra.}
\footnote{54. See Smith v. Maryland, 99 S. Ct. at 2580 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)); notes 34-42 and accompanying text supra.}
\footnote{55. 99 S. Ct. at 2581.}
\footnote{56. The Court noted that subscribers receive a list of their long distance calls on their monthly statements and that pen registers are used to detect fraud, to record numbers dialed from telephones subject to a special rate structure, to determine whether a home telephone is being used for business purposes, to check for a defective dial, and to check for overbilling. {\it Id.} at 2581. However, the Court conceded that "most people may be oblivious to a pen register's esoteric functions . . . ." {\it Id.}.}
scene calls.” Upon this factual assumption, the Court reasoned that “it is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret.” Additionally, the Court deemed irrelevant the fact that the telephone in question was located in Smith's home:

Regardless of his location [when he made the call], petitioner had to convey that number to the telephone company . . . . The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think it would.

The factual assumptions underlying the Court's decision in Smith are, at

57. Id. As evidence of such public awareness, the Court stated that most telephone directories contain a page entitled “Consumer Information,” informing subscribers that the telephone company “can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.” Id.

Dissenting from the Court's opinion, Justice Marshall derided “the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers” and refused to assume “general public awareness of how obscene phone calls are traced.” Id. at 2548 n.1 (Marshall, J., dissenting).

As pointed out by Justice Marshall, the majority's assumption that the public has any precise notion of how a telephone company identifies the source of an annoying call is indeed dubious. If pressed to speculate as to how this might be accomplished, most individuals would probably assume that the telephone company would attempt to trace the call backwards from the recipient telephone to the sending telephone. In fact, Smith himself may have — accurately — made such an assumption. The telephone company had traced some of the calls from the victim's telephone back to a public telephone located in the victim's neighborhood. See State v. Smith, 283 Md. at 158, 389 A.2d at 859.

Furthermore, the consumer information page of most telephone books is unlikely to enlighten even the most avid reader. To research this question, directories from fifteen cities were examined: Atlanta, Ga. (1978); Boston, Mass. (1979); Buffalo, N.Y. (1979); Dallas, Tex. (1979); Denver, Colo. (1978); District of Columbia (1979); Los Angeles, Cal. (1979); Manhattan, New York City (1978-79); Miami, Fla. (1977-78); Omaha, Neb. (1979-80); Philadelphia, Pa. (1978); Phoenix, Ariz. (1979); Rochester, N.Y. (1979); San Diego, Cal. (1979); Tulsa, Okla. (1978). None of these directories mentioned any special equipment or special procedures under the heading of “Annoyance Calls.” Eight directories did mention specialized equipment, however, under the heading “Fraudulent Use of the Telephone,” without explanation of the nature and use of the equipment. See the directories for the cities of Atlanta; Boston; Buffalo; Dallas; District of Columbia; Manhattan; Rochester; Tulsa.

On the other hand, all fifteen directories contained a heading entitled “Illegal Wiretapping.” There, the reader could learn that it is illegal to intercept a phone call without the consent of a participant and that the telephone company would not install a wiretap on any telephone for the police unless presented with a warrant.

It is unlikely that the general public, unaware of the niceties of telephone technology or constitutional law, would distinguish between a wiretap, which requires a special court order to authorize overhearing conversations, and a pen register, which merely records the numbers dialed. If anything, the consumer information page of these directories would increase, rather than diminish, the reader’s sense of security in the privacy of his telephone.

58. 99 S. Ct. at 2581.
59. Id. at 2582.
best, dubious. A telephone company rarely makes a record of the local numbers dialed from a telephone. When it does, such records are used only for valid internal business purposes relating to the service the telephone company provides its subscribers. Moreover, there was no evidence before the Court that the average telephone user is aware of the circumstances under which such a record will be made. Thus, it is more reasonable to assume that the absence of a listing of local calls on monthly telephone bills leaves most subscribers with the accurate impression that the telephone company does not record such numbers. In sum, the Smith Court's holding that society does not expect privacy with regard to local numbers dialed is patently inaccurate.

B. Reasonable Expectations; Assumption of Risk

Notwithstanding that Smith "did harbor some subjective expectation that the phone numbers he dialed would remain private," the Court held that such expectation "is not one that society is prepared to recognize as 'reasonable.'" The Smith majority reasoned that whenever a person voluntarily reveals information to a third person he "assumes the risk" that the third person will disclose the information to the authorities.

When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business.

60. See notes 4, 5, 56 and accompanying text supra.
61. See note 57 supra.
62. 99 S. Ct. at 2582.

In Hoffa, the Court held that when a suspect voluntarily reveals information to a government informant, such information is not subject to fourth amendment protection. 385 U.S. at 303. In Lopez, the Court held that no warrant is required to authorize a government agent to tape record his conversation with a suspect. 373 U.S. at 439. Similarly, White held that no warrant is required to authorize an agent to transmit electronically his conversation with a suspect to other agents. 401 U.S. at 751. See generally Fishman, The Interception of Communications Without a Court Order: Title III, Consent, and the Expectation of Privacy, 51 ST. JOHN'S L. REV. 41 (1976). See also Greenawalt, The Consent Problem in Wiretapping & Eavesdropping: Surreptitious Monitoring with the Consent of a Participant in a Conversation, 68 COLUM. L. REV. 189 (1968); Comment, Eavesdropping, Informers and the Right of Privacy: A Judicial Tightrope, 52 CORNELL L.Q. 975 (1967).

In Couch, the Court upheld an Internal Revenue Service summons requiring Couch's accountant to surrender Couch's business records. The Court ruled that Couch had voluntarily revealed the records to her accountant knowing that the accountant would have to disclose much of the information when he filed Couch's tax return. Therefore, the Court reasoned that Couch had no reasonable expectation of privacy with regard to the records. 409 U.S. at 335.
ness. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.64

In support of its "assumption of risk" theory, the Court quoted extensively from United States v. Miller.65 In Miller, the Court held that when a depositor "reveals" his financial affairs to a bank (by writing checks, filling out deposit slips, and the like), he or she assumes the risk that the bank will disclose this information to the government.66 The depositor, therefore, has no reasonable expectation of privacy if the bank actually does so.67

The Court's reliance on Miller to support an assumption of risk rationale in the context of electronic surveillance is rather tenuous. Miller is distinguishable from Smith on several significant grounds. First, Smith's reliance on Miller is inapt because bank records are regulated by a special statute, the Bank Secrecy Act.68 This statute's sole purpose is to require banks to preserve records of customer transactions so that they will be accessible to law enforcement officials pursuant to legal process.69 No comparable statute requires telephone companies to maintain records of either local or long distance calls.70 Second, in Miller, the government obtained the depositor's records pursuant to legal process.71 In contrast, the telephone company in Smith installed the pen register and preserved and re-

64. 99 S. Ct. at 2582 (emphasis supplied). The Court emphasized, and Smith conceded, that if he had placed his calls through an operator who subsequently disclosed the number called to the police, Smith would have had no legitimate expectation of privacy. The Court reasoned that no different constitutional result is required "because the telephone company has decided to automate." Id. However, this analogy to a live telephone operator is inapposite. See notes 79-84 and accompanying text infra.


66. 425 U.S. at 442-44.

67. See Alexander & Spurgeon, supra note 65, at 29-32.


70. During eight years as a prosecutor in New York City, the author had subpoenas issued for long distance toll records on several occasions, only to learn that some telephone companies regularly destroy their records of subscribers' calls after a specified period.

71. Both the legislative history and the regulations of the Bank Secrecy Act provide that the government can obtain access to a depositor's records only pursuant to "existing legal process." See California Bankers Association v. Schultz, 416 U.S. at 52. In Miller, the Court ruled that a grand jury subpoena duces tecum issued by a federal prosecutor and served upon the
revealed the information sought pursuant to nothing more than an informal police request.\textsuperscript{72}

Finally, when the bank depositor writes a check, fills out a deposit slip, or transacts other business, records of such transactions are \textit{regularly made and kept by the bank}.\textsuperscript{73} The depositor is reminded of this fact by each monthly statement. Thus, a depositor is aware that records exist and that it is possible for others to gain access to those records.\textsuperscript{74}

In contrast, since a monthly telephone statement does not include a listing of local telephone calls, the subscriber might reasonably conclude that no such record exists. Such a conclusion is not only logical but, in the ordinary course of events, factually correct.\textsuperscript{75} In fact, the \textit{Smith} Court acknowledged that telephone companies usually maintain records only of long distance calls and that the company would not have kept a record of banks at which Miller maintained accounts was adequate legal process under the Act. 425 U.S. at 446.

The facts in \textit{Miller}, however, suggest that the protections afforded by the Act's legal process requirement may be illusory. Miller was not notified that his records had been subpoenaed and thus had no opportunity to move to quash the subpoena prior to disclosure of his records. The subpoena had been made returnable for a date on which no grand jury was sitting. Moreover, instead of producing the records before the grand jury, the banks permitted a federal agent to examine microfilms of Miller's checks and deposit slips and reproduced copies of the specific checks and deposit slips the agent requested. 425 U.S. at 438. The Court, however, deemed the failure of the government and the bank to notify Miller as well as the alleged defects in the subpoena, to be irrelevant. \textit{Id.} at 440. Congress might better have balanced the needs of law enforcement and protection of privacy if the statute had required a prosecutor subpoenaing records to notify the depositor, thereby affording the latter an opportunity to move to quash the subpoena or limit its scope. Additionally, the statute might have provided for a subpoena without notice to the depositor if the prosecutor were able to convince an appropriate judge that there was a legitimate need for the records and that notice would jeopardize an ongoing investigation.

\textsuperscript{72} 99 S. Ct. at 2578.
\textsuperscript{73} See United States v. Miller, 425 U.S. at 436, 442-43. See note 68 supra.
\textsuperscript{74} In this respect, \textit{Miller} is consistent with \textit{Lopez}, \textit{Hoffa}, \textit{Couch}, and \textit{White}. See note 63 supra. When a person reveals information to another, he is aware that the one in whom he confides might be or might become a government agent who will disclose such information to the authorities. See, e.g., Hoffa v. United States, 385 U.S. 293 (1966). Similarly, no additional fourth amendment issue arises if the other participant to a conversation is in fact a government agent who records or transmits the disclosure, thereby rendering the information less vulnerable to challenges based upon the agent's memory or credibility. See, e.g., United States v. White, 401 U.S. 745 (1971); Lopez v. United States, 373 U.S. 427 (1963). Furthermore, a taxpayer who gives financial information to an accountant is aware that the accountant will have to reveal much of the information to federal and state tax agencies. See, e.g., Couch v. United States, 409 U.S. 322 (1973). Thus, in each situation, the person making a disclosure is actually aware that he is conveying information and can reasonably be held to have "assumed the risk" that such information will be revealed to governmental authorities.

\textsuperscript{75} The Court in \textit{Smith} conceded this fact but held it to be of no consequence. See notes 60-61 and accompanying text supra.
Smith's local calls but for the request by the police. Nevertheless, the Court deemed this insufficient to create a valid expectation of privacy concerning the local numbers Smith dialed from his home telephone. Smith assumed the risk that the telephone company would make a record of local as well as long distance numbers and reveal that information to the police. According to the majority, its acceptance of the local-long distance distinction as constitutionally significant would "make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." Thus, in the absence of a "legitimate" expectation of privacy, the installation and use of a pen register is not a search within the meaning of the fourth amendment, and therefore no search warrant is required.

The reasoning adopted by the Court in Smith is troubling in several respects. In rejecting the local/long distance distinction, the Court applied an "assumption of risk" analysis to privacy expectations under circumstances significantly different from those in previous assumption of risk cases. Absent the request of the police to the telephone company, information concerning Smith's local calls, for all practical purposes, probably never would have existed. Thus, the state not only obtained but, in a real sense, created evidence. In this respect, Smith is factually different from the prior assumption of risk cases cited by the Court. It is one thing to hold that the fourth amendment does not shield an individual from the risk that information freely conveyed to others might be disclosed to governmental authorities. It is something else again to hold that a person "assumes the risk" that the government will cause evidence to be created from one's home telephone without any constitutional safeguards or restrictions.

76. As noted earlier, the state apparently did not attempt to show that the telephone company would have installed a pen register if the request had come from the victim rather than the police. Had the company installed the register on its own initiative or its customer's, no state action would have been involved, and the fourth amendment would be inapplicable. See notes 7, 9 supra. Thus, an alternative approach to the facts in Smith is suggested: the state could have attempted to establish by clear and convincing evidence that the telephone company, provided with the same information, would have used the pen register even if not asked to do so by the police. Had the state made such a showing or had the Court remanded for consideration of this issue, it might not have been necessary for the Court to have decided the constitutional privacy question.

77. 99 S. Ct. at 2583.

78. Id.

79. Although this was not factually established at trial, the Court proceeded on the assumption that such was the case. See note 53 supra.

80. See notes 63-76 and accompanying text supra.

81. This is not to suggest that a fourth amendment search occurs whenever the state persuades a private individual to collect information for the police. For example, a police
Even more disturbing is the Smith Court's casual application of the "assumption of risk" doctrine to privacy expectations. Technology has developed to the point that virtually any activity, however private or guarded, may be vulnerable to surreptitious surveillance. Surely, mere public recognition of this unhappy fact does not constitutionally require persons to assume all risks and forfeit all reasonable and legitimate expectations of privacy from governmental surveillance.

In determining the scope of fourth amendment protections, it is not enough simply to recite the risks as did the Smith majority; it is also necessary to determine whether such risks should be constitutionally recognized as limitations on individual privacy rights. Justice Marshall, dissenting

officer might ask a building doorman to write down the comings and goings of a particular resident. Unlike the use of a pen register in Smith, the doorman's compliance with the request does not "create" information. The police request simply assures the accurate retention of facts the doorman would have otherwise perceived. In contrast, but for the police's request in Smith, no human being (other than Smith) would ever have known the numbers dialed from Smith's home telephone.

82. A nontecnological analogy may prove instructive. Several courts have held that when a suspect occupying a hotel room converses at a volume loud enough to be overheard by investigators who are (not coincidentally) located in an adjoining room, no unlawful search or seizure of the suspect's words has occurred and testimony concerning what was overheard is admissible at trial. See, e.g., United States v. Sin Nagh Fong, 490 F.2d 527 (9th Cir.), cert. denied, 417 U.S. 916 (1974); United States v. Ortega, 471 F.2d 1350 (2d Cir. 1972), cert. denied, 411 U.S. 948 (1973); Satterfield v. State, 127 Ga. App. 528, 194 S.E.2d 295 (1972). In United States v. Mallah, 503 F.2d 971, 975-76 (2d Cir. 1974), cert. denied, 420 U.S. 995 (1975), and United States v. Sperling, 506 F.2d 1323, 1344 n.31 (2d Cir. 1974), cert. denied, 420 U.S. 962 (1975) (appeals arising out of the same investigation in which the author participated), narcotics suspects' conversations, conducted on a public sidewalk, were overheard by a police officer hidden in the trunk of a car parked nearby. The court held in each case that the defendants lacked a reasonable expectation of privacy on the sidewalk. See generally C. Fishman, supra note 11, at 43-44.

83. Professor Amsterdam suggests that an intrusive government might not only exploit but actually initiate developments diminishing societal privacy expectations. For example, law enforcement officials might simply announce that, henceforth, they will randomly monitor the contents of first-class mail or private telephone conversations. Once the public has been put on notice of the risks they "assume" in such communications, under a strict application of the "assumption of risk" approach, privacy expectations respecting such communications would no longer be justified. See Amsterdam, supra note 38, at 349, 384, 407 (cited in Smith v. Maryland, 99 S. Ct. at 2585 (Marshall, J., dissenting)). Cf. Delaware v. Prouse, 440 U.S. 648 (1979) (without reasonable, articulable suspicion of motor vehicle violation, random police detention and search for driver's license violates fourth amendment).

84. When a person sends a telegram, he necessarily divulges the contents of his message to the Western Union clerk and presumably is aware that the clerk might disclose the message to others. When a person places a telephone call through a switchboard operator, he is aware that the operator might listen in and reveal what was said. When a person uses a party-line telephone or a telephone that has an extension in another room, he is aware that someone might be listening in and might disclose the conversation. In a factual sense, therefore, the individual "assumes the risk" that the government, in anticipation of the telegram
in Smith, set forth the appropriate inquiry: "whether privacy expectations are legitimate within the meaning of Katz depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society." The Smith majority gave passing recognition to this basic question, acknowledging that under some circumstances "a normative inquiry would be proper." The majority, however, did not engage in such an

or phone call, might ask the clerk, or the operator, or a person with access to the party line or extension phone, to report the contents of the message or to listen in and disclose the contents of the conversation. Similarly, when a person rents a hotel room he can be said to have "assumed the risk" that the hotel management might have bugged the room at the request of the police. Clearly, however, such surveillance would constitute a search subject to the fourth amendment.

85. 99 S. Ct. at 2585 (Marshall, J., dissenting). Although I agree with Justice Marshall that value judgments and not merely assessment of risks must be made, I disagree with his conclusions in a number of cases. In United States v. White, 401 U.S. 745 (1971), Justice Marshall asserted that the fourth amendment requires a search warrant before an informer may transmit or record his conversation with a criminal suspect. Id. at 795-96 (Marshall, J., dissenting). Since no warrant is required to authorize the informer's encounter with a suspect, there is no constitutional reason why a warrant should be required before the informer may record or transmit what he would in any event hear. Further, the imposition of a warrant requirement in this situation would often impose undue burdens on already limited law enforcement resources. See C. Fishman, supra note 11, at 93-98. Similarly, Justice Marshall dissented in California Bankers Ass'n v. Schultz, 416 U.S. 21 (1974), which upheld the constitutionality of the Bank Secrecy Act. See note 68 supra. Justice Marshall argued that to require an unwilling bank to preserve records that otherwise would have been destroyed, in effect, required the bank to collect evidence. He saw this as the constitutional equivalent of forcing a private citizen to make an illegal entry onto a premises and to photocopy documents kept there. Thus, the mandated preservation of a depositor's records constituted an illegal governmental "seizure." Further, Justice Marshall argued that the government's use of existing legal process to obtain the records would provide the depositor with no protection. He predicted that the Court would hold that the depositor lacked standing to contest a bank's compliance with a subpoena for the records. 416 U.S. at 94-97 (Marshall, J., dissenting). This prediction was confirmed in United States v. Miller, 425 U.S. 435 (1976). Although Congress might have struck a better balance between the government's legitimate need for the records and the depositor's right to privacy, see note 71 supra, Justice Marshall's categorization of the statute as the equivalent of an illegal seizure is unwarranted. Virtually all of the information covered by the Bank Secrecy Act is information that the bank would have made a record of in any event. Requiring a bank to preserve those records is not a seizure. The seizure occurs only when the bank, complying with a subpoena, delivers the records to the government. In this respect, the Act does not violate the fourth amendment.

86. The majority stated:

Situations can be imagined, of course, in which Katz' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously moni-
inquiry, explain why it did not, or indicate when such an inquiry would be appropriate or necessary.

Smith v. Maryland was an appropriate case for just such an inquiry. "Implicit in the concept of assumption of risk is some notion of choice." 87 The telephone has assumed a vital role in private communications. 88 Yet, much of that privacy is stripped away if an individual must "assume the risk" of pen register surveillance each time he dials his telephone. Indeed, it is absurd to speak in terms of assumed risks "where, as a practical matter, individuals have no realistic alternative." 89 Persons whose conduct involves no criminality may wish to avoid disclosure of their personal or professional contacts. For example, persons who quietly support unpopular causes or journalists wishing to preserve the confidentiality of their sources might fall into this category. 90 More fundamentally, it is simply "nobody's business" whom a person contacts by telephone unless a judicial officer is satisfied that the government has a valid basis for seeking to know. 91

Imposition of a search warrant requirement before law enforcement officials may seek telephone company cooperation in the use of a pen register would limit such privacy intrusions to those situations in which the need and basis for the intrusion are adequately demonstrated. The matter seems an appropriate subject for legislative correction.

IV. Statutory Regulation of Electronic Surveillance

Congress has enacted two statutes regulating governmental use of e

99 S. Ct. at 2580 n.5.
87. Id. at 2585 (Marshall, J., dissenting).
88. See id. at 2583 (Stewart, J., dissenting).
89. Id. at 2585 (Marshall, J., dissenting).
91. It can, of course, be argued that this principle applies to long distance toll records as well as to pen register surveillance of local calls. However, in contrast with the situation in Smith, the telephone company regularly keeps long distance toll call records for business purposes and subscribers are aware that such records might be available to the government. Thus, the "assumption of risk" theory, combined with the legitimate investigatory needs of prosecutors and grand juries, provide sufficient justification to permit governmental access to such records by request or subpoena without prior judicial scrutiny.
tronic surveillance: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)\(^2\) and the Foreign Intelligence Surveillance Act of 1978 (FISA).\(^3\) An examination of these two statutes indicates that Congress acted with the intent and the expectation that all surveillance, including that by pen register, would require authorization by court order. The result in *Smith* ignores this congressional expectation and therefore nullifies congressional intent. In addition, the *Smith* decision has introduced an absurd anomaly into federal law.

### A. Title III

Title III governs wiretapping and bugging by law enforcement officials.\(^4\) Its enactment marked Congress' first affirmative expression regarding both the constitutionality\(^5\) and propriety\(^6\) of electronic surveillance.\(^7\) Under Title III, before "intercepting"\(^8\) either "wire communications"\(^9\) or "oral communications,"\(^10\) law enforcement officials

---

97. Prior to the enactment of Title III, the primary statutory restraint on the use of electronic surveillance in federal criminal investigations was § 605 of the Federal Communications Act of 1934, ch. 652, § 605, 48 Stat. 1103 (1934) (current version at 47 U.S.C. § 605 (1976)). Its terms were prohibitory in nature, providing that "no person" could reveal the existence or content of a communication except under certain limited circumstances. See generally Note, supra note 4, at 1030-42.
99. Id. § 2510(1).
100. Id. § 2510(2).
must obtain a special eavesdropping order.101 The requirements for such a warrant are considerably more stringent than those governing ordinary search warrants.102 Title III directly regulates all federal law enforcement use of wiretapping and bugging103 and authorizes the states to enact similar legislation respecting wiretapping and bugging by state officials, provided that the state legislation is at least as restrictive as Title III.104

101. Surveillance outside the scope of these statutory definitions may be conducted without regard to Title III's requirements. Additionally, an "oral communication" is protected from nonorder interception only if it is uttered by a person exhibiting an expectation of privacy "under circumstances justifying such expectation." 18 U.S.C. § 2510(2) (1976). See S. Rep. No. 1097, 90th Cong., 2d Sess. 90, reprinted in [1968] U.S. CODE CONG. & AD. NEWS 2112, 2178. In contrast, "wire communications" are protected from noncourt authorized surveillance regardless of whether the participants have a reasonable expectation of privacy. 18 U.S.C. § 2510(1) (1976). Thus, even though persons communicating by telegram or party-line telephone are aware that their privacy is vulnerable to telegraph company employees or other party-line subscribers, law enforcement officials must obtain a Title III order before surveillance can be commenced. However, pen register surveillance was expressly excluded from the statutory definition of "intercept." See note 107 infra.

There are two other significant exceptions to Title III's court order requirement. First, no order is required to authorize interception if a party to the conversation himself records or transmits it or gives prior permission for others to do so. 18 U.S.C. § 2511(2)(c), (d) (1976). Second, communications common carriers are authorized to intercept communications for valid business purposes. Id. § 2511(2)(a)(i). See notes 4-6 and accompanying text supra.

102. Only certain serious crimes may be investigated by electronic surveillance, 18 U.S.C. § 2516(1), (2) (1976), and Title III sets forth exacting requirements. The Title III application and order must identify the persons (if known) whose communications are to be intercepted, id. § 2518(1)(b)(iv), (4)(a), must specify the facilities or location subject to surveillance, id. § 2518(1)(b)(ii), (4)(b), and must specify the offense and describe the communications sought. Id. § 2518(1)(b)(i), (iii), (4)(c). Moreover, there must be probable cause to believe that evidence of the specified crimes will be obtained through such interceptions. Id. § 2518(3)(a), (b), (d). The application must also demonstrate that ordinary investigative procedures have not been and will not be adequate to accomplish the goals of the surveillance. Id. § 2518(1)(c), (3)(c). Warrants must be of limited duration with a maximum of 30 days, id. § 2518(4)(e), (5), and interceptions must terminate when the authorized objective has been attained. Id. § 2518(5).

Importantly, surveillance must be conducted so as to "minimize" the interception of communications unrelated to the purposes of the surveillance. Id. § 2518(5). See generally Fishman, The "Minimization Requirement" in Electronic Surveillance: Title III, The Fourth Amendment, and the Dread Scott Decision, 28 AM. U.L. REV. 315 (1979); 28 CATH. U.L. REV. 143 (1978). Title III also regulates how recordings of interceptions are to be maintained, 18 U.S.C. § 2518(8)(a) (1976); restricts the disclosure and use of intercepted communications and derivative evidence, id. § 2517; and specifies how, when, and to whom notice of interception is to be served. Id. § 2518(8)(d), (9). In addition, Title III contains an exclusionary rule, id. § 2515, and specifies grounds for suppression of intercepted communications. Id. § 2518(10)(a). See generally C. Fishman, supra note 11.

103. On the federal level, applications for eavesdropping orders must be authorized by the Attorney General or a specially designated assistant attorney general. 18 U.S.C. § 2516(1) (1976). State applications must be authorized by the principal prosecuting attorney of a state or political subdivision. Id. § 2516(2).

104. See note 44 supra.
Additionally, surveillance conducted in violation of Title III may give rise to criminal penalties, and Title III created a civil cause of action for persons whose privacy rights are violated by unlawful surveillance.

Title III's legislative history indicates clearly that pen register surveillance does not constitute "interception" of a "wire communication" within the meaning of the statute. Thus, law enforcement officials need not

106. Id. § 2520. This section also provides that "A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or any other law." Id.
107. [18 U.S.C. § 2510(4) (1976)] defines "intercept" to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. An examination of telephone company records by law enforcement agents in the regular course of their duties would be lawful because it would not be an "interception." The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register," for example, would be permissible. But see United States v. Dote, 371 F.2d 176 (7th Cir. 1966). The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication.


The reference to Dote and the use of the signal "but see" are somewhat confusing. In Dote, a telephone company acting at government request installed a pen register on a telephone located in a gambling "wireroom." The register revealed that calls were being placed to the defendants' telephones, and the government used this information to obtain evidence leading to the defendants' indictment for gambling offenses. The issue in Dote was whether use of the pen register constituted an "interception or divulgence" of a wire communication in violation of 47 U.S.C. § 605 (1934). The government argued that the telephone company was the "intended recipient" of the electronic signals created when the wireroom phone was dialed, and that no "interception" occurs when the recipient of a wire communication discloses its content. The Seventh Circuit categorized this argument, which is difficult to distinguish from the reasoning adopted by the Supreme Court in Smith, as a "play on words" which had only "minimal plausibility." 371 F.2d at 180. Since human intervention was not required to connect the wireroom telephone to the numbers that were dialed, the court reasoned it was specious to contend that anyone other than someone at the called telephone was the intended recipient. Further, since the government for all practical purposes knew what types of messages were being sent over the wireroom telephone, use of the pen register revealed the contents of the calls, thereby violating both the sender's and the recipients' (defendants') statutorily protected rights. Id. Finally, the court noted that its decision did not render telephone company use of pen registers for legitimate business purposes unlawful so long as the company had the consent of the individual on whose phone the device was used. Id. at 181.

Although some may find the logic of the Dote decision persuasive, neither its holding nor its dictum survived the enactment of Title III. Title III deleted wire communications from the purview of § 605 of the Federal Communications Act, the statute applied in Dote. See 47 U.S.C. § 605 (1934), as amended by Pub. L. No. 90-351, § 803, 82 Stat. 223 (1968) (current version at 47 U.S.C. § 605 (1976)). Further, Title III specifically excludes all normal telephone company practices (including use of pen registers) from the restrictions and prohibitions of Title III. 18 U.S.C. § 2511(2)(a)(i) (1976). See note 6 supra. Thus, Title III has
obtain a Title III order before employing a pen register.\textsuperscript{108} Both Title III and its legislative history are silent, however, as to whether Congress in 1968 thought it necessary under the fourth amendment for law enforcement officials to obtain a standard search warrant before requesting a telephone company to install a pen register for investigative purposes.\textsuperscript{109}

B. The Foreign Intelligence Surveillance Act

The second federal statute regulating electronic surveillance is the Foreign Intelligence Surveillance Act of 1978.\textsuperscript{110} This Act governs the use of "electronic surveillance"\textsuperscript{111} within the United States\textsuperscript{112} by national security officials to acquire "foreign intelligence information."\textsuperscript{113} Of particular


\textsuperscript{108} See generally Note, Circumventing Title III: The Use of Pen Register Surveillance in Law Enforcement, 1977 DUKE L.J. 751.

\textsuperscript{109} Amendments to Title III enacted as part of FISA and indicative of congressional intent in 1978 are discussed in text accompanying notes 124-43 infra.


\textsuperscript{111} FISA's definition of "electronic surveillance" incorporates all forms of surveillance governed by Title III as well as several types not regulated by Title III, including the use of a pen register. 50 U.S.C. § 1801(f) (Supp. II 1978). See notes 98-103 and accompanying text supra.


\textsuperscript{113} Only federal, not state, officials may conduct FISA surveillance. 50 U.S.C. §§ 1802, 1804 (Supp. II 1978). "Foreign intelligence information" is information relating to the nation's ability to protect against actual or potential attack or other hostile acts, sabotage, international terrorism, and clandestine intelligence activities of foreign agents within the United States, information relating to national defense and security, and information relating to the conduct of foreign affairs, \textit{id.} § 1801(e). Activities protected by the first amendment, however, cannot constitute foreign intelligence information. \textit{Id.} § 1805(a)(3)(A).

FISA permits surveillance under circumstances prohibited by Title III. For example, FISA authorizes surveillance when there is no probable cause to believe that criminal activity is involved so long as there is probable cause to believe that foreign intelligence information will be obtained and other enumerated circumstances exist. \textit{Id.} §§ 1801(e), 1802. See S. REP. No. 701, 95th Cong., 2d Sess. 10-12, reprinted in [1978] U.S. CODE CONG. & AD. NEWS 3973, 3979-80 (Intelligence Committee). See generally 50 U.S.C. § 1802(a) (Supp. II 1978); C. FISHMAN, supra note 11, §§ 353, 359-365 (Supp. 1979). In other respects, however,
importance here is that FISA requires the issuance of an order before national security officials may conduct "electronic surveillance" to acquire the "contents" of a "wire communication."\(^{114}\)

The legislative history of FISA's definitions demonstrates that a pen register acquires the "contents" of a "wire communication." Commenting on FISA's definition of "contents," the House Select Intelligence Committee observed that such definition is meant to assure that the scope of the bill is sufficient to protect legitimate privacy interests. Inasmuch as three of the four definitions of electronic surveillance, which in fact define the coverage of [FISA], turn on the acquisition of "contents," it is necessary to assure that devices such as pen registers are included.\(^{116}\)

FISA is more restrictive than Title III. For example, FISA's restrictions concerning the retention and dissemination of information obtained from electronic surveillance are more rigid. 50 U.S.C. §§ 1801(1)(b), 1802(a)(1), 1804(a)(5), 1805(a)(5), (b)(1)(F) (Supp. II 1978). See generally C. FISHMAN, supra note 11, § 368 (Supp. 1979).

114. "Contents" is defined as "any information concerning the identity of the parties to [a] communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n) (Supp. II 1978).


116. H.R. REP. No. 1283, 95th Cong., 2d Sess. 67 (1978) (emphasis supplied). The FISA definition of "contents" is identical to that contained in Title III, 18 U.S.C. § 2510(8) (1976). In United States v. New York Tel. Co., 434 U.S. 159 (1977), the Supreme Court held that use of a pen register does not constitute an "interception" under Title III because a pen register does not acquire the "contents" of a "wire communication" as those terms are defined in Title III. Id. at 166-67. The House Select Intelligence Committee labeled this latter analysis "gratuitous" in light of the exclusion of pen registers from Title III's definition of "intercept." H.R. REP. No. 1283, 95th Cong., 2d Sess. 67 n.33 (1978). The Committee emphasized:

It is the intent of this committee that pen registers do acquire "contents" of "wire communications" as those terms are defined in [FISA]. The term "contents" specifically mentions the identity of parties and "identity" includes a person's phone number, which can as effectively identify him as the mention of his name. Moreover, the definition of "contents" includes information concerning the "existence" of a communication. When a person dials another's telephone number, whether or not the other person answers the phone, this is a communication under this bill. This is especially true in the intelligence field where signals to a spy may be conveyed merely by having the phone ring a designated number of times. The fact that the target of the pen registers has attempted to communicate with another person at a particular phone is information concerning the "existence" of the communication.
Since under FISA a pen register acquires the "contents" of a "wire communication," use of a pen register constitutes "electronic surveillance." Thus, national security officials must first obtain a court order before conducting pen register surveillance. Moreover, FISA's legisla-

Id.


118. The separate reports prepared by the House Select Committee on Intelligence and the Senate Intelligence Committee both contain the following definitional discussions of "electronic surveillance" respecting wire communications:

The surveillance covered by [50 U.S.C. § 1801(f)(2) (Supp. II 1978)] is not limited to the acquisition of the oral, or verbal contents of a wire communication. It includes the acquisition of any other contents of the communication, for example, where computerized data is transmitted by wire. Therefore, it includes any form of "pen register" or "touch-tone decoder" device which is used to acquire, from the contents of a wire communication, the identities or locations of the parties to the communication. Examination of telephone billing records in documentary form is not covered. The committee is concerned about the need to protect that privacy of such confidential records of the provision of telecommunications services, but does not believe that [FISA] is the appropriate measure in which to do so.

S. REP. NO. 701, 95th Cong., 2d Sess. 35-36, reprinted in [1978] U.S. CODE CONG. & AD. NEWS 3973, 4004-05; H.R. REP. NO. 1283, 95th Cong., 2d Sess. 51 (1978). This language could be interpreted as including the use of pen registers within the definition of "electronic surveillance" only when the register is used in conjunction with surveillance acquiring what is actually said during a telephone conversation. However, any ambiguity in this regard is resolved by FISA's definition of "contents" and that term's legislative history. See notes 114-16 and accompanying text supra.

119. If probable cause exists that pen register surveillance will reveal evidence of specific crimes, national security officials could choose between a FISA order and an ordinary search warrant to authorize the surveillance. FISA's procedures apply only when such officials either cannot or choose not to employ other legal surveillance options. A FISA order is far more difficult to obtain than a normal search warrant, and FISA imposes restrictions on the retention, use, and disclosure of the information obtained that are far more restrictive than statutes governing other types of warrants. See 50 U.S.C. §§ 1804-1806 (Supp. II 1978); C. Fishman, supra note 11, §§ 359-370 (Supp. 1979). Compare Fed. R. CRIM. P. 41, gov-
tive history mandates the imposition of a court order requirement whether national security officials use a pen register with the consent, over the objection, or with the knowledge of the telephone company.  

V. Smith v. Maryland and the Nullification of Congressional Intent

The Court in Smith refused to attach constitutional significance to the distinction between long distance calls, records of which are regularly kept by the telephone company, and local calls, records of which are normally nonexistent. Recognition of this distinction, the Court reasoned, would "make a crazy quilt of the Fourth Amendment. . . ." Ironically, it is the Smith decision that makes a crazy quilt of federal law regarding pen registers. It is incongruous that national security officials must obtain a special surveillance warrant before using a pen register to investigate threats to national security while a local police officer with the informal cooperation of the telephone company may, without any sort of court order, employ a pen register for any reason at all.

This result is contrary to what Congress intended. When FISA was enacted, Congress proceeded with the understanding that a search warrant or other court order is generally required to authorize law enforcement use of

1980] Pen Registers and Privacy 581

earning search warrants, with 18 U.S.C. §§ 2517, 2518 (1976). Nevertheless, for several reasons, national security officials are likely to rely almost exclusively on the procedures mandated in FISA. FISA authorizes issuance of an order authorizing electronic surveillance even where no criminal conduct is suspected so long as there is probable cause to believe that "foreign intelligence information" will be obtained. 50 U.S.C. § 1805(a)(3)(A)-(B) (Supp. II 1978). See C. Fishman, supra note 11, §§ 359-365 (Supp. 1979). Moreover, a FISA order may authorize surveillance for up to one year, depending upon the identity of the target. 50 U.S.C. § 1805(d)(1) (Supp. II 1978). See C. Fishman, supra note 11, §§ 363-365 (Supp. 1979). Unless the government decides to use FISA-obtained evidence in a criminal proceeding against someone aggrieved by FISA surveillance, the government need never disclose the occurrence of such surveillance. 50 U.S.C. § 1806(c)-(f) (Supp. II 1978). See C. Fishman, supra note 11, §§ 371-372 (Supp. 1979). Because of these procedural advantages and enhanced confidentiality, national security officials probably will prefer a FISA order even if the grounds for a regular search warrant exist.

120. FISA authorizes a telephone company to cooperate with national security officials in the conduct of electronic surveillance only if such cooperation is directed by court order (or by certification of the Attorney General that no warrant or court order is required by law, an exception not relevant to pen registers). Further, a telephone company is liable for civil damages if it cooperates with national security officials without being directed to do so by court order. See Pub. L. No. 95-551, §§ 201(a), 92 Stat. 1796-97 (1978), amending 18 U.S.C. § 2511(2)(a)(ii) (1976). The implications of this provision are discussed in notes 143-49 and accompanying text infra.

121. 99 S. Ct. at 2582-83. See notes 76-81 and accompanying text supra.

122. See notes 110-20 and accompanying text supra.
pen registers.\textsuperscript{123} This is demonstrated by FISA’s criminal and civil liability provisions and by the conforming amendments to Title III, enacted as part of FISA.\textsuperscript{124} Furthermore, there is strong circumstantial evidence that Congress also assumed that \textit{all} law enforcement use of pen registers was subject to the fourth amendment’s warrant requirement, even if the surveillance was conducted by the telephone company at the request of the police. This evidence will be developed by examining a substantive amendment to Title III enacted in FISA, which regulates telephone company cooperation with official wiretapping.\textsuperscript{125}

Before examining FISA’s civil and criminal liability provisions and its amendments to Title III, a preliminary comment is in order. In these statutory provisions and in the congressional reports discussing them, the phrase “search warrant or court order” appears several times. Yet, nowhere did Congress specify what type of court order, other than a search warrant, was contemplated. This lack of specificity has assumed a perhaps unintended significance in light of \textit{Smith}.\textsuperscript{126}

\textbf{A. Pen Register Surveillance in General}

\textbf{1. FISA’s Civil and Criminal Liability Provisions}

FISA imposes civil and criminal liability on any person who “engages in electronic surveillance under color of law except as authorized by statute” or knowingly discloses or uses information obtained through illegal electronic surveillance.\textsuperscript{127} It is a defense to both criminal prosecution and civil liability, however, “that the defendant was a law enforcement or investigatory officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search war-

\textsuperscript{123} This understanding is undisturbed by \textit{Smith}, for the Court held only that a warrant is unnecessary if the surveillance is conducted by a telephone company at police request. Had the police employed the pen register themselves, without telephone company involvement, this would have constituted an illegal search and seizure. See text accompanying note 64 supra.

\textsuperscript{124} See notes 127-33 and accompanying text infra.

\textsuperscript{125} See notes 134-43 and accompanying text infra.

\textsuperscript{126} See notes 168-83 and accompanying text infra.

\textsuperscript{127} 50 U.S.C. § 1809(a) (Supp. II 1978) (criminal liability); \textit{id.} § 1810 (civil liability) (Supp. II 1978). These provisions are similar to Title III’s. 18 U.S.C. §§ 2511(1) (criminal penalties), 2520 (civil liability) (1976). The conference committee that reconciled the House and Senate drafts of FISA “agree[d] that the criminal penalties for intelligence agents under [FISA] should be essentially the same as for law enforcement officers under [Title III]” and that “the civil liability of intelligence agents under [FISA] should coincide with the criminal liability.” H.R. CONF. REP. No. 1720, 95th Cong., 2d Sess. 33-34, \textit{reprinted in} [1978] U.S. CODE CONG. & AD. NEWS 4048, 4062-63.
rant or court order of a court of competent jurisdiction." 128 Commenting on these provisions, the House Select Intelligence Committee noted:

Since certain technical activities — such as the use of a pen register — fall within the definition of electronic surveillance under [FISA], but not within the definition of [interception of] wire or oral communications under [Title III], [FISA] provides an affirmative defense to a law enforcement or investigative officer who engages in such activity for law enforcement purposes in the course of his official duties, pursuant to a search warrant or court order. 129

Thus, federal agents — law enforcement officials as well as national security officials — who use a pen register without a search warrant or court order are subject to FISA's civil and criminal provisions. 130 Congress


129. H.R. REP. No. 1283, 95th Cong., 2d Sess. 96 (1978) (commenting on 50 U.S.C. § 1809(b) (Supp. II 1978), the good faith defense provision) (emphasis supplied). At the end of the quoted passage, the report cites United States v. New York Tel. Co., 434 U.S. 159, 165-68 (1977), in which the Court held that a court order issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, which governs the issuance and execution of search warrants, sufficed to authorize the use of a pen register and to compel a telephone company to provide the government with assistance.

The Senate Intelligence and Judiciary Committees' reports on S. 1566, the Senate version of FISA, contain a perplexing ambiguity. Each report comments that FISA does not apply to the use of pen registers for law enforcement purposes and then, in identical language, continues: "In such cases criminal penalties will not attach simply because the Government fails to follow the procedures in [FISA] (such penalties may, of course, attach if the surveillance is commenced without a search warrant or in violation of a court order)." S. REP. No. 701, 95th Cong., 2d Sess. 68, reprinted in [1978] U.S. CODE CONG. & AD. NEWS 4037; S. REP. No. 604, 95th Cong., 2d Sess. 61, reprinted in [1978] U.S. CODE CONG. & AD. NEWS 3963 (emphasis supplied). The use of the word "may," the primary meaning of which is "might," is perplexing. Certainly the Senate committees that drafted and favorably reported S. 1566 must have known whether they intended such surveillance to come within the scope of their bill's criminal provision. Fortunately, the ambiguity in the Senate reports is of no consequence because the Conference Committee adopted, with some modification, the House version of the criminal penalty provision. See H.R. CONF. REP. No. 1720, 95th Cong., 2d Sess. 33, reprinted in [1978] U.S. CODE CONG. & AD. NEWS 4048, 4062. Since the House Select Intelligence Committee Report does not contain similar ambiguities, federal law enforcement officials who conduct pen register surveillance without a warrant or court order are liable under FISA's criminal provisions.

130. Commenting on nonwarrant pen register surveillance by state officials, the House Select Intelligence Committee stated: "While such action may be unconstitutional, it is not made a [federal] crime by [Title III] and should not be by [FISA]." H.R. REP. No. 1283, 95th Cong., 2d Sess. 97 (1978). This exclusion of state officials from FISA's criminal provision has assumed a somewhat greater significance than Congress probably intended. Since the scope of FISA's criminal and civil liability provisions is identical, see note 127 supra, state officials are also exempt from the latter. By so exempting state officials, Congress has left a loophole in the overall regulation of pen register surveillance. See notes 146-50 and accompanying text infra.
would not have so provided had it not understood that law enforcement
use of pen registers was already subject to the fourth amendment warrant
requirement.

2. The "Exclusive Means" Provision

Several amendments to Title III were enacted as part of FISA. One
amendment added a provision to Title III mandating that the "procedures
in [Title III and FISA] shall be the exclusive means by which electronic
surveillance as defined in [50 U.S.C. § 1801], and the interception of
domestic wire and oral communications may be conducted." Commenting
on this provision, the House Select Intelligence Committee noted:

[T]he use of pen registers and similar devices for law enforce-
ment purposes is not covered by [Title III] or [FISA] and new
subsection (f) [of 18 U.S.C. § 2511(2)] is not intended to prohibit
it. Rather, . . . the "procedures" referred to in subsection (f) in-
clude acquiring a court order for such activity. It is the Com-
mittee's intent that neither this nor any other provision of the
legislation have any effect on the holding in United States v. New
York Tel. Co., 434 U.S. 159 (1977), that rule 41 of the Federal
Rules of Criminal Procedure empowers federal judges to author-
ize the installation of pen registers for law enforcement pur-
poses.

Rule 41 of the Federal Rules of Criminal Procedure regulates the issu-
ance, execution, and litigation of search warrants. Thus, FISA did not
expressly regulate law enforcement use of pen registers because Congress
understood that a search warrant or other court order was already required
to authorize such use.

B. The "Directed Assistance" Provision

A second significant FISA amendment to Title III regulates telephone

---

Stat. 1796 (codified at 18 U.S.C. §§ 2510-2520 (Supp. II 1978)). Most of these amendments
are technical in nature, designed to assure that the language of Title III reflects the enact-
ment of FISA. Thus, the words "under this chapter," "intercepted under this chapter," and
"intercepted pursuant to this chapter," were added to various sections of Title III. Pub. L.
No. 95-511, § 201(d)-(h), 92 Stat. 1797-98 (codified at 18 U.S.C. §§ 2518, 2519 (Supp. II
1978)). Additionally, 18 U.S.C. § 2511(3) (1976), which held Title III inapplicable to wire-
tapping and eavesdropping conducted for national security reasons, was repealed since that
provision had been superseded by FISA. See Pub. L. No. 95-511, § 201(c), 92 Stat. 1797
(1978).


133. H.R. Rep. No. 1283, 95th Cong., 2d Sess. 100 n.54 (1978) (Select Intelligence Com-
mittee). The New York Tel. Co. case is discussed at notes 11-14 and accompanying text
supra; notes 175-83 and accompanying text infra.
company cooperation with governmental surveillance efforts. This amendment strongly suggests that Congress acted with the belief that the fourth amendment required law enforcement officials to obtain a search warrant before using pen registers even where, as in Smith, the telephone company voluntarily installed the device at the request of the police.

Prior to FISA, Title III placed no explicit limitations on telephone company cooperation with law enforcement officials. Rather, the statute merely provided that it was "not unlawful" under Title III for a communications common carrier to provide "information, facilities, or technical assistance" to a law enforcement official who was authorized by a Title III or equivalent state court order to intercept a wire or oral communication. Cooperation in situations not involving actual interceptions of communications, including the use of pen registers, was completely unregulated.

As amended by FISA, Title III now "authorizes" a communications common carrier "to provide information, facilities, or technical assistance to persons authorized by law to intercept wire or oral communications [as defined in Title III] or to conduct electronic surveillance [as defined in FISA]" only if the carrier has been provided with "a court order directing such assistance signed by the authorizing judge" specifying the nature and duration of the cooperation required. Moreover, a violation of this provision "by a communications common carrier or an officer, employee or agent thereof, shall render the carrier liable for the civil damages provided

---

135. An implicit limitation is contained in 18 U.S.C. § 2511(1) (1976), which imposes criminal liability for illegal interceptions of communications. Except where specifically provided in Title III, "any person" who intercepts or who discloses or uses the contents of an intercepted wire or oral communication, or who endeavors or procures another to do so, may be punished by a fine and imprisonment. Id. Moreover, "any person" who unlawfully intercepts communications is also subject to civil liability. Id. § 2520. The statutory definition of "person" clearly includes telephone companies. See id. § 2510(6). Thus, a telephone company would be both civilly and criminally liable if it installed a wiretap on someone's telephone at the request of the police in the absence of a court order. Still, these provisions do not focus on the unique role a telephone company often plays in official wiretapping and bugging. Further, they apply only when there has been an "interception." In addition, 18 U.S.C. § 2511(2)(a)(i) (1976) expressly permits communications common carriers to intercept, disclose, or use wire communications where such interception, disclosure, or use "is a necessary incident" to the service it provides or is necessary to protect the carrier's rights or property, and if incriminating evidence is revealed during such interceptions, such evidence may be disclosed to and used by law enforcement officials. See notes 6-9 and accompanying text supra.
137. See notes 107-08 and accompanying text supra.
This amendment does not impose additional duties upon telephone companies to cooperate with law enforcement officials.\textsuperscript{140} To the contrary, the amendment to 18 U.S.C. § 2511(2)(a)(ii) expressly requires a warrant or other court order before a telephone company is "authorized" to provide such assistance.\textsuperscript{141} Since this provision is clearly applicable to pen register surveillance conducted by national security officials to acquire foreign intelligence information,\textsuperscript{142} it is inconceivable that Congress would have at the same time intended to permit a telephone company to install a pen register at the request of law enforcement officials absent a court order of any kind.\textsuperscript{143} This amendment, therefore, demonstrates that Congress

\textsuperscript{139} Id. 18 U.S.C. § 2520 (1976) created a civil cause of action permitting recovery of actual or liquidated damages, punitive damages, attorneys' fees, and litigation costs. However, a good faith reliance on a court order or legislative authorization constitutes a complete defense to both civil and criminal actions. \textit{Id.}

\textsuperscript{140} Even prior to the amendment of 18 U.S.C. § 2511(2)(a)(ii) (1976), another section of Title III authorized a judge to include within a Title III warrant an order directing communications common carriers, landlords, and the like to furnish "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively . . . ." \textit{Id.} § 2518(4). Thus, FISA's amendment of 18 U.S.C. § 2511(2)(a)(ii) (1976) did not impose additional duties of cooperation upon telephone companies because "the nature and scope" of the assistance provided for by that amendment "is intended to be identical to that which may be directed under § 2518(4)." S. REP. NO. 701, 95th Cong., 2d Sess. 69, \textit{reprinted in} [1978] U.S. CODE CONG. & AD. NEWS 3973, 4038.

\textsuperscript{141} Before the communications common carrier may provide such information or assistance, whether under Title III or FISA, the Government agent must furnish the carrier with an order signed by the court. "The conference substitute adopts . . . the Senate provision imposing civil liability upon a common carrier which provides assistance without a court order." H.R. CONF. REP. NO. 1720, 95th Cong., 2d Sess. 35, \textit{reprinted in} [1978] U.S. CODE CONG. & AD. NEWS 4048, 4064.

There is one exception to the court order requirement. In emergency situations requiring interception or surveillance before a court order can be obtained, 18 U.S.C. § 2511(2)(a)(ii) (Supp. II 1978) mandates cooperation if the telephone company has received a written certification from the Attorney General (or, in the case of surveillance by state officials, a state prosecutor) indicating "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." \textit{Id.} If such emergency surveillance is conducted, the government must obtain an order approving the surveillance within 24 hours for FISA surveillance, 50 U.S.C. § 1805(e) (Supp. II 1978), or 48 hours for law enforcement surveillance. 18 U.S.C. § 2518(7) (1976). A telephone company is also prohibited from revealing the existence of Title III interceptions or FISA surveillance unless compelled by legal process, and then only after notice to the Attorney General or state official who obtained the original court order authorizing the surveillance. 18 U.S.C. § 2511(2)(a)(ii) (Supp. II 1978).

\textsuperscript{142} \textit{See} notes 114-20 and accompanying text \textit{supra}.

\textsuperscript{143} That Congress did not intend such a result is illustrated by the gaping loophole it would create in FISA. If, for example, an F.B.I. agent assigned to national security matters wants to use a pen register, he must first obtain a FISA order. If the agent lacks the grounds for such an order (or simply wants to avoid the trouble of complying with the statute), the
believed that the fourth amendment required a search warrant or other court order to authorize law enforcement use of a pen register or derivative evidence even where, as in *Smith*, the telephone company was eager and willing to "provide information, facilities or technical assistance."

C. The Gap in FISA

The result intended by FISA's amendment to Title III can be stated simply. First, national security and federal law enforcement officials would incur both civil and criminal liability if they conducted pen register surveillance without a warrant or other court order issued pursuant to FISA if sought for national security purposes or issued pursuant to the fourth amendment and Federal Rule of Criminal Procedure 41 if sought for law enforcement purposes. Second, a telephone company that conducted such surveillance on behalf of federal or state law enforcement officials in the absence of a warrant or other court order would be civilly liable to the subscriber whose privacy was invaded. As a practical matter, therefore, no such surveillance could be conducted without a court order.

Concededly, Congress left a loophole in this scheme. Pen register surveillance by state law enforcement officials is not regulated by either Title III or FISA. Furthermore, a literal reading of the "directed assistance" provision indicates that a telephone company would not be civilly liable if it conducted such surveillance at the request of state officials in the absence of a court order. Prior to *Smith v. Maryland*, however, this loophole was

---

144. See notes 127-30 and accompanying text *supra.*
145. See notes 138-39 and accompanying text *supra.* Although Congress chose to exempt state officials from FISA's criminal and civil liability provisions, see note 130 *supra,* there is nothing in FISA's legislative history suggesting that Congress intended to permit a telephone company, in the absence of a warrant, to do for state officials what the amendment to 18 U.S.C. § 2511(2)(a)(ii) (1976) prohibits a company from doing for national security officials.
146. Pen register surveillance is not regulated by Title III, see notes 107-08 *supra,* and FISA's criminal and civil liability provisions are inapplicable to state officials. See notes 113, 130 *supra.* Thus, pen register surveillance by state officials is unregulated by FISA as well as by Title III. Nevertheless, absent telephone company cooperation, state officials are unlikely to conduct such surveillance without a warrant. To do so would require either an illegal trespass onto the suspect's premises or an unauthorized use of telephone company facilities.
147. Telephone company assistance to a state official conducting pen register surveillance would constitute neither an "interception" under Title III nor "electronic surveillance" under FISA. See note 146 *supra.* Thus, 18 U.S.C. § 2511(2)(a)(iii) (Supp. II 1978) would not be applicable to such assistance.
seemingly insignificant. If such surveillance violates the fourth amendment, as Congress apparently believed,\textsuperscript{148} evidence derived from the pen register would be suppressed. Thus, state officials would have little incentive to seek telephone company cooperation absent a warrant. But the holding in \textit{Smith v. Maryland}, that if the telephone company agrees to conduct the surveillance, law enforcement use of a pen register is not a fourth amendment "search" and therefore need not be authorized by a search warrant,\textsuperscript{149} has confounded congressional expectations and has partially nullified Congress' intent to subject all governmental pen register surveillance, state as well as federal, to a warrant requirement. As a result of \textit{Smith}, if the telephone company cooperates, state law enforcement use of pen registers is currently subject to no federal constitutional or legislative restraints.\textsuperscript{150}

This is not to suggest that the Supreme Court erred in not applying FISA to the facts in \textit{Smith}. The use of the pen register in \textit{Smith} preceded the enactment of FISA by several years. Still, it is curious that none of the opinions in \textit{Smith} contain any mention of FISA. In the past, the Court has often looked to existing federal legislation in assessing the constitutionality of federal or state law enforcement techniques and procedures.\textsuperscript{151} Further, one cannot but wonder whether the Court considered the impact its decision might have on Congress' effort in FISA to subject all law enforcement use of pen registers to a warrant requirement. The absence of any reference to FISA in the dissenting opinions is particularly puzzling. Both dissents chastise the majority for failing to consider whether the type of nonwarrant surveillance conducted in \textit{Smith} is one of the risks a person "should be forced to assume in a free and open society."\textsuperscript{152} Significantly, the language and legislative history of FISA demonstrate that Congress

\textsuperscript{148} See notes 123-43 and accompanying text supra.
\textsuperscript{149} See text accompanying note 78 supra.
\textsuperscript{150} The \textit{Smith} decision does not appear to effect the congressional scheme to impose a court order requirement on all federal use of pen registers.
\textsuperscript{151} There are numerous examples. In United States v. Watson, 423 U.S. 411, 415 (1976), the Court held that it was constitutional for federal agents to arrest a defendant without a warrant, despite ample opportunity to obtain a warrant prior to the arrest. The Court cited 18 U.S.C. § 3061(a)(3) (1976), which authorizes such arrests, as persuasive authority. In United States v. White, 401 U.S. 745, 753 (1971), the Court held that it was constitutional for federal agents to equip an informer with a transmitter and thereby overhear his conversation with a suspect without first obtaining a warrant. In upholding the constitutionality of the surveillance, which had been conducted several years prior to enactment of Title III, the Court cited Title III's consensual interception provision as persuasive authority.
\textsuperscript{152} 99 S. Ct. at 2588 (Marshall, J., dissenting). See id. at 2583-84 (Stewart, J., dissenting).
considered that very question and concluded that such surveillance should be unlawful unless authorized by a warrant. Logically, one might have expected the dissenting Justices to cite FISA as persuasive authority supporting their viewpoint. Thus, the absence of any reference to FISA gives rise to the question whether the litigants or the Court were aware of the statute at all.

VI. IMMEDIATE IMPLICATIONS

Although the Supreme Court's reasoning in *Smith v. Maryland* has disturbing long-range implications for personal privacy and has made a hash of congressional intent, its immediate impact is uncertain. This section will discuss the probable implications of the decision respecting federal and state use of pen registers.

A. Federal Implications

1. The FISA "Court Order" Requirement

Federal law enforcement use of pen registers constitutes "electronic surveillance" as defined by FISA. Such surveillance is unlawful and exposes the agents and cooperating telephone company to criminal or civil liability unless it is authorized by a "search warrant or court order." Thus, while the *Smith* decision removed any constitutional search warrant requirement, FISA still requires a "court order" to authorize such surveillance. Nowhere in FISA's statutory language or legislative history did Congress specify what type of "court order," other than a search warrant, was contemplated. Nevertheless, several aspects of FISA support the inference that the phrase "search warrant or court order" was intended to mean "search warrant, FISA electronic surveillance order or Title III interception order."

First, FISA's central purpose is to specify when and how an "order approving electronic surveillance" may be obtained, how evidence derived from such court order may be used, and how suppression issues respecting

153. FISA was not mentioned during oral argument before the Supreme Court. The only reference to FISA appearing anywhere in the *Smith* record is a passing reference in petitioner's brief, citing FISA-related hearings as evidence of congressional concern for privacy. Brief for Petitioner at 19-20, *Smith v. Maryland*, 99 S. Ct. 2577 (1979).

154. See notes 116-18 and accompanying text supra.

155. See notes 127-30, 133 and accompanying text supra. FISA was placed in title 50 (War and National Defense) of the United States Code rather than title 18 (Crimes and Criminal Procedure) to emphasize that FISA was not intended to govern law enforcement procedures. *See H.R. REP. No. 1283, 95th Cong., 2d Sess. 28 (1978) (Select Intelligence Committee).* Nevertheless, FISA's definition of "electronic surveillance," and its criminal liability provision, renders, the statute applicable to federal law enforcement use of pen registers.
the order are to be litigated.\textsuperscript{156} Title III's primary focus respecting an "order authorizing the interception of a wire or oral communication" is similar.\textsuperscript{157} Therefore, it is reasonable to infer that, as used in FISA, the term "court order" refers exclusively to an electronic surveillance order, and that, as used in Title III, "court order" refers exclusively to an interception order, unless a contrary meaning can be derived from the context of the statutes or their legislative history.\textsuperscript{158}

Second, FISA's statutory defense to a civil or criminal charge of illegal electronic surveillance is that the surveillance was conducted "pursuant to a search warrant or court order of a court of competent jurisdiction."\textsuperscript{159} FISA does not define the term "court of competent jurisdiction." However, Title III uses a similar term, "judge of competent jurisdiction," to define those judges authorized by Title III or corresponding state statutes to issue wiretapping or bugging orders.\textsuperscript{160} If FISA's use of the term "court of competent jurisdiction" was intended to mean "judge of competent jurisdiction," as defined in Title III, then the phrase "search warrant or court order of a court of competent jurisdiction" appears to mean "search war-

\textsuperscript{156} FISA permits electronic surveillance without a court order only under narrow circumstances. 50 U.S.C § 1802 (Supp. II 1978). The Act also provides for the establishment of a special court to receive applications for electronic surveillance orders, \textit{id.} § 1803, and specifies what the application for such an order must contain. \textit{id.} § 1804. Additionally, FISA enumerates what the order must contain, when it may be issued, and how it is to be executed. \textit{id.} § 1805. Congressional oversight of FISA-authorized electronic surveillance is built into the statute, \textit{id.} §§ 1807-1880, and persons may be civilly and criminally liable for conducting electronic surveillance except pursuant to a "search warrant or court order." \textit{id.} §§ 1809-1810. Concerning FISA's penalty provisions, see notes 159-65 and accompanying text \textit{infra}.

\textsuperscript{157} Although certain types of interceptions are exempted from the court order requirement, it is a crime to intercept communications unless such interception is authorized by Title III. 18 U.S.C. § 2511 (1976). Title III regulates the manufacture of interception devices, \textit{id.} § 2512, and authorizes their confiscation. \textit{id.} § 2513. Moreover, Title III mandates the exclusion of evidence derived from illegal interceptions. \textit{id.} § 2515. The statute defines when and by whom an interception order may be sought, \textit{id.} § 2516, and sets out what an interception application and order must contain, how the order is to be executed, who must be notified after the interceptions are terminated, and how suppression issues are to be litigated. \textit{id.} § 2518. Annual reports concerning interception orders are required, \textit{id.} at § 2519, and there is a civil cause of action for those aggrieved by illegal interceptions. \textit{id.} § 2520.


\textsuperscript{159} \textit{See} notes 127-29 and accompanying text \textit{supra}.

\textsuperscript{160} 18 U.S.C. §§ 2510(9), 2518(1), (3) (1976).
rant, FISA electronic surveillance order, or Title III interception order.\textsuperscript{161}

Finally, the "directed assistance" provision, which permits a telephone company to assist in the interception of communications or the conduct of electronic surveillance only if the company has been provided with "a court order directing such assistance signed by the authorizing judge,"\textsuperscript{162} itself provides additional support for the inference that the type of "court order" referred to therein is restricted to FISA electronic surveillance orders, Title III interception orders, or supplemental orders ancillary to a FISA or Title III order. Three aspects of this provision support such an inference. First, Title III employs the term "authorizing judge" to mean the judge who has issued the interception order.\textsuperscript{163} Second, in commenting on the directed assistance provision, the Senate Intelligence Committee noted that the order directing assistance need "not necessarily [be] the same order as authorizes the actual surveillance."\textsuperscript{164} Although this permits the government to obtain telephone company assistance without revealing to it all of the information contained in the Title III interception order, it also implies that there must be a Title III interception order before an order directing assistance can be obtained. Finally, the directed assistance provision allows certain government officials to obtain cooperation without a court order only if the official certifies, in writing, that an emergency exists requiring interceptions or electronic surveillance before a Title

\textsuperscript{161} In the absence of an explicit congressional statement, one should be cautious about inferring an intent to incorporate into FISA the definition of a similar but not identical term contained in Title III. Several factors, however, do provide circumstantial evidence that this was what Congress intended. First, when Congress enacted FISA, it also amended several provisions of Title III. \textit{See} notes 131-43 and accompanying text \textit{supra}. Second, Congress expressly intended FISA’s civil and criminal liability provisions to mirror those of Title III. \textit{See} note 127 \textit{supra}. Congress, therefore, considered FISA and Title III to be coextensive in several important respects. Finally, the Senate draft of FISA, S. 1566, had provided that, except for terms specifically defined in S. 1566, the definitions in Title III respecting the interception of wire and oral communications would apply to FISA as well. \textit{See} S. \textit{Rep. No. 701, 95th Cong., 2d Sess. 16, reprinted in [1978] U.S. \textit{Code Cong. & AD. News} 3973, 3985 (Intelligence Committee). Perhaps, therefore, FISA’s use of the phrase “court of competent jurisdiction” rather than “judge of competent jurisdiction” was simply a clerical error by the Senate committees that drafted S. 1566. When the congressional conferees decided not to incorporate Title III definitions, they may not have realized that they thereby stripped the phrase “court of competent jurisdiction” of any express definition.


\textsuperscript{163} The phrase “authorizing judge” appears in 18 U.S.C. § 2518(5) (1976). \textit{See also id. § 2518(1)(e).}

III or FISA order can be obtained.\textsuperscript{165}

Congress enacted FISA with the understanding that the fourth amendment required a search warrant to authorize pen register surveillance by government officials even if the telephone company was willing to cooperate in the absence of a warrant.\textsuperscript{166} Ironically, if the phrase “search warrant or court order” indeed means “search warrant, FISA electronic surveillance order, or Title III interception order,” then Congress, without realizing it, may have imposed precisely such a requirement, thereby rendering Smith v. Maryland a nullity when applied to federal officials.\textsuperscript{167}

2. The New York Telephone Dictum: Rule 57(b) and the All Writs Act

The counter-argument to the preceding analysis is readily stated. If Congress had intended to permit federal pen register surveillance only when authorized by a search warrant, a Title III interception order, or a FISA electronic surveillance order, it could have said so explicitly. Since it did not, the phrase “search warrant or court order” must mean something else.

It is here that the Smith Court’s reliance on United States v. Miller,\textsuperscript{168} the Bank Secrecy Act case, is particularly significant. The Bank Secrecy Act compels banks to preserve their customers’ bank records in order to ensure their availability to the government.\textsuperscript{169} In Miller, the Court held that, when a customer transacts business with a bank, he assumes the risk that the bank will reveal those records to the government in compliance with a subpoena.\textsuperscript{170} Therefore, the subpoena does not constitute a search, and the customer lacks standing to contest its validity.\textsuperscript{171}

An application of Miller leads to the following analysis. The fourth amendment does not require a search warrant to authorize pen register surveillance when the telephone company cooperates because, by “voluntarily convey[ing] numerical information to the telephone company,” anyone using a telephone “assume[s] the risk that the company would reveal to police the numbers he dialed.”\textsuperscript{172} Although FISA prohibits telephone


\textsuperscript{166} See notes 122-43 and accompanying text supra.

\textsuperscript{167} The implications of Smith for state officials are discussed at notes 184-91 and accompanying text infra.


\textsuperscript{169} See notes 68-69 and accompanying text supra.

\textsuperscript{170} 425 U.S. at 442-43.

\textsuperscript{171} See notes 66-67 and accompanying text supra.

\textsuperscript{172} Smith v. Maryland, 99 S. Ct. at 2582. See note 64 and accompanying text supra.
companies from cooperating with federal officials in the absence of a
"search warrant or court order," the telephone user nevertheless "assumes
the risk" that the company will comply with a court order to provide
whatever assistance is needed to enable the government to discover the
"numerical information" the dialer "voluntarily conveys" to the company.
Logically, the telephone user would not even have standing to contest the
validity of the court order since the order, like the subpoena in Miller, is
not directed at the customer. 173 All the government need do, therefore, is
obtain a court order that is the functional equivalent of a subpoena. 174

In United States v. New York Telephone Co., 175 the Supreme Court held
that a search warrant sufficed to authorize law enforcement pen register
surveillance 176 and that a federal district judge had the authority under the
All Writs Act 177 to issue an order compelling telephone company coopera-
tion. 178 The Court found support for this conclusion in rule 57(b) of the
Federal Rules of Criminal Procedure, which provides: "If no procedure is
specifically prescribed by rule, the court may proceed in any manner not
inconsistent with these rules or with any applicable statute." 179 The Court
commented, however, that "[w]e need not and do not decide whether Rule
57(b) by itself would authorize the issuance of pen register orders." 180

Although this language was dictum in New York Telephone Co., the
Smith decision may have elevated it to black letter law. The Department
of Justice, in any event, regards it as such. It is now that agency's policy
that, when a pen register is sought, the government will apply for a court
order pursuant to rule 57(b) authorizing such surveillance and will simult-
aneously apply for an order pursuant to the All Writs Act compelling the
telephone company to provide the necessary information, facilities, and
assistance. 181

The suggested form for the rule 57(b) application recites only that law
enforcement agents have been engaged in an investigation of specified in-
dividuals for violations of specified crimes, that it is believed that these

---

173. Similarly, in Couch v. United States, 409 U.S. 322, 335-36 (1973), the Court, using
the same assumption of risk rationale, upheld an I.R.S. summons that required Couch's
accountant to produce Couch's financial records. See note 63 supra.
174. As discussed earlier, the analogy between bank records and pen registers is inapt.
See notes 68-84 and accompanying text supra.
176. 434 U.S. at 165-68.
178. 434 U.S. at 168-78.
179. FED. R. CRIM. P. 57(b).
180. 434 U.S. at 170.
181. Memorandum from Assistant Attorney General Philip P. Heymann, Chief of the
Criminal Division, Department of Justice (December 19, 1979).
individuals use the targeted telephone to discuss or conduct criminal activity, and that the installation and use of the pen register may provide further evidence of the crimes being investigated. A showing of probable cause is not required. If the courts are willing to issue such orders then, despite Congress' expectations and intent to the contrary, the government will be able to conduct pen register surveillance almost at will.

B. State Implications

As a result of Smith, state law enforcement use of pen registers is subject to no federal regulation at all. This does not necessarily mean, however, that state officials are not subject to any restrictions. Prior to Smith, some states had insisted on a search warrant, supported by probable cause, to authorize such surveillance. Other states can be expected to do likewise, either by specific legislation or by court interpretation of state constitutional or statutory provisions.

Finally, even on the state level, the holding in Smith applies only to pen register surveillance conducted by the telephone company at police request. It is to the telephone company that a telephone user "convey[s] numerical information," thereby "assum[ing] the risk that the company would reveal" the information to the police. If the police employ a pen register directly, without obtaining telephone company consent and cooperation, the assumption of risk rationale does not apply. Such surveillance would, therefore, constitute an illegal search and seizure and might expose the police to criminal or civil liability under state law.

182. Id.
183. Id.
184. See notes 146-50 and accompanying text supra.
186. In recent years, several state courts have interpreted their own laws and constitutions more restrictively than have federal courts in interpreting analogous federal law. This has been particularly true in such areas as electronic surveillance and search and seizure. See, e.g., People v. Beavers, 393 Mich. 554, 567, 227 N.W.2d 511, 514, cert. denied, 423 U.S. 878 (1975) (state constitution requires a warrant to authorize use of transmitter to monitor consenting informer's conversation with suspect); State v. Opperman, 89 S.D. 25, 247 N.W.2d 673 (S.D. 1976) (state constitution requires suppression of evidence seized in a search that the Supreme Court, in South Dakota v. Opperman, 428 U.S. 364 (1976), had held did not violate the fourth amendment); State ex rel. Arnold v. County Court, 51 Wisc. 2d 434, 187 N.W.2d 354 (1971) (state statute's consensual interception provision, though worded identically to 18 U.S.C. § 2511(2)(c) (1976), interpreted to require a warrant to authorize evidentiary use of such interceptions). See generally 18 CRIM. L. REP. (BNA) 2507 (1976). In addition, it is noteworthy that while Title III authorized states to enact legislation permitting state law enforcement agents to intercept wire and oral communications, 28 states have not done so. See C. Fishman, supra note 11, at 5-6.
Thus, the practical impact of Smith on state use of pen registers may depend upon the attitudes and policies of the nation's telephone companies. When police request pen register surveillance for reasons that coincide with a business purpose for which a company would utilize a pen register on its own initiative, cooperation may be forthcoming. For example, in Smith, the company did at police request what it probably would have done on its own had the recipient of the harassing calls complained directly to the company. As a rule, however, it is unlikely that telephone companies will install pen registers upon police request. In recent years, the nation's telephone companies have resisted cooperating with law enforcement even when directed to do so by court order. Such resistance predated the amendment to Title III that imposes civil liability on a telephone company that provides "information, facilities, or technical assistance" to law enforcement officials unless ordered to so do by a court. That legislation will, in all likelihood, increase telephone company reluctance to conduct pen register surveillance at police request in the absence of a court order.

Thus, despite Smith v. Maryland, state law enforcement officials will be able to conduct pen register surveillance only by obtaining a search warrant or other court order — not because the fourth amendment requires it, not because any statute requires it, not because Congress intended it, since Smith effectively nullified that intent, but because the telephone company insists upon it.

Whether Smith has any significant impact on the state level, therefore, will depend upon whether state courts are willing, without requiring a showing of probable cause, to issue orders similar to those permitted under

188. See note 5 and accompanying text supra.
189. See, e.g., United States v. New York Tel. Co., 434 U.S. 159 (1977) (pen register); Michigan Bell Tel. Co. v. United States, 565 F.2d 385 (6th Cir. 1977) (in-progress trace); United States v. Southwestern Bell Tel. Co., 546 F.2d 243 (8th Cir. 1976) (pen register); Application of United States, 427 F.2d 639 (9th Cir. 1970) (Title III warrant); Application of United States, 458 F. Supp. 1174 (W.D. Pa. 1978) (pen register); Re In Progress Trace, 76 N.J. 255, 386 A.2d 1295 (1978) (in-progress trace). In each case, the order directed that the telephone company be compensated at the prevailing rates, so company resistance could not have been based on financial reasons. Presumably, the companies sought doubly to protect themselves from possible subsequent civil suits brought by the subscribers.
191. 18 U.S.C. § 2511(2)(a)(ii) (Supp. II 1978) apparently does not subject a telephone company to civil liability for cooperating with state pen register requests. See note 130 and accompanying text supra. Nevertheless, the recent resistance to court orders, see note 189 supra, suggests that the nation's telephone companies are unlikely to be willing to test the applicability of that statute to such a situation.
rule 57(b) of the Federal Rules of Criminal Procedure and the All Writs Act.

VII. CONCLUSION

In *Smith v. Maryland*, the Supreme Court held that when a telephone company, acting at the informal request of the police, uses a pen register to make a record of the local numbers dialed from a suspect’s phone, use of the pen register does not constitute a “search”; therefore, the fourth amendment is irrelevant, and no search warrant is required. It would be melodramatic to contend that the decision seriously and immediately jeopardizes individual privacy. The decision is directly applicable only if the telephone company complies with a police request. Telephone companies are unlikely to do so, absent circumstances under which a company would have used a pen register on its own initiative.

Nevertheless, *Smith v. Maryland* is troubling for several reasons. In arriving at its decision, the Supreme Court relied on dubious factual assumptions, nullified congressional intent, and created an absurd anamoly in federal law. Worse, it extended the “assumption of risk” approach to the fourth amendment in a fashion that has unsettling implications on the question of the right to privacy generally. Finally, it is disturbing to realize that, as a result of *Smith v. Maryland*, a not insignificant aspect of personal privacy is protected, not by legislation or by the mandate of the fourth amendment, but only by the benevolence of the local telephone company.