1980

Pen Registers After Smith v. Maryland

John S. Applegate
Indiana University Maurer School of Law, jsapple@indiana.edu

Amy Applegate
Indiana University Maurer School of Law, aga@indiana.edu

PEN REGISTERS AFTER *SMITH V. MARYLAND*

INTRODUCTION

In *Smith v. Maryland*[1] the Supreme Court held that the use of pen registers without a warrant does not violate the fourth amendment.[2] A pen register is a device that is installed at the telephone company and automatically records all numbers dialed from the line to which it is attached, as well as incoming rings.[3] Unlike a wiretap, a pen register does not require constant monitoring. As a consequence, the pen register is an attractive surveillance tool.

Law enforcement officers need not secure a warrant before installing a pen register because the use of the device was found not to be a "search" within the meaning of the fourth amendment. But the pen register can reveal much about a person's private life. The device also implicates associational rights under the first amendment: information from many pen registers, or from one at a group's headquarters, can develop a complete picture of the network of associations among a large number of people.[4]

Smith reversed earlier assumptions about pen registers,[5] and is an example of the trend in federal courts to exempt from fourth amend-

---

[1] 442 U.S. 735 (1979).

[2] 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. The fourth amendment has been held applicable to some telephone surveillances. *See, e.g.,* Katz v. United States, 389 U.S. 347 (1967) (wiretaps).

[3] United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977). A modern pen register will simultaneously record the date and time of the call. The often-cited description of pen registers in United States v. Giordano, 416 U.S. 505, 549 n.1 (1974), describes an earlier and less sophisticated machine. *See* Brief for Respondent at 16, United States v. New York Tel. Co., 434 U.S. 159 (1977).

[4] *See, e.g.,* NAACP v. Alabama, 357 U.S. 449 (1958) (requiring political organization to divulge its membership list infringes members' freedom of association).

[5] *See* United States v. New York Tel. Co., 434 U.S. 159, 165 n.7 (1977) (government conceded applicability of fourth amendment to pen registers and Court expli-

ment limitations such governmental surveillance tools as mail covers,[6] tracking devices[7] and scrutiny of bank records.[8] The authors contend that the trend fails to reflect the first and fourth amendment interests. Part I of this Comment will examine the trend in the light of current fourth amendment doctrine. Part II examines the possibility of limiting the *Smith* decision to its facts. Part III suggests that the first amendment can work as a safeguard against extended or unlimited use of pen registers. Part IV will conclude with a discussion of the absence of federal statutory protection against pen register surveillance, and offer a statutory method of providing such protection.

I. FLAWS IN FOURTH AMENDMENT ANALYSIS

A. Degrees of Privacy

Justice Harlan, concurring in *Katz v. United States,*[9] most clearly explained the test used by the Court to determine whether a search has been conducted. He recognized a search only if the victim of the search

---

citly declined to decide question); United States v. Giordano, 416 U.S. 505, 553-54 (1974) (probable cause requirement of fourth amendment satisfied, mooting issue of applicability of fourth amendment to pen registers) (Powell, J., concurring in part and dissenting in part). *See also* United States v. Southwestern Bell Tel. Co., 546 F.2d 243, 245 (8th Cir. 1976), *cert. denied,* 434 U.S. 1008 (1978); *In Re* Order Authorizing the Use of a Pen Register, 538 F.2d 956, 959 (2d Cir. 1976), *rev'd on other grounds sub nom.* United States v. New York Tel. Co., 434 U.S. 159 (1977); United States v. John, 508 F.2d 1134, 1141 (8th Cir.), *cert. denied,* 421 U.S. 962 (1975); United States v. Illinois Bell Tel. Co., 531 F.2d 809, 812 (7th Cir. 1975); United States v. Doolittle, 507 F.2d 1368, 1371 (5th Cir.), *aff'd,* 518 F.2d 500 (en banc), *cert. denied,* 423 U.S. 1008 (1975); United States v. Brick, 502 F.2d 219, 223 (8th Cir. 1974); United States v. Falcone, 505 F.2d 478, 482 n.21 (3d Cir. 1974), *cert. denied,* 420 U.S. 955 (1975).

[6] *See, e.g.,* United States v. Choate, 576 F.2d 165 (9th Cir.), *cert. denied,* 439 U.S. 953 (1978). Mail covers involve the recording by postal employees of the outsides of first-class envelopes, and sometimes the insides of lower-class mail, addressed to a given person. 39 C.F.R. § 233.2 (1980).

[7] *See, e.g.,* United States v. Hufford, 539 F.2d 32 (9th Cir.), *cert. denied,* 429 U.S. 1002 (1976). *Contra,* United States v. Holmes, 521 F.2d 859 (5th Cir. 1975), *aff'd,* 537 F.2d 227 (1976) (en banc) (warrant required).

[8] United States v. Miller, 425 U.S. 435 (1976). *See also* California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974).

[9] 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

"exhibited an actual (subjective) expectation of privacy" and "society is prepared to recognize [that expectation] as 'reasonable.' "[10] Under this test one's privacy expectations depend, among other things, on technology and legal rules.

Two bank records cases demonstrate the consequences of allowing the fourth amendment to expand or contract as technology grows or legal rules change. In *California Bankers Association v. Schultz,*[11] the Court held that "the mere maintenance of the records [i.e., checks, deposits, withdrawals, etc.] by the banks under the compulsion of the regulations invaded no fourth amendment right of any depositor,"[12] because the recordkeeping "regulation [does not] require that any information contained in the records be disclosed to the Government."[13] Two years later, in *United States v. Miller,*[14] the Court decided that although the bank may have been forced to keep these records, the depositor could claim no legitimate expectation of privacy in them.[15]

In both *California Bankers* and *Miller,* the judicially approved bank-record laws narrowed the scope of the fourth amendment by contracting citizens' expectations. More importantly, the bank records cases demonstrate the Court's general insensitivity to *degrees* of privacy[16] in fourth amendment analysis. People reveal information about themselves for various, often very limited, purposes. Financial information is conveyed to a bank in order to get a loan processed, not to evaluate—or prosecute—a person in light of the transaction. The

[10] *Id.* at 361. Smith v. Maryland, 442 U.S. 735, 740 (1979), confirms that this is still the standard for determining the applicability of the fourth amendment.

[11] 416 U.S. 21 (1976).

[12] The Bank Secrecy Act of 1970, 12 U.S.C. §§ 1829b, 1952–1953 (1976 & Supp. III 1979), authorizes the Secretary of the Treasury to issue regulations requiring banks insured by the Federal Deposit Insurance Corporation to keep copies of checks and other financial records that have "a high degree of usefulness in criminal, tax or regulatory investigations or proceedings."

[13] 416 U.S. at 52, 54. The Court determined that the depositors lacked standing because none of them alleged a transaction of sufficient amount to come under Treasury Regulations, *id.* at 68–69, but the holding is stated in much broader terms and was so read in United States v. Miller, 425 U.S. 435, 439, 447 (1976).

[14] 425 U.S. 435 (1976).

[15] 425 U.S. at 442–43.

[16] "Privacy is not a discrete commodity, possessed absolutely or not at all." Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

Supreme Court in *Miller,* however, reasoned that bank records are "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," and that thus the records "are not confidential communications."[17]

Miller based this "assumption of risk" argument on two informer cases, *United States v. White*[18] and *Hoffa v. United States.*[19] But to name these cases suggests the distinction: one expects a human being to evaluate, digest, recall, and perhaps repeat information; a bank merely performs and registers a transaction. An HEW report has said, "There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[20] Similarly mail covers involve a transaction in which the post office is intended to be simply the medium, not an evaluator or recorder. Yet mail covers have been held not to be searches because the envelope is "voluntarily conveyed to the Postal System," based on the analogy to *Miller.*[21]

Mail surveillance also reveals a second factor in analyzing degrees of privacy: the amount of information exposed at any one time. A person's correspondence is carried on in small parts. As former Judge Hufstedler noted in *United States v. Choate,* "While an individual may realize that an isolated piece of mail may attract the attention of postal employees, he knows that ordinarily no one would have the ability or inclination to remember who writes to him."[22] By exposing

---

[17] 425 U.S. at 442.

[18] 401 U.S. 745, 751–52 (1971) (agent listened to defendant with a microphone attached to an informer).

[19] 385 U.S. 293, 302 (1966) (defendant revealed incriminating information to a government informant). The informer case is similar to one-party consent wiretapping. A person can consent to government wiring of him for sound and, according to United States v. White, 401 U.S. at 752, a speaker assumes this risk in choosing persons with whom to speak. Banks are not analogous; a "speaker" cannot choose between trustworthy and nontrustworthy banks because the government can obtain information from all banks with equal ease.

[20] SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 41 (1973).

[21] United States v. Choate, 576 F.2d 165, 175 (9th Cir.), *cert. denied,* 439 U.S. 953 (1978) (mail cover used to determine the address in South America of defendant's source of smuggled goods).

[22] *Id.* at 202 (Hufstedler, J., concurring in part and dissenting in part).

isolated pieces of information, the intention to expose, or the responsibility for the risk of exposure of, an entire pattern of activities cannot be assumed.[23]

This distinction is clear in the tracking device cases. While one undoubtedly has no expectation of privacy in being sighted once by a single individual or policeman while driving in a car, the combination of all of the sightings by all of the individuals who saw the car is another matter entirely. To argue that because each sighting is not private the total is also unprotected ignores the reason why the tracking device was installed in the first place: the total of the individual sightings is in fact private unless a surveillance device is used.[24]

The distinction between exposure to other private persons and entities and exposure to the government, has also escaped the courts. The Supreme Court in *Miller,* for example, said that "[t]he depositor takes the risk . . . that the information will be conveyed by that person [i.e., the bank] to the Government."[25] But the government prosecutes while other citizens do not. The government has very different *purposes* in acquiring the same information possessed by a citizen—tax fraud as opposed to idle curiosity, membership in a subversive organization as opposed to gossip. "Mailmen should be our messengers, not the state's newsgatherers."[26]

The government is also different from individual citizens in terms of the amount of information held. While a person driving his car may

---

[23] The Supreme Court recognized the threat to privacy posed by massive collections of personal information in Whalen v. Roe, 429 U.S. 589, 605-06 (1977) (New York statute recording, *inter alia,* the names and addresses of physicians and patients respectively dispensing and receiving dangerous legitimate drugs held constitutional).

[24] United States v. Holmes, 521 F.2d 859, 866 n.13 (5th Cir. 1975), *aff'd,* 527 F.2d 227 (1976) (en banc). In *Holmes* a tracking device was attached to a van being used to transport marijuana; government agents used this device to follow the van to a shed where the marijuana was stored. In United States v. Hufford, 539 F.2d 32 (9th Cir.), *cert. denied,* 429 U.S. 1002 (1976), a tracking device was attached to a drum of caffeine to be used in the production of illegal amphetamines. In United States v. Moore, 562 F.2d 106 (1st Cir.), *cert. denied,* 435 U.S. 926 (1977), agents placed tracking devices in a car, a van and a box of chemicals to locate a "factory" manufacturing controlled substances. Congress has since required federal agents to obtain warrants for the use of tracking devices. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1804 (1978).

[25] 425 U.S. at 443.

[26] Hufstedler, *Invisible Searches for Intangible Things: Regulation of Governmental Information Gathering,* 127 U. PA. L. REV. 1483, 1521 (1979).

be happy to let another citizen know that he passed the corner of Main and Washington Streets, the driver may still reasonably expect that his friend on the sidewalk will not also have access to the information that the driver went through the railway underpass, and then turned right at Sixth Street, and so on. Similarly, the individual postman or bank teller will not be expected to retain large amounts of information. Indeed, the information "exposed" in these ways may be meaningful or useful only to the government. Knowing exposure to one to whom the information will mean nothing is not equivalent to exposure to the government, to whom it may mean a great deal.

All three measures of the degree of privacy, the purposes for which the information is exposed, the amount of information exposed and to whom it is revealed, are especially relevant to telephone numbers. First, although the telephone company is a recipient in a sense of the number dialed, it can be expected to complete the transaction "mechanically." The vast majority of telephone calls are forwarded solely by machine.[27] The information in numbers dialed is "exposed" only to the telephone company and for the very limited and specific purpose of reaching the telephone line called.

Second, human contact with phone numbers is carried on only in small, discrete parts, with no expectation by the dialer that the pieces are being compiled. Telephone company review of a bill or correction of an error in a bill would ordinarily be of a similar, piecemeal nature.

Third, revelation to the telephone company is not revelation to the government. The telephone company has a policy of maintaining the confidentiality of the numbers dialed.[28] Any use the telephone company might make of such information—billing, determination of correct rate structure—is very different from government evidence gathering.

---

[27] [I]t is only by analogy that [telephone] dial pulses are viewed as a request for a connection. Of course, no person was the intended recipient of the dial pulses, but rather [, the recipient was] the communication system through which the pulses were to be relayed as a signal to activate the telephone of the intended recipient of the telephone call.

United States v. Dote, 371 F.2d 176, 180 (7th Cir. 1966).

[28] Claerhout, *The Pen Register,* 20 DRAKE L. REV. 108, 115–16 (1970). *See also* Reporters' Comm. for Freedom of the Press v. AT & T, 593 F.2d 1030, 1038 (D.C. Cir. 1978), *cert. denied,* 440 U.S. 949 (1979).

All three measures of the degree of privacy lead to a conclusion that people usually expect privacy to attach to the telephone numbers they call or from which they receive calls. Nevertheless, due primarily to a disregard of these measures of the degree of privacy, the Court in *Smith* found no such privacy, and thus no "search" to activate the protections of the fourth amendment.

B. The Prohibition Against General Searches

In addition to its failure to recognize varying degrees of privacy the Supreme Court has not considered that the scope of a surveillance may also indicate whether or not a search has taken place. Specific surveillance is, for example, the monitoring by the police of a single suspect's telephone for a *particular* number—that of the complaining party.[29] Not only is this minimally intrusive, but the police have the consent of the party whose number is being called for the disclosure of that communication. There is a specific crime of which the suspect is accused, and more often than not the police possess probable cause.

General surveillance, by contrast, involves targeting one or a number of individuals and checking out *all* the numbers they call, getting a complete and detailed picture of their lives, and others' as well. There may be no specific crimes of which these people are accused, let alone probable cause; law enforcement officers might merely consider their conduct undesirable.

One need not turn to Orwell[30] to find general governmental surveillance. The technology for such surveillance certainly exists,[31] and recent history affords ample evidence of the willingness of government

---

[29] A typical situation is that of obscene or harrassing calls.

[30] G. ORWELL, NINETEEN EIGHTY-FOUR (1949).

[31] *See generally* A. MILLER, THE ASSAULT ON PRIVACY (1971):

> Perhaps the most significant threats to personal freedom are presented by the inevitable linking of computers to existing surveillance devices for monitoring people and their communications. One of the simplest contemporary snooping devices is the pen register. . . . This snooping capability could be magnified if the information drawn in by the pen register were automatically fed into a central computer for analysis. Widespread use of this technique would quickly reveal patterns of acquaintances and dealings among a substantial group of people.

Id. at 43.

officials to use that technology.[32] The usefulness and convenience of pen registers in such schemes is apparent. They are a cheap and semi-automatic way to monitor a person's or group's contacts.

The fourth amendment itself distinguishes between general and specific surveillances. In the second clause of the amendment (i.e., the warrant, probable cause, and particularity requirements), *every* search must be for particular things in particular places, regardless of the type of search conducted.

History corroborates this reading of the language of the amendment. General warrants, which were used to support the Crown's licensing of printed matter,[33] and writs of assistance,[34] are the nemesis of the fourth amendment.[35] Though limited in England by the landmark case of *Entick v. Carrington,*[36] general warrants were often employed in the American Colonies in the 1760's to control the Colonists' presses and to uncover their smuggling operations.[37] Public reaction was so fierce that general warrants could seldom be enforced.[38] As a result, the states built safeguards against general searches into their constitutions, and these served as models for the fourth amendment.[39]

When the Supreme Court has been confronted with general warrants, the results of the search have been suppressed. *Stanford v. Texas* involved a warrant authorizing the search and seizure of two thousand books, pamphlets and other documents in an effort to confiscate

---

[32] *See, e.g.,* SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 223-24 (1973) (documenting former Attorney General John Mitchell's expansion of government surveillance of citizens); Jacobs, *An Overview of National Political Intelligence,* 55 U. DET. J. URB. L. 853, 855 (1978) (discussing former FBI Director J. Edgar Hoover's policy of surveillance).

[33] J. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT 20 (1966).

[34] Writs of assistance were used to combat Colonial smuggling. *Id.* at 22 n.8.

[35] See Stanford v. Texas, 379 U.S. 476, 481-84 (1965), for an excellent discussion of this point.

[36] 19 How. State Trials 1029 (1765). *See also* Wilkes v. Wood, 98 Eng. Rep. 489 (1763). Parliament was also aroused to limit them in 1766. T. TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 35 (1969).

[37] N. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 57-63 (1937).

[38] *Id.* at 73-76.

[39] J. LANDYNSKI, *supra* note 33, at 38-42.

Communist literature.[40] The Court unanimously held that the search violated the fourth amendment's prohibition of general searches. In *Berger v. New York,* the Court based its rejection of the New York wiretap statute on the lack of specificity as to the material to be seized.[41]

Despite the overwhelming animus against general searches, the Supreme Court has structured its analysis of the fourth amendment so that the whole question of the generality or specificity of a "search" does not become relevant until it has been determined that a search took place. Instead of focusing on the "unreasonableness" of the search,[42] the Court has concentrated on the definition of *search.*[43]

This focus is incorrect on its face and as a matter of history. To search is to take affirmative steps to acquire desired information. Wiretaps and pen registers are surely both used for "searches" in this sense. The sensible focus of the Court should be on whether these "searches" are *reasonable:* is there probable cause to believe the search will yield specific evidence about a specific illegal act? Whether a law enforcement official or not, no rational being expends effort to monitor telephones or to canvass a person's mail or to track a person's car if he is not searching for information. It is, of course, true that, if a policeman sees someone carrying a marijuana plant down Main Street, there is no search, but this is because that detection was mere happenstance, a coincidence. But, if a police officer is told that a person has marijuana plants five feet tall in his backyard and the officer goes over to the house, looks through the chain-link fence and sees the

---

[40] 379 U.S. 476, 477 (1965).

[41] 388 U.S. 41, 55 (1967).

[42] Although determination of the existence of a search under the *Katz* expectations test is a flexible matter because of the open-ended nature of that test, once the determination is made the consequences rigidly follow. If a search exists, then the full panoply of safeguards in the fourth amendment apply, absent exigent circumstances or a search incident to arrest, *see* note 66 *infra* and accompanying text.If there is no search, no protections whatsoever apply. The Court has rigidly separated the definition of *search* from the question of *reasonableness.* Thus, current judicial interpretations of the fourth amendment not only refuse to recognize differences in degrees of privacy, and thus of "search," *see* text accompanying notes 16-28 *supra,* but has also refused to apply different degrees of fourth amendment protections.

[43] *See, e.g.,* Katz v. United States, 389 U.S. 347, 353-54, 356-57 (1967). For a criticism of the Court's approach, see N. LASSON, *supra* note 37, at 103.

plants, the Supreme Court would say that this does not constitute a search. But it does in a nonlegal sense: the officer has gone to the house for the specific purpose of looking into the yard. He has taken affirmative steps to look for evidence. A good rule of thumb might be that if law enforcement officers must exert great effort and employ sophisticated surveillance techniques, they must be searching for something, and that therefore a search exists unless there is *clearly* no expectation of privacy involved. However this standard is defined, it would be more in keeping with the language and spirit of the fourth amendment if courts would focus less on the rigidly interpreted *Katz* requirements for the existence of a search, which has led to such anomalies as the conclusions that wiretaps are searches and pen registers are not, or that massive government canvassing of a person's mail is not a search. Instead, broaden the definition of a search as suggested above, or assume in doubtful cases that a search exists, and concentrate judicial energy on more appropriate inquiry into the reasonableness of the "search." We become too embroiled in questions of subjective expectations and amorphous zones of privacy when attention is focused on whether the policeman looking through the chain-link fence is conducting a search; the policeman was acting reasonably, and reasonableness should be our focus.

II. *SMITH V. MARYLAND*

The *Smith* case illustrates the use of a pen register for specific surveillance. The facts as found by the Maryland Court of Appeals were as follows:[44] The victim, Patricia McDonough, was assaulted and robbed late one night near her home. She gave the police a description of her assailant and told them that she had seen him changing a tire on his green Monte Carlo automobile just before the robbery. Shortly after the crime, she began to receive a number of threatening and obscene phone calls from a man who identified himself as her assailant. In one of these calls, the man requested that she step out onto her porch so that he could see her. When she did, she saw driving by her home the same green Monte Carlo she had observed the night of the robbery. The next day, defendant Smith, in the vicinity of McDonough's home, stopped and sought the assistance of a police officer

[44] Smith v. State, 283 Md. 156, 157–59, 389 A.2d 858, 859–60 (1978).

(the same officer to whom the victim had reported the crime) in opening the locked door of his green Monte Carlo. The officer took the license number of the vehicle, learned that it was registered to Smith, and notified other investigating officers.

The next day, at the request of police, the telephone company installed a pen register at its central offices to record the phone numbers of calls made from the telephone at Smith's residence. The pen register showed that on that same day a call was made from Smith's residence to McDonough's home. The police then obtained a warrant to search Smith's automobile and residence: they found in Smith's residence a telephone book with the page containing McDonough's name and number turned down. Subsequently, she identified Smith as the man who had robbed her.

Smith moved to suppress the pen register evidence, which was obtained without use of a warrant, but the motion was denied and Smith was convicted of robbery and sentenced to ten years' imprisonment.[45]

The Supreme Court, affirming the lower court, held broadly that the installation and use of a pen register by the telephone company at police request did not constitute a search within the meaning of the fourth amendment and that therefore no warrant was required. The Court rejected Smith's claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.[46] The Court doubted that people entertain an actual expectation of privacy in the numbers they dial because "[a]ll subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."[47] Moreover, the Court assumed that people are aware the phone company records numerical information for a variety of legitimate business reasons.

The Court also rejected Smith's argument that, regardless of general expectations, he had demonstrated an expectation of privacy by using "the telephone *in his house* to the exclusion of all others."[48] The Court found the site of the call immaterial to the analysis. The site

[45] 283 Md. at 160, 389 A.2d at 860.

[46] Smith v. Maryland, 442 U.S. 735, 742 (1979).

[47] *Id.*

[48] *Id.* at 743 (emphasis in original).

might have been calculated to keep the contents of the conversation private, but it could not preserve the privacy of the number dialed.[49]

Justice Blackmun did concede that the determination of whether or not there was a subjective expectation of privacy may not alone be adequate in certain contexts.[50] Using the example of a government announcement on national television that all homes henceforth would be subject to warrantless entry, Blackmun stated that, although individuals would probably no longer entertain an actual expectation of privacy regarding their houses, papers and effects, "a normative inquiry would be proper" to determine "whether a 'legitimate expectation of privacy' existed in such cases."[51]

Despite this concession, the Court also found that even if the petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, that expectation was not "one that society is prepared to recognize as 'reasonable.'"[52]

The Court analogized the switching equipment that processes phone numbers dialed to the human operator. Since one has no legitimate expectation of privacy in phone calls placed through an operator, no "different constitutional result [was] required because the telephone company ha[d] decided to automate."[53]

> 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. In so doing, petitioner assumed the risk that the company would reveal to police the numbers dialed.[54]

The Court rejected Smith's argument that there was a legitimate expectation of privacy in making local calls in view of the fact that the telephone company does not usually record local calls. The Court refused to allow fourth amendment protection to "exist, or not,

---

[49] *Id.*

[50] *Id.* at 740 n.5.

[51] *Id.*

[52] *Id.* at 743, *quoting* Katz v. United States, 389 U.S. 347, 361 (1967).

[53] *Id.* at 745.

[54] *Id.* at 744.

depending on how the telephone company chose to define local dialing zones, and depending on how it chose to bill its customers for local calls."[55]

The *Smith* case was wrongly decided even when analyzed under current fourth amendment doctrine. Telephone users do in fact assume privacy; the majority's "assumption of risk" argument is seriously misguided; and the actual expectation of privacy in numbers dialed is one which ought to be recognized by society as a legitimate one.

The argument advanced by the Court that telephone users know that records will be made of toll calls and thus have no expectation of privacy is unconvincing.[56] As Justice Marshall pointed out, the assumption of risk analysis[57] was first advanced in third-party consensual surveillance cases, where "the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications."[58] In the case of pen registers, however, "unless a person is prepared to forego use of what for many has become a personal or professional necessity, he cannot but accept the risk of surveillance."[59] Furthermore, the legitimacy of privacy expectations "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."[60]

The most serious defect in the Court's assumption of risk argument is its distinction between verbal and digital transmissions. No one would claim that people assume the risk of disclosing conversations to telephone company circuits. The dialing of a telephone number places the telephone company in the same position of mechanical connector of the two lines. The Supreme Court is apparently unwilling to let fourth amendment protection depend upon the records that subscribers know are being kept, like bills, but is willing to let it depend on

---

[55] *Id.* at 745.

[56] 283 Md. at 182, 389 A.2d at 872 (Cole, J., dissenting). *See also Recent Decision: Installation and Use of a Pen Register Does Not Constitute a Fourth Amendment "Search"*—Smith v. Maryland, 38 MD. L. REV. 767, 776–78 (1979).

[57] 442 U.S. at 749–50 (Marshall, J., dissenting).

[58] *Id.* at 749.

[59] *Id.* at 750. *See also* Katz v. United States, 389 U.S. 347, 352 (1967).

[60] 442 U.S. at 750 (Marshall, J., dissenting). *See also* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

other intricate details of the operation of a telephone company—for example, the mechanics of switching machines.

The Court should recognize a legitimate expectation of privacy in numbers dialed. Telephones are a modern necessity[61] and, as was noted above,[62] pen registers can help reveal travel patterns, personal and professional associations, and other such information. Knowledge of the date, time and parties to a telephone conversation often yields knowledge of the conversation itself: a call from a bookie to a racetrack leaves little doubt as to what was discussed.[63]

Legitimate expectations of privacy should be deemed to exist in all information that individuals without criminal motives want to keep out of the public eye. By this standard, numbers dialed deserve protection, for they convey information that most private telephone subscribers would not want "to have broadcast to the world."[64]

The Court could claim, without contradicting itself, that legitimate and actual expectations of privacy do not extend to the occasional number dialed but do extend to the development of a complete and detailed picture of a person's life. The possible consequences of *Smith* may convince the Court to impose such a limitation.[65]

The Court ought at least to require a showing of probable cause that evidence of a specific criminal act will be uncovered. There is precedent for requiring probable cause and excusing the warrant requirement in the search incident to arrest and exigent circumstances doctrines.[66] Though situations in which the pen register is used will seldom involve the exigency or danger to police which this compromise envisions, the probable cause requirement would at least provide the remedy of suppression for capricious or malicious surveillance.[67]

---

[61] 442 U.S. at 746 (Stewart, J., dissenting).

[62] *See* text accompanying note 3 *supra.*

[63] United States v. Dote, 371 F.2d 176, 181 (7th Cir. 1966) (police using pen register on bookmaker's telephone knew the "likely character" of his conversations).

[64] 442 U.S. at 748 (Stewart, J., dissenting).

[65] In United States v. United States Dist. Ct., 407 U.S. 297, 325-26 (1972) (Douglas, J., concurring). Justice Douglas cited Justice Department statistics estimating that wiretaps not supervised by a court were six to sixteen times longer in average duration than unsupervised ones.

[66] *E.g.,* Chimel v. California, 395 U.S. 752, 762-63 (1969) (search incident to arrest); Warden v. Hayden, 387 U.S. 294, 298-300 (1967) (exigent circumstances).

[67] Mapp v. Ohio, 367 U.S. 643 (1961).

Nevertheless, even such a limited *Smith* decision fails to protect individual privacy adequately. The next Part considers the use of the first amendment to challenge general surveillance with pen registers.

III. PEN REGISTERS AND FREEDOM OF ASSOCIATION

While the fourth amendment protects privacy in general, the first amendment is concerned with the basic freedoms of thought, expression and association.[68] Associational rights under the first amendment in particular are implicated by general surveillance. In *NAACP v. Alabama*[69] the Supreme Court observed, "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association."[70]

Recognizing this need for privacy, the Court has struck down state attempts to compel disclosure of NAACP membership lists,[71] organizational affiliations of school teachers[72] and political affiliations of applicants to the bar.[73] Disclosure of political contributors has also been limited.[74] The pen register, the basic function of which is to establish associations, encroaches upon freedom of association when used for general surveillance.

A first amendment freedom of association claim has several advantages for litigants contesting pen register surveillance. Because the first amendment occupies a "preferred position" in the Bill of Rights, a court must give great weight to first amendment-based claims[75] and uphold challenged governmental action only on the basis

---

[68] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise therof; or abridging freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

[69] 357 U.S. 449 (1958).

[70] *Id.* at 462.

[71] Louisiana v. NAACP, 366 U.S. 293 (1961); Bates v. City of Little Rock, 361 U.S. 516 (1960); NAACP v. Alabama, 357 U.S. 449 (1958).

[72] Shelton v. Tucker, 364 U.S. 479 (1960).

[73] *In re* Stolar, 401 U.S. 23 (1971); Baird v. State Bar of Ariz., 401 U.S. 1 (1971).

[74] Pollard v. Roberts, 283 F. Supp. 248 (E.D. Ark.), *aff'd per curiam,* 393 U.S. 14 (1968).

[75] Gooding v. Wilson, 405 U.S. 518 (1972); Freedman v. Maryland, 380 U.S. 51 (1965); Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963).

of an immediate, substantial and compelling state need[76] met by the least intrusive method possible.[77] This last element, the least restrictive alternative requirement, is analogous to the fourth amendment's particularity requirement. Further,

> the general requirement of particularity in warrants is more strictly applied in situations involving the seizure of materials which arguably fall within the First Amendment's protection of free expression. This is necessary to guard against an executing officer's seizing protected expression, if he is not given some guidelines to direct his exercise of discretion.[78]

There are difficulties, however, in obtaining the first amendment remedy sought. First, such a claim is stronger in cases of general rather than specific surveillance. In the case of specific surveillance, the law enforcement interest is compellingly concrete. In cases of general surveillance, the law enforcement interest is vaguer and less weighty. The language and history of the fourth amendment[79] further bolsters the relative strength of the first amendment claim.

The second difficulty of first amendment claims against the use of pen registers is that such associational claims have been granted only to groups whose ends have first amendment significance, such as political advocacy or religious worship.[80] Where the group's goals do not closely concern the first amendment, or where individuals rather than identifiable and cohesive groups are involved, the cases offer little hope that the claim will be accepted.[81]

---

[76] Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 544–46 (1963); NAACP v. Button, 371 U.S. 415, 438–39 (1963).

[77] United States v. O'Brien, 391 U.S. 367 (1968); Shelton v. Tucker, 364 U.S. 479, 488 (1960).

[78] United States v. Manarite, 314 F. Supp. 607, 610 (S.D.N.Y. 1970), *aff'd,* 448 F.2d 583 (2d Cir.), *cert. denied,* 404 U.S. 947 (1971). *See also* Marcus v. Search Warrant, 367 U.S. 717 (1961); United States v. Marti, 421 F.2d 1263 (2d Cir. 1970), *cert. denied,* 404 U.S. 947 (1971).

[79] *See* text accompanying notes 33–39 *supra.*

[80] L. TRIBE, AMERICAN CONSTITUTIONAL LAW 702 (1978).

[81] Nevertheless, there are persuasive arguments against such a limited view of the freedom of association. *See, e.g.,* Raggi, *An Independent Right to Freedom of Association,* 12 HARV. C.R.-C.L. L. REV. 1, 14 (1977) (proposing that "freedom of asso-

A third difficulty with first amendment-based pen register claims is the requirement of concreteness of injury. In *Laird v. Tatum,*[82] the Supreme Court found no justiciable controversy in the allegation that United States Army Intelligence was conducting "surveillance of lawful and peaceful civilian political activity"[83] because there was no showing by the plaintiffs of objective harm or the threat of specific future harm. The allegation of a subjective "chill" was deemed to be an insufficiently concrete injury to fall within the scope of the first amendment.[84]

Tatum has been cited in support of findings of no justiciable controversies in cases involving police surveillance of demonstrations and public meetings, and the retention of photographs of those events in police files;[85] collection of information concerning a government job applicant's acquaintances and their "homosexual mannerisms;"[86] and an FBI investigation of an antiwar demonstration.[87]

No justiciable controversy was found in two other contexts. In *California Bankers Association v. Shultz,*[88] the American Civil Liberties Union challenged a requirement, under the Bank Secrecy Act, that banks keep certain records as chilling to first amendment rights. The first amendment threat was seen as too remote.[89] And in *Reporters Committee for Freedom of the Press v. AT&T,*[90] the court, while agreeing "*in theory* that subpoenas issued in bad faith may in some

---

ciation, long recognized as a vechicle for the exercise of . . . first amendment rights . . . [should] now be seen as protecting associational activity that is non-speech or non-political as well').

There is some judicial support for an expanded view of freedom of association, *see, e.g.,* United States Dep't of Agriculture v. Moreno, 413 U.S. 528, 541 (1973) (Douglas, J., concurring); Griswold v. Connecticut, 381 U.S. 479, 484, 486 (1965). However, more recent decisions seem to reverse this expansion, *see, e.g.,* Garcia v. Texas State Bd. of Medical Examiners, 384 F. Supp. 434 (W.D. Tex. 1974), *aff'd mem.,* 421 U.S. 995 (1975).

[82] 408 U.S. 1 (1972).

[83] *Id.* at 2.

[84] *Id.* at 13–14.

[85] Donohoe v. Duling, 465 F.2d 196 (4th Cir. 1972).

[86] Finley v. Hampton, 473 F.2d 180 (D.C. Cir. 1972).

[87] Fifth Ave. Peace Parade Comm. v. Gray, 480 F.2d 326 (2d Cir. 1973), *cert. denied,* 415 U.S. 948 (1974).

[88] 416 U.S. 21 (1974).

[89] *Id.* at 56–57.

[90] 593 F.2d 1030 (D.C. Cir. 1978), *cert. denied,* 440 U.S. 949 (1979).

cases abridge First Amendment rights," refused to intervene in the subpoena process unless the plaintiff established "a *clear and imminent* threat of such future misconduct."[91]

The Supreme Court has, however, found justiciable controversies in cases involving a city ordinance requiring handbills to include the names and addresses of the persons who had prepared, distributed or sponsored them;[92] a state statute compelling the NAACP to produce membership lists;[93] a state statute requiring that a loyalty oath of unclear meaning be taken as a prerequisite to employment by a government agency;[94] and statutes or actions, including data gathering, aimed at discouraging "subversives" in public academic institutions.[95] Also considered cognizable are actions for the expungement of arrest records,[96] and actions based on a claim of injury to an individual's business and reputation resulting from a government investigation.[97]

The principle to be drawn from these cases would appear to be that some personal or specific injury must be alleged to bring a claim within the first amendment. Although data gathering and record keeping can clearly be seen as injurious,[98] the modern judicial trend is to view that threat as not justiciable.

---

[91] *Id.* at 1071 (emphasis in original).

[92] Talley v. California, 362 U.S. 60 (1960). The Court said, "There can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression." *Id.* at 64.

[93] NAACP v. Alabama, 357 U.S. 449 (1958) (NAACP claims such disclosure would injure the association by reducing its membership and injure its individual members by inhibiting their associational choice).

[94] Baggett v. Bullitt, 377 U.S. 360 (1964).

[95] Keyishian v. Board of Regents, 385 U.S. 589 (1967). *See also* Paton v. La Prade, 469 F. Supp. 773 (D.N.J. 1978); White v. Davis, 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975).

[96] Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974); Sullivan v. Murphy, 478 F.2d 938 (D.C. Cir.), *cert. denied,* 414 U.S. 880 (1973).

[97] Jabara v. Kelley, 476 F. Supp. 561 (E.D. Mich. 1979).

[98] Laird v. Tatum, 408 U.S. 1, 26 (1972) (Douglas, J., dissenting): "One need not wait to sue until he loses his job or until his reputation is defamed. To withold standing to sue until that time arrives would in practical effect immunize from judicial scrutiny all surveillance activities, regardless of their misuse and their deterrent effect."

See also California Bankers Ass'n v. Shultz, 416 U.S. 21, 98 (1974) (Marshall, J., dissenting).

In the context of pen registers, then, cognizability of a claim requires that some specific injury would result from compelled disclosure of phone numbers dialed—such as injury to reputation, business, educational pursuit, or political associations. This is a far heavier burden than that imposed under the fourth amendment, where the invasion of a legitimate privacy interest, without more, establishes a justiciable issue.

The fourth problem is how to assert a first amendment claim when the government is using a pen register or subpoenaing telephone records. After *Reporters Committee,* which denied plaintiff's claim that the first amendment requires telephone companies to give journalists notice before turning the latters' long-distance billing records over to the government,[99] it seems clear that neither the press nor ordinary citizens will receive prior notification of governmental investigation: they are precluded, at least initially, from raising objections. Thus, the only way to get review of pen register use, before the kind of extreme damage is done that is needed to get first amendment protection, appears to be through the telephone company.

The Court in *New York Telephone* appears to assume that a telephone company may object before the enforcement of a pen register order.[100] The Third Circuit recently held that a telephone company was entitled to a hearing before enforcement of a tracing order on the issue of whether the trace would be too costly and burdensome.[101] Additional support for the position that the phone company may object on behalf of telephone subscribers can be gleaned from *NAACP v. Alabama,* where the Supreme Court held that the NAACP had the right to assert, on behalf of its members, a right personal to them to be protected from compelled disclosure by the state of their affiliation with

[99] 593 F.2d 1030 (D.C. Cir. 1978), *cert. denied,* 440 U.S. 949 (1979). The case was remanded as to the other five plaintiffs for further fact-finding. In the lower court, the remaining reporters would have to show that there was an imminent danger that the government would subpoena their toll records in bad faith. *Id.* at 1070–71.

[100] United States v. New York Tel. Co., 434 U.S. 159, 174–75 (1977).

[101] *In re* Order Authorizing the Installation of a Pen Register, 610 F.2d 1148 (3d Cir. 1979). The burdensomeness of a pen register on a telephone company is, however, less than that of a tracing order. In these suits, both the courts and the telephone companies are primarily concerned with the financial burden on the companies rather than on the rights of third parties.

the Association as revealed by the membership lists.[102] Whether or not a bank (which is arguably analogous to the phone company) could assert rights on behalf of its depositors is not clear.[103]

Assuming the telephone company could assert rights on behalf of telephone subscribers, some sort of hearing prior to enforcement of the pen register order can be used. In *Bell Telephone,* the court held that a hearing was necessary before enforcement of the tracing order.[104] A commentator has noted that in the sensitive area of the first amendment, due process mandates that judicial review either precede or expeditiously follow final governmental action.[105] "[W]here First Amendment rights are at stake, the Supreme Court has insisted on procedural safeguards which demonstrate 'the necessary sensitivity to freedom of expression.'"[106]

In sum, the first amendment right of association provides a promising route by which to prevent the more egregious uses of pen registers. The advantages of such a claim are that it will engage a court's close scrutiny and that it will be outweighed only by a compelling state interest satisfied by the least intrusive means. Nevertheless, its disadvantages and limitations are significant; such claims will usually succeed only in cases of general surveillance of groups engaging in core first amendment activities where those groups can show a concrete injury. As plaintiffs' cases recede further from this paradigm, success on the first amendment claim becomes more unlikely. Because the vast majority of pen register cases are far from the paradigm, a statutory strategy, pursued in the next Part, is necessary to cancel the effects of *Smith.*

IV. STATUTORY SOLUTIONS

Present federal legislation provides inadequate protection from general pen register surveillance. While all federal officers are forbid-

---

[102] 357 U.S. 449, 458-60 (1958). *See also* Pollard v. Roberts, 283 F. Supp. 248, 259 (E.D. Ark.), *aff'd per curiam,* 393 U.S. 14 (1968).

[103] *See* California Bankers Ass'n v. Shultz, 416 U.S. 21, 55-56 (1974).

[104] *In re* Order Authorizing the Installation of a Pen Register, 610 F.2d 1148, 1156-57 (3d Cir. 1979).

[105] Monaghan, *First Amendment "Due Process,"* 83 HARV. L. REV. 518, 532 (1970). *See also* Reporters Comm. for Freedom of the Press v. AT&T, 593 F.2d 1030, 1088 (D.C. Cir. 1978) (Wright, J., dissenting), *cert. denied,* 440 U.S. 949 (1979).

[106] Freedman v. Maryland, 380 U.S. 51, 58 (1965).

den by the Foreign Intelligence Surveillance Act of 1978 (FISA)[107] from using pen registers without a warrant or court order,[108] state authorities remain uncontrolled. The statute governing electronic surveillance generally, Title III of the Omnibus Safe Streets and Crime Control Act of 1968,[109] does not apply to pen registers.[110] This is a large gap in the statutory scheme; states have sufficient money, technology and inclination to make frequent use of pen registers.

Moreover, federal officers are not as controlled in the use of pen registers as a first reading of FISA suggests. FISA provides that acquisition of a "search warrant *or* court order" by a federal officer using a pen register is an affirmative defense to claims of violations of the Act.[111] *Court order* is undefined and can mean either: (a) a FISA or Title III order, or (b) a Rule 57(b)[112] or All Writs Act[113] order. The former have fourth amendment standards; the latter do not.

Further, even if FISA fully prohibited federal abuse of pen registers, FISA's location in the War and National Defense title of the United States Code invites restrictive interpretation. Instead of being placed in Title III, where general federal wiretapping policy is expressed, FISA is placed within the specialized area of national security. While the language of FISA is quite clear, a narrow interpretation of the Act might be imposed on the grounds that the federal policy was, given the context, obscure. The courts have established that national security is a very different matter from law enforcement in the fourth amendment area,[114] and could impute to Congress a similar distinction.

In addition to providing citizens with greater privacy rights against federal law enforcement than against state law enforcement,

---

[107] 50 U.S.C. §§ 1801–1811 (Supp. III 1979).

[108] *Id.* at § 1804(a).

[109] 18 U.S.C. §§ 2510–2520 (1976).

[110] United States v. New York Tel. Co., 434 U.S. 159, 165–68 (1977).

[111] 50 U.S.C. § 1809(b) (Supp. III 1979).

[112] FED. R. CRIM. P. 57(b). This rule provides for interstitial orders in aid of law enforcement.

[113] 28 U.S.C. § 1651(a) (1976). One commentator has developed an elaborate argument, founded upon the assertion that Congress assumed that the fourth amendment applied to pen registers, that "court order" means an FISA or Title III order. Fishman, *Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent,* 29 CATH. U. L. REV. 557, 589–92 (1980).

[114] *E.g.,* United States v. United States Dist. Ct., 407 U.S. 297 (1972).

the statutory scheme permits evasive cooperation between state and federal officials. While FISA includes a criminal penalty for the use of pen register information not obtained under statute,[115] the provision requires that such use be "knowing or [with] reason to know."[116] Although a finding of taint in the evidence will still result in suppression of that evidence,[117] the greater protection provided by the criminal penalty can be nullified by a free flow of information from state to federal law enforcement officers with "no questions asked" about its source. Further, the suppression remedy would be more satisfactory if the principal targets of pen register abuse were subject to prosecution; that, however, is not the case. The most frightening use of pen register surveillance is to spy on and harass citizens, rather than to prosecute them.

Finally, the user of a pen register can achieve full wiretap capability simply by plugging headphones or a tape recorder into one of the jacks on the register.[118] The ease of such wiretapping and the difficulty of detection encourages this practice.

To eliminate this confusion and to fill in the gap in protection against pen register use by state authorities, Congress should amend Title III to include pen registers. Such increased protection would not unduly hamper law enforcement efforts. Although Title III limits the crimes for which electronic eavesdropping can be used and requires a relatively high level of decision to use this technique,[119] there has been no suggestion that these requirements have been especially difficult to meet.[120] Depending on the state, it is possible that a county or local

---

[115] 50 U.S.C. § 1809(a) (2) (Supp. III 1979).

[116] *Id.*

[117] *Id.* at § 1806(e).

[118] *In re* Joyce, 506 F.2d 373, 377 n.4 (5th Cir. 1975).

[119] 18 U.S.C. § 2516 (1976). The limitation is to serious crimes. Robbery, the crime in *Smith v. Maryland,* would be included, *id.* at § 2516(2).

[120] Although this is not an easily quantifiable statistic, a suggestion of how little law enforcement has been hampered by Title III can be gleaned from the authorization rate of interception requests by state and federal officials since Title III was enacted. From 1968 to 1976, the average annual authorization rate was 99.7%. In absolute numbers, about two requests are denied per year. ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, XVIII REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS Table 7 (1977).

district attorney can make the application. This is not a burdensome requirement.[121] Furthermore, the complex application which is at the heart of the Title III protections is dispensable in emergency situations[122] with respect to conspiratorial activities involving national security interests or activities characteristic of organized crime. Considering the very great dangers of abuse without regulation this minimal cost to law enforcement seems tolerable.

It is not unreasonable to believe that Congress will be amenable to incorporation of pen registers in Title III. In fact, the legislative history indicates that, if today's judicial doctrines and technological capability were before Congress when Title III was passed in 1968, pen registers would have been incorporated into the body of that Act.

Perhaps the strongest evidence that widespread pen registers use is inconsistent with congressional intent is in the insistence that Title III is to be "pattern[ed] . . . after what the Supreme Court said in the *Berger* and *Katz* decisions."[123] The *Katz* decision to which Congress was trying to conform in 1968 was a high point in fourth amendment protection. One ought not read into Title III the conservative understanding of "legitimate expectation" that has emerged from the Burger Court.[124]

Berger v. New York is even more important in this context. The principal complaint in *Berger* was that the New York wiretapping statute "lacked [the] particularization" required by the fourth amendment.[125] Particularization of a wiretapping order was of great concern to the drafters of Title III, however badly that concern was translated into the statutory language.[126] One manifestation of the desire to parti-

---

[121] If authorized to do so by state statute, he would be "the principal prosecuting attorney of any political subdivision" of the state, 18 U.S.C. § 2516(2) (1976). *See also* United States v. Tortorello, 342 F. Supp. 1029 (S.D.N.Y. 1972), *aff'd,* 480 F.2d 764 (2d Cir.), *cert.denied,* 414 U.S. 866 (1973); State v. Frink, 296 Minn. 57, 206 N.W.2d 664 (1973).

[122] 18 U.S.C. § 2518(7)(a) (1976).

[123] 114 CONG. REC. 14,484 (1968) (remarks of Sen. McClellan), S. REP. No. 1097, 90th Cong., 2d Sess. 66 (1968).

[124] *See* note 5 *supra* and accompanying text.

[125] 388 U.S. 41, 55 (1967).

[126] 18 U.S.C. § 2519(1)(1976). "Each of these requirements reflects the constitutional command of particularization . . . ." S. REP. No. 1097, 90th Cong., 2d Sess. 74-75, 101 (1968).

cularize in Title III was the requirement that wiretapping "be conducted in such a way as to *minimize*" interception of communications not authorized to be intercepted.[127] Congress clearly wanted to authorize only *specific* searches through electronic eavesdropping. Though this intent to particularize has been eviscerated by the Supreme Court in *Scott v. United States,*[128] the general congressional aversion to general surveillance in Title III is apparent.

Since the enactment of Title III, new developments in pen register technology and the law have made the argument for inclusion even more forceful. A modern pen register does far more than simply record numbers dialed: it also records the date and time of dialing and the ringing of incoming calls.[129] These features increase the temptation for frequent use because no great amount of manpower need be expended. Transfer of the data to key punch cards is easy and data bank use is thereby encouraged. Frequent, widespread use, and connection to a data bank, are the hallmarks of general surveillance today.

Moreover, the possibility of abuse by surreptitious use of a tape recorder or headphones to obtain full wiretap capability has been enhanced in newer models, in which a voice-activated switch can automatically turn on an attached tape recorder.[130] This new technology, which Title III did not contemplate, makes amending Title III to cover pen registers the logical way to update the Act to protect privacy of communications to the same extent intended in 1968.

The law governing pen registers has changed considerably since 1968, most notably in their removal from fourth amendment protection by *Smith v. Maryland.* The issue of the applicability of the fourth

---

[127] 18 U.S.C. § 2518(5) (1976) (emphasis added).

[128] 436 U.S. 128 (1977) (agents' *willful* noncompliance with minimization requirement did not necessitate supression of evidence so obtained). The problem might be attributed to the Act itself, which fails to define *minimization.* For critiques of the Supreme Court's analysis of Title III minimization requirements, see 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); 53 TUL. L. REV. 264 (1978).

[129] *See* note 3 *supra* and accompanying text.

[130] Note, *Circumventing Title III: The Use of Pen Register Surveillance in Law Enforcement,* 1977 DUKE L.J. 751, 759 n.45, *citing* Brief for Appellant at 10, United States v. Illinois Bell Tel. Co., 531 F.2d 809 (7th Cir. 1976).

amendment to pen registers did not squarely arise until 1973, but in several cases decided between 1973 and 1977 the courts consistently held that the fourth amendment did apply to pen registers.[131] This threshold protection against the use of pen registers must have been assumed in 1968.

Amendment of Title III to include pen registers is consistent with renewed congressional interest in citizen privacy. In the Privacy Act,[132] the Right to Financial Privacy Act of 1978,[133] the proposed Citizens Privacy Protection Act,[134] and the Foreign Intelligence Surveillance Act of 1978,[135] Congress has demonstrated a desire to protect privacy even in areas, such as wiretapping and bank records, where individual privacy might hamper law enforcement efforts. The Right to Financial Privacy Act is a particularly clear rejection of the Supreme Court's insensitivity to privacy needs. It overrules the *Miller* case by requiring that the government "reasonably describe" the bank records it wants, in addition to going through one of a number of formal procedures, each of which requires notice to the customer and often an opportunity to object.[136]

CONCLUSION

Smith v. Maryland is the latest in a line of cases excludng sophisticated surveillance devices from constitutional search requirements. Although there are persuasive arguments that current fourth amendment analysis is fundamentally misguided, a complete overhaul of search and seizure doctrine is unlikely. Attorneys can attempt to limit *Smith* to the situation of specific surveillance which occurred in that case. Associational claims under the first amendment are other ways

---

[131] *See* note 5 *supra* and cases cited therein. *See also* Note, *The Legal Restraints upon the Use of the Pen Register as a Law Enforcement Tool,* 60 CORNELL L. REV. 1028, 1044 n.94 (1975).

[132] 5 U.S.C. § 552a (1976).

[133] 12 U.S.C. §§ 3401-3422 (Supp. III 1979).

[134] S. 855 and H.R. 3486, 96th Cong., 1st Sess. (1979).

[135] 50 U.S.C. §§ 1801-1811 (1976).

[136] 12 U.S.C. §§ 3402, 3404-3408 (Supp. III 1979).

to lessen the impact of *Smith,* but those claims will be of doubtful value in the vast majority of pen register cases. The most effective solution seems to be a statutory one: congressional overruling of *Smith* by explicit incorporation of pen registers in Title III, or similar legislation by receptive states.

—John Applegate
Amy Grossman