Assumption of Risk Doctrine: Erosion of Fourth Amendment Protection through Fictitious Consent to Search and Seizure, The Fourth Amendment

JoAnn Guzik

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation

Available at: http://digitalcommons.law.scu.edu/lawreview/vol22/iss4/3

This Symposium is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
THE ASSUMPTION OF RISK DOCTRINE:
EROSION OF FOURTH AMENDMENT
PROTECTION THROUGH FICTITIOUS
CONSENT TO SEARCH AND SEIZURE

Taken individually, each increment of police power may be of little consequence . . . . But the process is insidious. Death takes little bites when devouring our freedom.

O. Garrison

I. INTRODUCTION

The prevention of indiscriminate governmental intrusion into the private spheres of an individual's life was a fundamental doctrine in the formation of American democracy. Protection against this invasion of privacy is guaranteed by the fourth amendment to the Constitution. Americans, as members of a nation of free people, value their security from unreasonable "searches and seizures." The foundation of this protection, however, is gradually being eroded. Judicial flexibility in the interpretation of the fourth amendment has expanded the scope of permissible and unregulated surveillance activities. The following hypothetical based on recent judicial decisions illustrates this point:

The year is 1982. The government has decided you are a possible suspect in a tax evasion investigation. You are placed under surveillance. A "mail cover" is placed on

©1982 by JoAnn Guzik
3. 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 Warrant 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.
4. The mail cover is a procedure used by law enforcement agencies, with the
your correspondence; a "pen register" is placed on your telephone line; this same pen register is monitoring the data requests you make on your home or office computer as well as any electronic banking transactions you complete by telephone; your business and personal acquaintances are surreptitiously recording your conversations with them and turning the tapes over to the government; your spouse consents to a search of your home; your business partner consents to a search of your business; and an electronic tracking device is monitoring where you drive your automobile. You have no knowledge of these activities.

At the end of an average day, the following information has been collected: The names and addresses of all your mail correspondents; the phone numbers (and subsequently the identity) of all individuals or data banks you have contacted by phone, and a record of the amounts of your telephone banking transactions; recorded or repeated conversations made in the privacy of your home or office; potentially incriminating evidence obtained in the consensual searches, as well as full documentation as to your public movements.

This information is then researched, compiled, and stored with the data the government regularly collects on every individual, a "dossier" is created presenting an in-depth picture of your private life.

cooperation of the Postal Service, to determine the identities of an individual's correspondents by observing and listing names and addresses on envelopes. See infra notes 119-36 and accompanying text.

5. The pen register is a device attached to a telephone line which records telephone numbers dialed from a particular phone. It does not intercept the contents of the conversation. See infra notes 95-118 and accompanying text.

6. See infra note 29 (defining consent monitoring); see generally infra notes 29-52.

7. See infra notes 139-40 and accompanying text.

8. An electronic tracking device, more commonly known as a "beeper," allows the police to monitor an individual's movements. See infra notes 137-38 and accompanying text.

9. Generally, all of these activities are not performed at the same time. The hypothetical serves to emphasize the cumulative effect of uncontrolled government surveillance and investigatory tactics.

10. A massive amount of information is compiled daily by the federal government. For example, one of the largest databanks is located in the central files of the Social Security Administration. Additional computer files are located within the FBI's National Crime Information Center. All state regulatory and licensing agencies maintain files on individuals within their jurisdictions. See A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY 29-101 (Report of the Project on Computer Data Banks of the Computer Science and Engineering Board, National Academy of Sciences)
If this hypothetical brings to mind "Big Brother" in George Orwell's 1984, understand that the above surveillance activities are routinely initiated at the discretion of law enforcement agencies, and in many instances may not be considered "searches" or "seizures" within the fourth amendment. The average member of society would be shocked, if not outraged, upon realizing the extent of his vulnerability to such surveillance. This vulnerability could, in the worst case, lead to withdrawal from social interaction and force into seclusion those individuals who value their privacy. At best, as uninhibited freedom to move about in society is destroyed, individuals will sense that their "privacy" is being invaded.

These uncontrolled invasions of privacy are sanctioned, in part, by the United States Supreme Court's use of fourth amendment "assumption of risk" analysis. The "assumption of risk doctrine" is a line of reasoning that denies constitut-

(1972); A. MILLER, THE ASSAULT ON PRIVACY: DATA BANKS, AND DOSSIERS 126-61 (1971).

The Privacy Act of 1974 established the Privacy Protection Study Commission to study the databanks of the federal government. 5 U.S.C. § 552a (1976 & Supp. IV 1980). One of the Commission's goals was to determine if the laws and regulations that require governmental agencies to obtain information on individuals are consistent with the right to privacy. The Commission's 1977 report found that government access to private information is virtually unrestricted. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 348 (1977) [hereinafter cited as PRIVACY REPORT].

Moreover, the Supreme Court has failed to provide protection in this area. See infra note 90. One authority refers to a Senate Subcommittee report that described only the databanks maintained by the executive departments and the independent governmental agencies; the report is 3500 pages long! Bigelo, The Privacy Act of 1974, 4 COMPUTER L. SERV. (CALLAGHAN) § 5-2, Art. 5 at 1 (1975). The Privacy Protection Study Commission found that the individual has no control over the disclosure of this information. PRIVACY REPORT at 13. Furthermore, the Commission recommended that Congress provide all individuals with a statutory expectation of confidentiality in these records. Id. at 362. One commentator has expressed that this accumulation of data damages an individual's freedom from surveillance: "The issue of privacy raised by computerization is whether the increased collection and processing of information for diverse public... purposes, if not carefully controlled, could lead to a sweeping power of surveillance by government over individual lives..." A. WESTIN, PRIVACY AND FREEDOM 158 (1967).

11. The only possible exception to this generalization concerns the use of beepers. The courts are split over whether or not the device violates fourth amendment search and seizure standards. See infra note 137 and accompanying text.

12. This would not assume any violation of a "constitutional" invasion of privacy, but rather the natural reaction of an individual who feels spied upon. Freedom of anonymity is threatened. The ability to be the master of one's own life is important to most people; when this ability is infringed upon, a person's privacy is breached. See generally A. WESTIN, supra note 10.
tional protection against governmental search and seizure relating to whatever information or activity an individual voluntarily exposes to the public or releases from his sole control. This comment will trace the inception and expansion of the doctrine and analyze its impact on the amendment's protection of individual privacy.

Initially, "risk" analysis was applied to allow the use of government informers and secret agents to infiltrate the very core of an individual's privacy. Eventually, the Supreme Court approved indiscriminate access to bank records by rationalizing that when an individual supplies information to a bank he assumes the risk that the information will be made known to the government. Although free access to bank records was subsequently prohibited by Congress, the Court's reasoning retains its destructive force through repeated application of risk analysis in related areas. The doctrine has been expanded to allow the use of information obtained by mail covers and pen registers. The possible ramifications from application of the doctrine to new technological developments in communication and information processing have not been totally realized; however, they may very well cause a further erosion of the fourth amendment and may necessitate additional Congressional action.

In viewing the major areas where risk analysis is applied, this comment emphasizes the cumulative effect of allowing a high degree of unregulated government surveillance. While the negative exponential effect on individual privacy rights results in an equal contraction of fourth amendment scope and force, this contraction only broadens police power which inherently reduces the ability to prevent unreasonable intrusions into private areas of a person's life. A framework devel-

13. The "assumption of risk" doctrine discussed in this comment should not be confused with the legal doctrine in the area of tort law that is also referred to as assumption of risk. The tort doctrine refers to assumed risk that may mitigate one's claims for damages.


16. See W. LAFAVE, SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT, § 2.7, 399 (Supp. 1981) [hereinafter cited as LAFAVE] where the author states: "It is the cumulative effect of these [surveillance] techniques which provides the strongest basis for the claim that they constitute an intrusion into . . . privacy . . . . [I]t is the breadth of the intrusion rather than its depth at any particular instant in time which is most threatening to privacy."
ops that can only create fear in the citizens and undermine the foundations of a free society.\textsuperscript{17} This comment will conclude that notification should be required in most of the "risk" areas to improve the ability of all individuals to secure their privacy and preserve their liberty. The effect of a notification requirement on law enforcement investigative activities would vary from being only minimal in some areas to severe in others. Such a balance must be struck, however, to temper the major fallacy in the "assumption of risk" doctrine: that alternatives exist for the individual who wishes to avoid assuming these risks.\textsuperscript{18} In a free-choice society, when there is no option but to accept governmental control, a means must be provided to protect the innocent from unrestrained police power. The minimal notification standard suggested in this comment would not provide a complete alternative to having such information exposed, but it would allow the opportunity to protest indiscriminate access to this information.

II. THE FOURTH AMENDMENT—PROTECTORATE OF PRIVACY

The Constitution of the United States contains no express language protecting privacy; however, judicial interpretation of the Constitution has established an implied "right to privacy."\textsuperscript{19} The constitutional provision most associated with

\textsuperscript{17} See generally A. Westin, supra note 10.

\textsuperscript{18} In analyzing the Court's application of risk theory, it becomes clear that in almost all situations the individual is held to have "assumed" a risk, even though he was unaware of this risk. That is, there may be an awareness of the natural risk one takes in confiding in another, but there is also a complete unawareness that the government also has immediate access to this information. Justice Marshall joined by Justice Brennan in a 1979 "risk" decision pinpointed the major fallacy in the Court's reasoning: "Implicit in the concept of assumption of risk is some notion of choice . . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." Smith v. Maryland, 442 U.S. 735, 749-50 (1979)(Marshall, J., dissenting).

\textsuperscript{19} A discussion of the development of the constitutional "right to privacy" is beyond the scope of this comment. It is important to note, however, that as the Court has developed an expanding privacy right in the area of equal protection, it has lessened the individual's right to privacy by substantially narrowing fourth amendment protections. On the development of the right to privacy, see generally Clark, Constitutional Sources of the Penumbral Right to Privacy, 19 VILL. L. REV. 833 (1974); Glancy, The Invention of the Right to Privacy, 21 ARIZ. L. REV. 1 (1979); and Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 SUP. CT. REV. 173. For the original analysis of the right to privacy concept, see Warren & Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890).
the concept of privacy protection is the fourth amendment.\textsuperscript{20} Freedom from unreasonable searches and seizures is a basic right of all citizens.\textsuperscript{21} To understand the damaging effects of risk analysis, it is necessary to realize that any contraction of fourth amendment protection results in destruction of privacy rights.\textsuperscript{22}

A. Surveillance and the Fourth Amendment—The Origin of Risk Analysis

1. Background

The Supreme Court’s delineation of permissive “eavesdropping” surveillance presents the first indication of risk analysis. In a 1928 Supreme Court decision, \emph{Olmstead v. United States},\textsuperscript{23} “wiretapping”\textsuperscript{24} was held not violative of the fourth amendment. Adhering to a trespass-property\textsuperscript{25} standard...

\begin{itemize}
\item[\textsuperscript{20}] See supra note 3. In general, fourth amendment protection is implemented in the following manner: When a law enforcement practice is considered unreasonable and is defined as a search or seizure, protection is implemented through application of the warrant clause. Upon showing of probable cause to a magistrate, a warrant will be issued which must particularize the person or things to be seized and the place to be searched. The evidence obtained in the search will only be admissible in court if the warrant requirements have been met. It is this judicially created “exclusionary rule” that provides the individual protection, and at the same time acts as a control on the police. For a detailed treatment of the exclusionary rule, see \textsc{LaFave, supra} note 16, at § 1.1, 3-20. For a concise analysis of fourth amendment substantive rules, see Amsterdam, \textit{Perspectives On The Fourth Amendment}, 58 Minn. L. Rev. 349, 356-61 (1974).
\item[\textsuperscript{21}] See generally \textsc{Landynski, supra} note 2.
\item[\textsuperscript{22}] Throughout this comment, reference is made to the contraction of fourth amendment protection. This generally refers to the Court’s determination that a particular investigative activity is not a search or seizure and therefore the warrant requirements of the fourth amendment do not have to be met. The requirement of particularity in the warrant clause emphasizes the intent of the framers of the constitution to forbid indiscriminate searches and seizures. Surveillance activities, by their very nature, allow seizure of information totally unrelated to the suspected criminal activity. It is this indiscriminate access to information that erodes the force of fourth amendment protections.
\item[\textsuperscript{23}] 277 U.S. 438 (1928).
\item[\textsuperscript{24}] “Wiretapping” involves the placement of an electronic listening device on an individual’s telephone line in order to overhear conversations. This procedure is now controlled by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1976).
\item[\textsuperscript{25}] The \emph{Olmstead} trespass-property standard was based on the concept that the fourth amendment protects “persons” and their tangible property (i.e. “houses, papers, and effects”) against unreasonable search and seizure. The fourth amendment would apply only if the police invaded or trespassed into one of these constitutionally protected areas. In \emph{Olmstead} there was no search because the telephone wires ex-
standard of fourth amendment interpretation, the Court reasoned that a wiretap does not intrude into a constitutionally protected area. Because an individual does not own the wires that carry his conversation beyond the walls of his home, there could be no trespass, and hence no search. Furthermore, a conversation possesses no tangible qualities that permit seizure. The majority opinion, which planted the seed for the development of risk analysis, suggested that persons who were exposed to warrantless electronic interception were volunteering their statements to the government by the very act of speaking to each other.26

Congress subsequently placed statutory controls on wiretapping,27 and the Court eventually held that such evidence, if illegally obtained, was inadmissible at trial.28 This statutory control, however, is not applicable to the surveillance activity of "consent or participant" monitoring effectuated through the government's use of secret agents and informers.29 In addition, the Supreme Court has been steadfast in its unwillingness to control the use of consent monitoring. The Court has consistently placed the activities of secret agents and informers, with or without recording devices, beyond the control of the fourth amendment.30 It is the Court's decisions in this

26. 277 U.S. at 466. Justice Brandeis, dissenting in Olmstead, wrote of the now famous "right to be let alone" guaranteed by the Constitution in the fourth amendment. Id. at 478 (Brandeis, J., dissenting).


29. Participant or consent monitoring involves three basic situations. In each situation, one of the parties is usually under the direction of a governmental agency and, without the knowledge of the other party, does one of the following: 1) uses an electronic device to transmit the conversation directly to a government agent, 2) consents to the use of a recording device by a government agent or informer to overhear or record the conversation, or 3) records the conversation himself. Throughout this comment, the terms "bugged" or "wired" refer to the informant's use of a recording or transmitting device. See Greenwalt, The Consent Problem in Wiretapping & Eavesdropping: Surreptitious Monitoring With the Consent of a Participant in a Conversation, 68 Colum. L. Rev. 189, 190 n.11 (1968). Governmental consent monitoring is specifically exempted from statutory control. See infra note 73.

30. It is argued by law enforcement agencies that the use of secret agents and informers is necessary for the detection of consensual crimes such as illegal narcotics transactions, prostitution, and tax evasion. The Supreme Court has apparently ac-
area that have given the assumption of risk doctrine its initial momentum. An examination of these decisions will illustrate the foundation and expansion of the risk doctrine.

2. Assumption of Risk Becomes a Judicial Doctrine

In the earliest consent monitoring case, *On Lee v. United States*, the Court upheld the use of evidence obtained through a wired informer. The informer, an old friend of On Lee's, twice entered On Lee's laundry and engaged in conversation in which On Lee made self-incriminating statements regarding illegal narcotics activity. Unknown to On Lee, the conversations were simultaneously transmitted to a federal agent outside the building. Relying on the *Olmstead* trespass doctrine, the Court held that On Lee had lost his fourth amendment rights by consenting to the informer's entry into the laundry. The majority could see no fourth amendment issues and stated that it would be "farfetched" to analogize the questions involved in eavesdropping on a conversation in which one party had consented to those involved in an unreasonable search and seizure. This emphatic advocacy of the use of informers was strengthened in 1971 when the Court refused to overrule *On Lee* in *United States v. White*.

In 1957, assumption of risk language expressly appeared in *Rathbun v. United States*, where the Court approved the use of evidence obtained through overhearing a conversation with the permission of one of the parties. The *Rathbun* Court held that "[e]ach party to a conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation." When such a risk is taken, the Court concluded, there is no violation of the privacy rights of any party to the conversation. In the midst of the development of the assumption of risk doctrine, the Court changed direction in basic fourth amendment interpretation.

32. See supra note 25.
33. 343 U.S. at 754.
34. 401 U.S. 745, 750 (1971). See infra notes 59-75 and accompanying text.
36. Id. at 111 (emphasis added).
In the next section, it will be seen that this development did little to suppress the use of risk analysis.

3. Transition Away From the Strict Trespass-Property Standard of Fourth Amendment Interpretation

In the early 1960’s, after decades of strict adherence to the *Olmstead* trespass doctrine, the Court decided that fourth amendment property-based analysis should give way to a determination of whether or not the privacy of the home is considered invaded by a particular surveillance activity. A “constitutional area of privacy” developed which allowed for a more flexible interpretation of whether or not a government activity constituted an unreasonable intrusion. The fourth amendment gained added strength when the Court also provided constitutional protection for overheard conversations.37 The implementation of fourth amendment safeguards no longer hinged on the occurrence of non-consensual physical trespass to seize tangible “papers and effects.” This transition, nevertheless, did not displace risk analysis. Instead of defining a particular government surveillance technique as nontrespassory and therefore permissible, the use of risk analysis addressed the activity of the individual. By placing this activity beyond the constitutional area of privacy, an individual was held to assume the risk of surveillance and was consequently denied fourth amendment protection.

In *Lopez v. United States*,38 the defendant was convicted of attempted bribery of an Internal Revenue agent. Under pretense of desiring to accept a bribe, the agent equipped himself with a recording device and induced Lopez to repeat an incriminating statement. Lopez’ conviction was based on both the agent’s testimony and the corroborating recording. The Supreme Court in upholding the conviction refused to accept the argument that Lopez’ consent for the agent to enter his office was negated by the agent’s falsification as to his purpose. As there was no unlawful invasion into Lopez’ constitutionally protected area of privacy, there could be no illegal

37. *Silverman v. United States*, 365 U.S. 505 (1961). In *Silverman* the Court held that a microphone driven into a party wall connected to the heating ducts of Silverman’s dwelling was a search, even though no physical trespass had occurred. In addition, the *Silverman* decision recognized that the intangible conversation had been seized. *Id.* at 511-12.

seizure of his words. The risk that Lopez took in offering the bribe included the risk that the offer would be accurately reproduced in court. The electronic device was not used to gain information that the government would not have otherwise obtained, it merely provided the "most reliable evidence possible." The device neither saw nor heard more than the agent.\footnote{In the dissent, Justice Brennan directly addressed the concept of risk analysis. He granted that Lopez had assumed a risk that the agent could repeat the conversation because this was a risk inherent in all communications not privileged by law. He cautioned, however, that this risk became significantly different with the introduction of recording devices. Because an individual in ordinary circumstances does not assume his conversation is being recorded, the risk doctrine becomes a fictitious waiver of privacy rights that is incompatible with free communication. Justice Brennan further reasoned that because there was no way to avoid this risk, and no alternative to mitigate it, there was no privacy unless an individual "keeps his mouth shut on all occasions."\footnote{In the mid-sixties, the trend of the Court's decisions to place restrictions on police activities\footnote{Hoffa v. United States\footnote{United States v. Hoffa, 385 U.S. 293 (1966).} upheld the jury tampering conviction of Teamster president James Hoffa. Federal agents contacted Partin, a local union official known to Hoffa. Partin was instructed to maintain close contact with Hoffa and gather information on Hoffa's activities.\footnote{Partin had spent over two months in his role as government informer. For a complete account of Partin's activities, see Note supra note 30, at 996-99.} the evidence\footnote{Id. at 439.\footnote{Id. at 450 (Brennan, J., dissenting). Chief Justice Warren joined the dissent in suggesting that On Lee should be overruled in light of the Court's abandonment of the trespass doctrine. 373 U.S. at 442 (Warren, C.J., concurring in result). The Chief Justice was able to distinguish Lopez on the basis of the corroborative value of the recording. Such a distinction indicates that, at least as far as the Chief Justice is concerned, the purpose of the evidence obtained appears to determine its constitutionality. Id. at 443.\footnote{See, e.g., Miranda v. Arizona, 384 U.S. 436 (1966); Escobedo v. Illinois, 378 U.S. 478 (1964); Massiah v. United States, 377 U.S. 201 (1964); Mapp v. Ohio, 367 U.S. 643 (1961).} 385 U.S. 293 (1966).} 39. Id. at 439.\footnote{Id. at 450 (Brennan, J., dissenting). Chief Justice Warren joined the dissent in suggesting that On Lee should be overruled in light of the Court's abandonment of the trespass doctrine. 373 U.S. at 442 (Warren, C.J., concurring in result). The Chief Justice was able to distinguish Lopez on the basis of the corroborative value of the recording. Such a distinction indicates that, at least as far as the Chief Justice is concerned, the purpose of the evidence obtained appears to determine its constitutionality. Id. at 443.}}
obtained by Partin was the basis for Hoffa's jury tampering conviction. Justice Stewart, writing the Court's opinion, referred to Justice Brennan's dissent in *Lopez* and held that Hoffa had assumed the risk inherent in normal conversation when he divulged information to Partin. The Court noted that Hoffa's misplaced confidence in Partin was a voluntary risk and as such was beyond the scope of constitutional protection. In denying Hoffa's claim that his privacy was invaded, Justice Stewart explained that fourth amendment protection was afforded only when an individual relied on the security of a protected area; in risking conversation with Partin, Hoffa did not rely on the security of his hotel room and had therefore assumed the risk of surveillance.

*Lewis v. United States*, decided the same day as *Hoffa*, upheld a conviction based on an undercover agent's purchase of narcotics from Lewis at his residence. Chief Justice Warren, in a unanimous opinion, stressed that because Lewis had turned his home into a commercial center and invited the agent in for a felonious purpose, he was not entitled to fourth amendment protection. The *Lewis* Court emphasized that the agent had entered the premises for the very purpose contemplated by Lewis and had heard, seen, and taken only what was necessary for that purpose. In *Hoffa*, there was no such invitation to the informer, Partin, for a specific and limited purpose. It would not have mattered if the sale in *Lewis* had taken place in another location, while in *Hoffa* it was imperative that Partin invade Hoffa's private life. This conflict in reasoning indicates the Court's willingness to condone this type of surveillance regardless of how offensive it may be to

---

44. Chief Justice Warren dissented on the merits. Justice Clark, joined by Justice Douglas dissented based on an improper grant of certiorari. Justice Douglas wrote a separate dissent arguing that he would reverse Hoffa's conviction if he were sure that the government had placed Partin in his role as informer. 385 U.S. at 349 (Douglas, J., dissenting).

45. 385 U.S. at 301 (quoting *Lopez v. United States*, 373 U.S. at 439).

46. Hoffa had argued that Partin's failure to disclose his role as a government informer negated any consent for Partin to be in the hotel room and that Hoffa's words were therefore illegally "searched." 385 U.S. at 300.

47. Id. at 301.


49. But see Kitch, *Katz v. United States: The Limits of the Fourth Amendment*, 1968 Sup. Cr. Rev. 133, 145 (suggests that the agent did not enter for the purposes contemplated by Lewis, but rather to obtain evidence against him).
the individual or to society. An inherently intrusive characteristic of these investigative activities is the inability to limit the surveillance to obtaining only incriminating evidence. Access is also gained to information unrelated to any alleged criminal conduct. The result is a "general search" for evidence in direct contradiction to the specific purpose of fourth amendment protection. An individual, whether innocent or guilty, loses control over the dissemination of information he desires to keep within the confines of the immediate conversation. Thus the rule remaining after Hoffa indicated that simple awareness of the mere presence of another person resulted in assuming both the risk of government surveillance and disclosure of private information.

Before continuing this review of the evolution of risk analysis in the area of consent monitoring, it is necessary to

50. This conflict in the Court's reasoning can be further illustrated by the fact that the Court could have dismissed Lewis' claim by relying on its decision in Lopez because there was no electronic recording involved in either case. Instead, the Court chose to address the fourth amendment secret agent issue. Furthermore, on the same day the Court decided Hoffa and Lewis, it also decided Osborn, where a court order was obtained to plant a wired informer. In Osborn, the Court held the evidence obtained by the informer was admissible. The Court stated: "There could hardly be a clearer example of 'the procedure of antecedent justification before a magistrate that is central to the Fourth Amendment' as a 'precondition of lawful electronic surveillance'." 385 U.S. 323, 330 (1966)(quoting Ohio ex rel. Eaton v. Price, 364 U.S. 263, 272 (1960) and Lopez v. United States, 373 U.S. at 464). Thus, in three opinions decided the same day, the Court found three different rationales for denying fourth amendment protection against the use of secret agents. See Kitch, supra note 49, at 135-40; Note, supra note 30, at 995-1019.

51. See LANDYNISKI, supra note 2.

52. See Note, supra note 30, at 999, where the author considers the likely reactions of citizens should they be asked to, rank the offensiveness of three practices:

(1) the police will be allowed to search your house without force during the daylight hours;

(2) the police will be allowed to offer your friends very strong inducements to report to them any illegal activities on your part;

(3) the police will be allowed to employ agents who may be strangers, business associates or friends, to invite or encourage you to take part in a criminal venture.

The clear state of constitutional law after Hoffa is that (1) represents an invasion abhorrent to the American way of life, but (2) and (3) are quite proper. The average citizen would hardly agree.

Id. at 1010. See Note, Interception of Conversations by Government Informers, 81 Harv. L. Rev. 191, 193 (1967)(the Hoffa decision presents a "gaming view of the fourth amendment"). Contra Greenwalt, supra note 29, at 225 (widespread participant monitoring would likely have only a "subtle negative effect on people's willingness to communicate").
digress and examine the Court’s landmark fourth amendment
decision in *Katz v. United States*.\(^5\) This 1967 decision was
viewed as a timely redefinition of the scope of fourth amend-
ment protection against electronic surveillance.\(^4\) *Katz* was
convicted of interstate transmission of gambling information.
Evidence obtained through a warrantless wiretap on a public
telephone was used against the defendant. The Supreme
Court reversed his conviction and reaffirmed the demise of the
Olmstead trespass doctrine by focusing on the result of the
surveillance rather than the method utilized.\(^5\) Justice Stew-
art, writing for the Court, found no “constitutional signifi-
cance” in the government’s claim that the listening device did
not penetrate the wall of the telephone booth. Furthermore,
the Court declined to adopt a rigid formulation of a constitu-
tionally protected area, but indicated a broader interpretation
by noting that Katz was justified in relying on the privacy of
the telephone booth. This transition to the individual’s intent
to keep his activities private broadened the area of constitu-
tionally protected privacy. Justice Stewart set forth the new
standard to determine the scope of fourth amendment protec-
tion: “What a person *knowingly* exposes to the public, even in
his own home or office, is not subject of Fourth Amendment
protection . . . . But what he seeks to preserve as private,
even in an area accessible to the public, may be constitution-
ally protected.”\(^6\)

Declaring that the fourth amendment could not be trans-
lated into a general constitutional right to privacy, the Court
avoided defining the specific interests the amendment does
protect. The Court did find, however, that the fourth amend-
ment provided protection against “certain kinds of govern-
mental intrusions” and that the amendment should be inter-
preted as protecting “people,” not “areas.”\(^7\) This
indecisiveness may be what caused the transformation of the
concurring opinion in *Katz* to the one generally used to define
fourth amendment protection. Justice Harlan, in his concur-
rence, suggested a twofold test to determine if an activity de-

---

54. Kitch, *supra* note 49, at 133; see Amsterdam, *supra* note 20, at 382 (“*Katz*
is a watershed in fourth amendment jurisprudence”).
55. See *supra* note 25.
56. 389 U.S. at 351 (emphasis added).
57. *Id.* at 50-53.
served constitutional protection: First, an individual must exhibit an actual (subjective) expectation of privacy, and second, that society recognize this exception as reasonable. Admittedly, this is no more precise than the majority opinion, but it was hoped that the combination of the two would provide a flexible vehicle to allow increased constitutional protection in a rapidly advancing technological environment.

B. The Conflict Between “Reasonable Expectation of Privacy” and “Assumption of Risk”

To understand the conflict between the Katz "justifiable reliance" or "reasonable expectation" privacy tests and the risk doctrine, it must be realized that any misdirected interpretation of limitations imposed by Katz leads to a broad application of the risk doctrine. For example, in a situation where it is determined that an individual maintains an "unreasonable" expectation of privacy, he is considered to "knowingly" expose this information to the public and thereby assumes the risk of further publication or transmission of his private activities.

Although Katz defined a privacy oriented standard for protection against government surveillance, the decision left open the question of whether the government's use of consent or participant monitoring would be constitutionally proscribed under this new standard. Therefore, to complete this analysis of the evolution of the assumption of risk doctrine, it is necessary to examine the 1971 decision in United States v. White which considered consent monitoring.

The White decision, and the subsequent opinions which relied on its reasoning, may have done the greatest damage to the viability of Katz as a major precedent for the protection of privacy. Federal agents, acting without a warrant, equipped an informer with a transmitting device to monitor conversations with White, a suspected drug dealer. These conversations, concerning the price and delivery of heroin, were overheard by federal agents. The agents' testimony regarding the

58. Id. at 361 (Harlan, J., concurring).
59. Contra Amsterdam, supra note 21, at 383-84 (the test developed by Justice Harlan in his concurring opinion "destroys the spirit of Katz and most of [its] substance"). For a complete discussion of the Katz decision, see Kitch, supra note 49.
60. 401 U.S. 745 (1971).
illegal drug transactions resulted in White's conviction. On appeal, the seventh circuit relied on *Katz* and overturned the conviction by holding that the government's warrantless electronic eavesdropping violated the fourth amendment.

The Supreme Court, in a plurality opinion, reversed the seventh circuit on two grounds. Four Justices found that White did not present a fourth amendment issue in light of the *Katz* and Hoffa decisions, and alternatively, that the seventh circuit erred in applying *Katz* retroactively. The White Court revitalized the assumption of risk doctrine by holding that a person who "contemplat[es] illegal activities must realize and risk that his companions may be reporting to the police." The Court also upheld the viability of *On Lee, Lopez, Lewis* and *Hoffa*.

Justice White, writing for the plurality, focused on the risks undertaken by the speaker rather than using either of the tests proposed by Justices Stewart or Harlan in *Katz*. If there is any possibility or probability that an individual's colleague is cooperating with the police, then there is no constitutional protection because the speaker assumed this risk. Furthermore, Justice White found no persuasive difference in

61. The agents had monitored a total of eight conversations: Four in the informant's home and four in either White's home, the informant's car, or a public restaurant. *Id.* at 747.
62. United States v. White, 405 F.2d 838 (7th Cir. 1969) (en banc).
63. Justice White, writing for the plurality, held that the informant's use of the transmitter was not violative of the fourth amendment any more than the informant's own testimony would be. Justices Stewart, Blackmun, and Burger agreed. The four Justices refused to apply *Katz* retroactively. 401 U.S. at 754; see infra note 64. Justice Black concurred on the grounds that eavesdropping by electronic devices is not a search and seizure within the fourth amendment. 401 U.S. at 754. Justice Brennan, concurring, agreed on the retroactivity issue, but stated that a warrant should be required both where an informant secretly records the conversation and where he secretly transmits the conversation to the police. *Id.* at 755. Justice Douglas dissented on the grounds that electronic surveillance violates the fourth amendment whether by recording or transmitting and that *Katz* should be applied retroactively. *Id.* at 468-95. Justice Marshall dissented on the grounds that electronic surveillance violates the fourth amendment and that *Katz* should be applied retroactively. *Id.* at 795-96. Four of the Justices, Marshall, Douglas, Harlan, and Brennan, also believed that *On Lee* should be overruled in light of *Katz*. The seventh circuit had so held by overturning White's conviction. Justice Brennan also went further and suggested that *Lopez* also be overruled. *Id.* at 755. The split on the Court was 4-4 on the validity of consensual monitoring, and 5-4 on the use of an informant to do the monitoring.
64. The Court had previously held in Desist v. United States, 394 U.S. 244 (1969), that *Katz* would not be applied retroactively.
65. 401 U.S. at 752.
66. *Id.* at 749-50, 749 n.3.
the risk simply because the participant to the conversation was bugged rather than unbugged. Again reviving the Lopez "reliable evidence" argument, Justice White stated the need to avoid creating constitutionally sanctioned barriers to accurate and reliable evidence. Apparently, the use of the risk doctrine allows the justification for warrantless searches to turn on the degree of incriminating evidence accumulated. Justice White further reasoned that since there is no constitutional prohibition against the use of unaided testimony, there should be no denial of the use of a more accurate version of the same testimony. The opinion clearly avoids any attempt to place judicial or constitutional controls on the government's use of secret agents.

Justice Douglas, dissenting, found electronic surveillance to be a great threat to human privacy. He questioned how most forms of this activity could ever be considered reasonable within the meaning of the fourth amendment. Analyzing the Court's decisions in this area and recognizing the lack of self-restraint on the part of law enforcement officials, he concluded that the application of the warrant clause in this area was essential to the preservation of a free society. Justice Harlan, in a separate dissent, examined the assumption of risk concept and concluded that because it is the law itself that determined what risks to impose on society, the judiciary should not simply mandate societal expectations. To determine if the risk of surveillance should be imposed on citizens, he suggested that the extent of the impact on an individual's sense of privacy should be balanced against the usefulness of a form of surveillance as a technique of law enforcement.

Consequently, despite the constitutional standards enunciated in Katz and the statutory controls on electronic surveil-

67. Id. at 752.
68. Id. at 753. See supra note 39 and accompanying text.
70. 401 U.S. at 756 (Douglas, J., dissenting).
71. Id. at 765. In a situation like White where government authorities plant an informer based on a high degree of suspicion, there is no reason why a warrant could not be obtained based on probable cause as in Osborn. See supra note 50; see generally Comment, Electronic Eavesdropping And The Right To Privacy, 52 B.U.L. Rev. 831 (1972).
72. 401 U.S. at 786 (Harlan, J., dissenting).
lance through federal legislation, the government is totally unrestrained in the use of the secret agents and informers. In failing to delineate any recognizable difference between monitored and unmonitored agents, the Court has ignored its own decisions criticizing the inherent evil nature of electronic eavesdropping. As a result, an innocent person is placed in an untenable position; he can be subjected to surveillance and when the evidence proves valueless the invasion of his privacy becomes justified because he assumed the risk of having a conversation that might have produced evidence for the government.

Commentators have espoused the need for fourth amendment protection in this area, and most agree that the White opinion cannot be rationally justified in light of Katz. An individual does not knowingly expose his words to be recorded or used against him by a government agent. Under Katz this expectation of freedom from electronic recording is certainly considered reasonable by society. It becomes essential to remove the fictitious notion of consent and apply Katz as a general prohibition against electronic surveillance by government informers. Furthermore, as long as the police are allowed to freely plant informers, an individual is left with no choice: If electronics surveillance is suspected, a person will be afraid to talk to anyone either in the privacy of his home, office, or on the telephone, and if the individual fears the use of an unbug-

---

73. 18 U.S.C. §§ 2510-2520. See supra note 29. Government participant monitoring is specifically exempted from statutory control: "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c).


75. In White, Justice White specifically focused the holding on the typical criminal. 401 U.S. at 752-53. Even if it is granted that the typical criminal would not change the substance of his communication when he is aware of assuming the risk of surveillance, the same cannot be said for the innocent citizen who becomes aware that he has assumed this risk. "[T]alk about 'criminals' assuming the risks means that we all assume the risks." Amsterdam, supra note 20, at 470 n.492. Such an all or nothing approach to assuming the risk of surveillance does not recognize that individuals may change their expectations of privacy in response to the police activity involved. Note, supra note 69, at 254.

76. One commentator declares that this notion of consent is an absurdity. Elsewhere in the law, any voluntary consent would be vitiating by the fraudulent representations of another. Posner, supra note 19, at 188.
The following sections of this comment consider the wide range of additional surveillance activities allowed under an assumption of risk theory. In these areas, the government does not utilize a third party to invade an individual's privacy, but is permitted to gain access to private information without an individual's knowledge or knowing consent. The narrowing scope of fourth amendment protections precludes protection against these unreasonable searches and seizures.

III. THE PERVERSIVENESS OF RISK ANALYSIS

A. Bank Records

In *Miller v. United States* the Supreme Court extended the assumption of risk doctrine to allow access to an individual's bank records. Legislative reaction to *Miller* was swift and to the point: Congress passed the Financial Privacy Act of 1978 in direct response to the Supreme Court's decision.

77. Amsterdam, supra note 20, at 407. Professor Amsterdam also emphasizes that a distinction must be made between the risks inherent in normal conversation and those that occur when the government introduces informers into the conversation. The latter situation creates the danger of destroying liberty. He further notes that even if there is a normal risk assumed by an individual, the government should not be unrestrained in adding to those risks. *Id.* at 406.

As more and more individuals become aware of this destruction of liberty, they are taking steps to protect themselves from surveillance. The demand for anti-bugging devices has grown steadily in recent years. Advertisements for surveillance detection devices are found in many newspapers and magazines throughout the country. For example, the March 1982 edition of *United Mainliner*, a magazine distributed by United Airlines to all its passengers, featured an advertisement for the "007 Bionic Briefcase." This unobtrusive looking case can sweep nearby telephone systems to detect wiretaps and phone bugs, warn of any electronic bugging device in the vicinity, and allow the person holding the case to monitor conversations. *United Mainliner*, March 1982, at 18. One can also purchase briefcase lie detectors, automobiles with built-in debugging, and electronic eavesdropping detectors that are "disguised as packs of cigarettes." *Quade, Lawscape, For Someone on Your Gift List*, 69 A.B.A. J. 142 (1983).


80. "[This act] is a congressional response to the Supreme Court's decision in *United States v. Miller*. . . . The Court did not acknowledge the sensitive nature of these records . . . and decided . . . the customer had no constitutionally recognizable privacy interest in them . . . Congress may provide protection for individual rights beyond that afforded in the Constitution." H.R. 1383, 95th Cong., 2d Sess., 124 Cong. Rec. 9306 (1978). This comment suggests a similar standard to protect privacy in some "risk" areas.
Under the Act governmental access to financial records is prohibited unless:

1. The customer authorizes the disclosure in conformance to strict waiver requirements; or
2. Disclosure of the records is in response to an administrative subpoena or summons which will be issued only if there is reason to believe the records relate to a legitimate law enforcement inquiry; and notification is given to the customer on or before the bank receives the order. This notification procedure allows the customer ten days in which action may be taken to prevent disclosure; or
3. General federal search warrant requirements are met.

As can be seen, the Financial Privacy Act precludes the

81. 12 U.S.C. § 3402 reads in part:
   No Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and:
   (1) such customer has authorized such disclosure in accordance with section 3404 of this title;
   (2) such financial records are disclosed in response to an administrative subpoena or summons which meets the requirements of section 3405 of this title;
   (3) such financial records are disclosed in response to a search warrant which meets the requirements of section 3406 of this title;
   (4) such financial records are disclosed in response to a judicial subpoena which meets the requirement of section 3407 of this title; or
   (5) such financial records are disclosed in response to a formal written request which meets the requirements of section 3408 of this title.

82. 18 U.S.C. § 3404 provides in pertinent part:
   (a) A customer may authorize disclosure if he furnishes to the financial institution and to the Government authority a signed and dated statement which:
      (1) authorized such disclosure for a period not in excess of three months; (2) states that the customer may revoke such authorization at any time; (3) identifies the financial records to be disclosed; (4) specifies the purpose for which, and the Government authority to which, such records may be disclosed.

83. 12 U.S.C. §§ 3405-3407 contain similar provisions regarding the issuance of an administrative or judicial summons, or formal written request from a Government authority.

84. 12 U.S.C. § 3406 provides in pertinent part:
   (a) A Government authority may obtain financial records if it obtains a search warrant pursuant to the Federal Rules of Criminal Procedure.
   (b) No later than ninety days after the Government authority serves the search warrant, it shall mail to the [customer] a copy of the search warrant.
government from obtaining personal records unless advance notice is given. This notification requirement provides protection against indiscriminate access by investigative agencies seeking to escape the warrant requirement. It appears feasible that the basic scheme of this act can be utilized to provide protection in other areas where the Court has applied the risk doctrine. 85

Although the Miller decision, as it pertains to bank records, is moot, the Court’s holding provides considerable room for a volatile expansion of risk analysis into related areas. It is therefore necessary to consider the reasoning in the Miller opinion and its effect on privacy rights.

Miller was convicted of conspiring to defraud the government of tax revenues due from his operation of an illegal whiskey distillery. Responding to a subpoena from the United States Attorney, Miller’s banks surrendered evidence necessary for Miller’s conviction. The evidence included copies of checks written by Miller as well as his complete account records. In upholding the conviction, the Supreme Court looked to the Hoffa 86 decision and reasoned that because Miller had placed this information outside any zone of constitutionally protected privacy, his fourth amendment rights were not violated. 87

The Miller Court declared that because the documents were not Miller’s property, but rather property of the bank, there was no invasion of his privacy. By this analysis, the Court appears to have returned to a property-based standard. 88 The importance of this transition is the potential neg-

---

85. The conclusion of this comment will point out the areas where government surveillance in related areas could be controlled by similar statutory regulation.
87. 425 U.S. at 440.
88. The Court’s return to this standard is further complicated by the passage of the Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970)(codified as amended at 12 U.S.C. § 1829b (1976 & Supp. IV 1980)), requiring banks to maintain certain records. Checks drawn on the bank and presented for payment, account statements, and records necessary to reconstruct a checking account and furnish an audit trial are just some of the records that must be maintained. In an incredibly circuitous line of reasoning, the Miller Court assumed that Miller had lost any reasonable expectation of privacy concerning the bank records when Congress enacted this legislation. Because the express purpose of the Act was to require that records be kept for their usefulness in criminal, tax, and regulatory investigations, the individual (Miller) could not expect them to be private. 425 U.S. at 441. This broad grant of statutory control over constitutional privacy protection undermines Katz and emphasizes the erosion of fourth amendment protections by the Supreme Court. Miller and Katz
ative effect on a society where massive amounts of information are required daily for basic transactions. The Court's failure to provide privacy protection for individuals in our information gathering society is clearly stated in the following passage:

This Court has repeatedly held that the Fourth Amendment does not prohibit the obtaining [of] information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for the limited purpose and the confidence placed in the third party will not be betrayed.\(^8\)

The deleterious effect of this passage is compounded by the Court's determination that Miller, in using a negotiable instrument (a check), had taken a risk that the bank would convey pertinent information to the government. If this reasoning is valid, a startling paradox is presented by the above passage: How can an individual assume information will be used for a limited purpose and that his confidence will not be betrayed, and at the same time assume the risk that the opposite will occur simply as a result of the otherwise completely legal means by which he was required to convey that information?\(^9\)

\(^8\) 425 U.S. at 443 (emphasis added).

\(^9\) The Supreme Court has not yet ruled that the right to privacy limits government powers in the collection of data concerning individuals. See supra note 10 for a discussion of data collection by the government. In Whalen v. Roe, 429 U.S. 589 (1977), the Court upheld the legality of a New York statute requiring physicians and pharmacists to forward to state authorities copies of prescriptions for medicines containing certain narcotics. The majority opinion, while recognizing the threat to privacy that such data collection involved, found legitimate state goals to be the overriding concern. Justice Brennan, in his concurrence, noted that data collection must be limited if the individual is deprived of a constitutional right. Id. at 606-07. Justice Stewart, in a separate concurrence, however, suggested that the Constitution, to the extent that it protects privacy, does not recognize a "general interest in freedom from disclosure of private information." Id. at 607-08.

The Freedom of Information Act, 5 U.S.C. § 522 (1976) and the Trade Secrets Act, 18 U.S.C. § 1905 (1980), both govern the control of data that is in the possession of the federal government. The Court has held that neither of these acts grant an implied private right of action to enjoin disclosure by the government agency.
The dissent in Miller relied on Burrows v. Superior Court, a California decision in which the acquisition of bank records was found violative of both the fourth amendment under Katz, and the California state constitution. Commentators have praised Burrows as being the correct approach for the protection of privacy right of citizens. The reasoning of the California court directly supports the main thesis of this comment: "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."

In light of the rejection of property concepts in defining fourth amendment protection in the Katz case, the Miller decision seems to be an anomaly. Had the Court looked at the totality of the information gathered, rather than at who possessed the documents, it could not have found that Miller knowingly exposed such personal information to the public.


91. 13 Cal. 3d 328, 529 P.2d 590, 118 Cal. Rptr. 166 (1974). The Burrows court expressed concern over the totality of information that is revealed by depositor records: "In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits, and associations. Indeed, the totality of bank records provides a virtual current biography." Id. at 247, 529 P.2d at 596, 118 Cal. Rptr. at 172. The California Supreme Court has shown a willingness to grant extensive expectations of privacy to its citizens. For example, in People v. Krivda, 5 Cal. 3d 357, 86 P.2d 1262, 96 Cal. Rptr. 62 (1971), the court held that an individual maintains a constitutionally protected privacy interest in the contents of his trash can placed outside his home.


93. 13 Cal. 3d at 247, 529 P.2d at 595, 118 Cal. Rptr. at 172.

94. The Miller decision appears to have far-reaching ramifications. In United States v. Payner, 447 U.S. 727 (1980), IRS agents arranged to obtain bank records by burglary. The Court without hesitation decided under Miller that the depositor had no protectable fourth amendment interests in the copies of checks and deposit slips that had been retained by the bank. In Reporters Comm. for Freedom of the Press v. American Tel. & Tel. Co., 593 F.2d 1030 (D.C. Cir. 1978), cert. denied, 440 U.S. 949 (1979) the court, relying on Miller, held that telephone subscribers have no fourth amendment basis for challenging government inspection of their toll records, since subscribers, like bank depositors, have taken the risk in revealing their affairs to third parties. This risk includes the possibility that the information will be conveyed by that person to law enforcement officials, either voluntarily or in response to compulsory process.
B. Pen Registers

The cumulative effect of the erosion of fourth amendment protections stemming from the application of the risk doctrine is most evident in the government use of "pen registers."95 A pen register is used to determine the identity of the individuals with whom a suspect communicates by telephone. The device is attached to telephone company equipment at the request of an investigative agency and records the numbers dialed out on the telephone line. The numbers of incoming calls are not recorded.96 Federal legislation prohibiting the interception of telephone conversations is not applicable to pen registers97 because the register does not intercept the communication itself.98 The use of the pen register was not considered by Congress to be a serious threat to an individual's privacy.


The pen register is a device attached to a given telephone line usually at a central telephone office. A pulsation of the dial on the line to which the pen register is attached records on a paper tape dashes equal in number to the number dialed. The paper tape then becomes a permanent and complete record of outgoing numbers called on the particular line . . . . The pen register cuts off after the number is dialed on outgoing calls and after the ringing is concluded on incoming calls without determining whether the call is completed or the receiver is answered.

There is neither recording nor monitoring of the conversation.

Id. at 807. A TR-12 Touch-Tone decoder is a device analogous to the pen register. It is used for touch-tone telephones and prints out the number in arabic numerals rather than a series of dashes. Note, The Legal Constraints Upon the Use of a Pen Register as a Law Enforcement Tool, 60 CORNELL L. REV. 1028, n.3 (1975).

96. There are devices termed "grabbers" or "trappers" that are able to monitor incoming numbers. They are used frequently by telephone companies to detect misuse of their equipment, primarily to trace obscene phone callers. Investigative agencies also make use of these devices to learn the identity of persons calling into a phone. See, e.g., In re Application of the United States of America for an Order Authorizing an In Progress Trace of Wire Communications Over Tel. Facilities, 616 F.2d 1127 (9th Cir. 1980)(grabber used to learn the identity of callers to three phones: IRS suspected that the phones were being used for an illegal gambling operation).


98. S. REP. No. 1097, 90th Cong., 2d Sess. 90 (1968) reads in part:

Paragraph 4 of [§ 2520] 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 . . . . The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register," for example, would be permissible . . . . The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication.
In a 1977 Supreme Court case involving the telephone company's refusal to install a pen register, the Court did not consider any fourth amendment issue but affirmed the specific legislative exclusion. Decisions in the lower courts were in conflict about the degree of intrusion presented by the use of a pen register. Some courts, in granting orders for the installation of the device, assumed the activity was a search and seizure, while other jurisdictions deemed it unnecessary to determine if a search was taking place. The ninth circuit, in 1977, directly addressed the fourth amendment issue and held that the use of pen registers did not violate substantive fourth amendment standards. Relying on Katz, the ninth circuit held that an individual's expectation of privacy attached to the context of the conversation and not to the fact that a conversation occurred.

In an effort to resolve this conflict, the Supreme Court granted certiorari in Smith v. Maryland. In Smith, a young woman was robbed and then began receiving obscene phone calls from the alleged thief. After tracing the suspect, the police requested the telephone company to install a pen register. No warrant or court order was obtained. The register revealed a call to the victim's home. On this basis a warrant was obtained and a subsequent search produced a phone book opened to the victim's number. Smith's conviction was based primarily on this evidence.

Recognizing that Smith had no property right in the telephone company's equipment, the Court addressed his claim that his reasonable expectation of privacy was violated by the use of the pen register. Justice Blackmun, writing for the majority, did great violence to the Katz rationale by stating that people in general probably do not maintain any expectation of privacy in the telephone numbers they dial. It is difficult, if not impossible, to reconcile this reasoning with Katz. Considering the Katz ruling that the fourth amendment protects "people," and that only what an individual "knowingly" ex-

100. See, e.g., Application of the United States of America in the Matter of an Order Authorizing the Use of a Pen Register, 538 F.2d 956 (2d Cir. 1976).
101. See, e.g., United States v. John, 508 F.2d 1134 (8th Cir. 1975).
102. Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254 (9th Cir. 1977).
103. 442 U.S. 735 (1979).
104. Id. at 743.
poses to the public will be denied protection, it cannot be realistically concluded that Smith knowingly exposed to the public the fact that he dialed the young woman's number. It destroys any meaningful interpretation of the word "knowingly" to suggest that every individual exposes his partners in communication to the public by the simple act of dialing his telephone.108

In applying the assumption of risk analysis to Smith's phone calls, the Court noted that it was irrelevant that he made the calls in the privacy of his own home. Regardless of where he had placed the call, he still would have given the number to the phone company. In conclusion, Justice Blackmun acknowledged that even if Smith had entertained an expectation of privacy as to his phone calls, this was an area of privacy that society would not recognize as reasonable.106 This analysis avoids the result of obtaining the numbers an individual dials. The number is used to locate and identify the person whose numbers are dialed, and to determine the relationship of a suspect to a particular location he calls. Thus, when any individual dials his phone he is assuming the risk that the telephone company will reveal the number to the police, and that the police may subsequently identify the parties to the conversation.

Justice Marshall, dissenting, emphasized the underlying fallacy in the application of the risk doctrine: because the telephone has become a personal and professional necessity, the individual cannot help but assume the risk of surveillance.107

105. Furthermore, when Justice Stewart made the determination in Katz that what an individual "knowingly" exposes to the public is not given constitutional protection, he was referring to the Lewis situation, where the individual invited the government agent into his home for the limited purpose of committing a crime. He was not mandating a general prohibition of constitutional protection for any and all information that an individual makes public. 389 U.S. at 351. Justice Stewart dissented in Smith on the basis of the Katz decision. 442 U.S. at 745.

106. 442 U.S. at 743.

107. Id. at 748 (Marshall, J., dissenting). See supra note 18 for a discussion of Justice Marshall's dissent in Smith. Justification for pen registers is found in one area of investigation. When the use of the phone is itself the substantive crime that is being committed, as in the making of obscene phone calls, there is probably no other means to apprehend the criminal. This justification disappears when the register is used to obtain all the numbers dialed by an individual who is suspected of some other type of illegal activity which is not strictly limited to the use of a telephone. This activity may have no relationship at all to the information gained by the law enforcement agency. This data is used to identify acquaintances of the suspect and create an
A number of technological innovations designed to improve the quality and efficiency of communication are severely threatened by the Smith reasoning. Today, the primary means of transmitting information, often in forms other than the human voice, from one area to another is by the use of telephone lines. This advanced concept of information transmission is not limited to businesses possessing computer networks. Anyone today may gain access to a number of modern data systems.

For example, an individual may pay bills or make transfers from one bank account to another simply by pressing a particular sequence of numbers on a Touch-Tone Phone. If an investigative agency were trying to identify an individual's bank in order to apply for a warrant or bank record subpoena, and the suspect was unlucky enough to have a pen register placed on his telephone line, the pulses that pay his bills and transfer his funds would also direct the police to his bank.

The greatest threat created by use of a pen register exists in the use of a computer, either at home or in the office. In the case of the home user, he merely purchases an "acoustic coupler" and his home computer becomes a device that can communicate with various data-banks and information agencies. By paying a small fee, the computer can be linked to a wide variety of services. An individual can make his own airline reservations, contact stock exchanges, and receive Dow Jones reports in the privacy of his own home. A pen register

---

108. See, e.g., R. Glasgel, Basic Techniques in Data Communications, (Rev. 2d Ed. 1979).

109. For example, in using Bank of America phone banking, a sequence of numbers pressed on a touch-tone phone activates a computer at the bank. Dollar amounts are then pressed on the phone buttons, and the computer at the other end of the line enters and records the transaction. The bank will make the necessary transfers to the accounts activated (e.g. utility bills, credit card payments, auto and home loan payments, etc.) Bank of America, Brochure: Versatell Phone Banking, AD-767 (Oct. 1981). The pen register although not identifying the specific accounts is recording the dollar amounts as well as any code numbers entered.

110. The Privacy Protection Commission was particularly concerned over the loss of privacy rights from Electronic Fund Transfers. Privacy Report, supra note 10, at 116.

111. An "acoustic coupler" is a device that converts the standard telephone into a data transmission device. See generally Glasgel, supra note 108.

112. Source is a data-bank service company. Their brochure lists the following...
installed on the telephone line of an individual who utilizes all these services would reveal the identity of all the data banks he contacted. This potential surveillance capability is magnified if a central computer is used to store all the information obtained from surveillance of a broad range of individuals or business firms. A massive cross pattern of communication and correlative acquaintances could be revealed. It has been suggested that the most significant threat to personal freedom in the future will be the inevitable link of the pen register and the computer.\footnote{113}

There is electronic equipment available today that can be placed anywhere along a data transmission line. Such equipment is capable of copying, storing, reading, and decoding any and all data transmitted.\footnote{114} There is no aural acquisition as the information is basically recorded in \emph{readable form} as it flows along the telephone line. These “data monitors” are primarily used to check the accuracy of the data flow; however, the potential for abuse is more than obvious. The data monitor, in effect, eavesdrops on the electronic pulses that flow along the line. If the information being monitored is considered “content,”\footnote{115} and if the monitor is intercepting the communication, protection may be afforded under federal wiretapping legislation.\footnote{116} However, in applying the Court’s reasoning in \textit{Smith}, in conjunction with \textit{Miller} and the traditional statutory interpretation of “content inception,” there remains an undefined issue. If the register or data monitor is installed on telephone company equipment, in which the individual has no interest under \textit{Smith}, and under \textit{Miller} he has no interest in the information he voluntarily releases to a

\footnote{113} \textsc{Westin}, supra note 10, at 43. \textit{Newsweek}, reported that it is estimated that 3 million home computers will be sold in 1982 alone. Worldwide sales of home computers are expected to reach 50 million by 1985. \textit{Newsweek}, Feb. 22, 1982, at 50.

\footnote{114} Data monitors are produced by a large number of firms. Some representative examples are Halcyon Communications, Inc., San Jose, Ca. and Atlantic Research Inc., Alexandria, Va.

\footnote{115} 18 U.S.C. § 2510(8) defines “content” as follows: “‘Contents’ . . . includes any information concerning the identity of the parties to [the] communication or the existence, substance, purport, or meaning of [the] communication.”

\footnote{116} See supra notes 24, 73 & 115 for pertinent sections of the Title III wiretapping legislation.
third party, it is possible for the Court to deny protection to the individual whose data transmission is monitored. The uncertainty as to the ability of federal legislation to provide protection in this type of situation was foreseen by one commentator who noted that recent legislation in the area is a "technological anachronism" because of its failure to deal with the new computer technology and new forms of data transmission.

This expansion of risk analysis which denies fourth amendment protection to individuals when using the telephone illustrates the far-reaching effect of unrestrained surveillance. There is no way for the individual to realize he is being monitored in this way, unless the government later acknowledges the use of a pen register or data monitor. A statutory notification requirement prior to installation of the devices would afford a substantial degree of privacy protection. If the individual fails to prevent the surveillance, he is at least aware that his communications are being monitored.

C. Mail Covers

The Supreme Court has not ruled on the constitutionality of mail covers. The Court of Appeals for the Ninth Circuit, however, relied on the Miller bank records decision and applied assumption of risk analysis in Choate v. United States to mail covers. Choate first came to the attention of law enforcement authorities when an undercover informant alleged Choate was connected with a cocaine importation

117. In reading the definition of "contents," supra note 113, the data transmission appears protected; however, a literal reading of the statute also appears to prohibit the use of pen registers because the numbers obtained lead to the identity of the parties to the communication.

118. MILLER, supra note 10, at 161-68.

119. Under the postal regulations, a mail cover is defined as follows:

"Mail cover" is the process by which a record is made of any data appearing on the outside cover of any class of mail matter, including the contents of any second; third; [or] fourth-class mail matter as now sanctioned by law, in order to obtain information in the interest of (i) protecting the national security, (ii) locating a fugitive, or (iii) obtaining evidence of commission or attempted commission of a crime.


120. United States v. Choate, 576 F.2d 165 (9th Cir. 1978) (reh'g and reh'g en banc denied).

121. It is generally agreed that the Supreme Court would follow this reasoning. See, e.g., LAFAVE, supra note 16, § 2.7 at 66-67 (Supp. 1981).
scheme. After various other investigative tactics failed to produce substantial evidence, the Bureau of Customs placed a mail cover on Choate's correspondence. Identification of a South American return address was listed as the purpose of the cover; nevertheless, information gathered through the use of the mail cover pertained only to Choate's domestic affairs.\footnote{122}

The district court suppressed the evidence obtained through the mail cover\footnote{128} and determined that Choate's expectation of privacy in the mails was violated. Any voluntary disclosure of the information on his mail was for the postal employees' limited purpose in sorting and routing the mail. The district court stated that the only interest of the Postal Service in performing this surveillance was to aid the government in "snooping." The government's only basis for the warrantless intrusion was a "feeling in the acknowledged absence of probable cause that a crime was being committed."\footnote{134} Recognizing that the Postal Service was a government sanctioned monopoly, the district court emphasized the individual's lack of alternatives to process the mail. Furthermore, the court found that in a free society, if government were given such a monopoly and then allowed to utilize it, at its own discretion, to invade the privacy of its citizens, such action would be tantamount to a licensing of "blatant circumvention of constitutional rights."\footnote{125}

The court of appeals,\footnote{126} reversing the district court, likened the mailing of a letter to the risk a depositor takes under \textit{Miller}, and concluded that there was no unreasonable invasion of Choate's privacy. Choate had voluntarily conveyed this information to the postal employees and waived any constitutional right to keep the information private. The court of appeals also referred to the \textit{Hoffa-Lopez} line of cases and held that even if the district court assumed the information was for a limited purpose, the fourth amendment would not prevent

\begin{footnotes}
\item 122. Justice Hufstedler, dissenting, reasoned that because the mail cover information was procured by fraudulent misrepresentations on the application, there was an even greater constitutional violation. 576 F.2d at 193 (Hufstedler, J., dissenting).
\item 124. \textit{Id.} at 270.
\item 125. \textit{Id.} at 271.
\item 126. 576 F.2d 165 (9th Cir. 1978).
\end{footnotes}
its seizure when it was given a third party.\textsuperscript{127}

The need for privacy protection in this area is paramount. Although the mail cover is regulated by the Postal Service, the procedure is neither authorized nor controlled by an act of Congress.\textsuperscript{128} It is implemented at the sole discretion of the Postal Service. No judicial officer is involved at any stage. Any law enforcement agency may obtain a mail cover by submitting a written request to the Postal Service's investigative division. A showing of reasonable grounds that such a mail cover is necessary to gain information regarding the commission or attempted commission of a crime is all that is required.\textsuperscript{129} There is no notification requirement even after the investigation is complete. It is possible that an individual may never learn that a mail cover was used against him.\textsuperscript{130}

Far-reaching implications of this procedure become evident when it is possible to learn the identities, addresses, and frequency of contact of most of an individual's correspondents through a one-month mail cover operation. Considering that in its most basic use the mail cover is a method to defeat the probable cause requirement of the warrant clause, it appears to be an egregious affront to the concept of constitutionally protected privacy.\textsuperscript{131} Any attempt to rationalize the use of the mail cover with an individual's expectation of privacy falls in-

\textsuperscript{127} Id. at 175.

\textsuperscript{128} In \textit{Choate}, counsel for the Postal Service admitted that there was no statutory authority for the practice. Id. at 189, n.80 (Hufstedler, J., dissenting).

\textsuperscript{129} Law enforcement agencies include any federal, state or local unit which has as one of its "functions . . . [the investigation] of commission or attempted commission of acts constituting a crime." 39 C.F.R. § 233.2(c)(4) (1981). O. Garrison, \textit{Spy Government} (1967) lists the following agencies as being among those which typically apply for mail cover placement: The Bureau of Immigration and Naturalization; The Dept. of Justice; The U.S. Dist. Atty; The Army, Navy, and Air Force Intelligence; The National Security Agency; NASA; The FBI; The SEC; The Treasury Dept.; as well as state and local sheriffs and police departments. This list is not all inclusive. Id. at n.112. The mail cover practice was investigated by the Senate Subcommittee on Administrative Practice in 1965; see Note, \textit{Invasion of Privacy: Use and Abuse of Mail Covers}, 4 Colum. J.L. & Soc. Probs. 165 (1968).

\textsuperscript{130} In fact, in \textit{Choate} the use of the mail cover was inadvertently discovered in a pre-trial motion to suppress a hearing. 576 F.2d at 187 (Hufstedler, J., dissenting). The dissent went on to emphasize that \textit{Miller} should be inapplicable because the depositor willingly gives his records to the bank, while in the mail cover operation, the individual is unaware that this information file is being created. Id. Justice Hufstedler also pointed out the consistent fallacy in risk analysis when she stated that "that addressee of mail cannot by choice opt out of the system." Id. at n.70.

\textsuperscript{131} \textit{Contra} United States v. Isaacs, 347 F. Supp. 743 (N.D. Ill. 1972)(holding that there is no reasoning in \textit{Katz} to hold a mail cover operation unconstitutional).
adequately short of reality. Even if a person realizes that the postal employee must read the mail in order to process it, to say that this lessens an expectation that the mail is private reduces the concept of privacy protection to meaninglessness. What is reasonable is the assumption that the information, once used for its intended limited purpose, will be forgotten and not stored or recorded for future use.

Applying risk analysis in this area illustrates the doctrine's inherent irrational nature. If an individual is unaware that a correspondent is mailing him a letter, there can be no voluntary consent to assume the risk that the identity of the sender will be made known to any and all interested persons. Until he receives the mail, he cannot know the quality of the information he is voluntarily conveying. It follows that where there is a single governmental agency controlling the mails, any individual, innocent or guilty, must assume that any and all use of this mail service exposes him to arbitrary scrutiny, even before he is aware of his use of the service. His only choice would be to have absolutely no mailing address. This lack of alternatives and the lack of pre-investigation notice is crucial in understanding the shrinking scope of fourth amendment protection.

The legal justification for using mail covers may also have significant effects on the current expansion and development of electronic mail systems. Correspondence may be transmitted electronically in a variety of ways. Private manufacturers of facsimile printers have set up long range networks to allow firms to transmit their intra-company correspondence directly over telephone data transmission lines. In February of 1982, the Postal Service began operation of Electronic Computer Originated Mail (ECOM) which allows large volume mailers to electronically transmit a letter to the post office. The transmission is then turned into a printed letter, put into envelopes, and then delivered to the recipients. The long range plan of the Postal Service is to provide this service

---

133. "To send a handwritten letter electronically, it is fed into a facsimile machine, transmitted, and received by another facsimile machine which produces a copy. Most of today's facsimile machines transmit . . . over telephone lines." Id. at 264.
for everyone as a means of sending first class mail.\textsuperscript{135} Considering the ease of obtaining a mail cover at the present time, an individual who must "voluntarily" use this system is assuming an even greater risk: the voluntary exposure of the contents of the communication to the government.\textsuperscript{136}

By applying the warrant requirement to the use of mail covers, the necessary protection is obtained. If this is shown to be a serious detriment to the efficiency of police investigations, then the less stringent notification requirement should be mandatory to preserve the concept of a free society. Given the high degree of respect this nation places on the right of free speech and open disclosure, there is nothing more chilling than a surveillance activity that places individuals in fear of all their correspondents becoming known. Correspondence is speech—it is the free transference of ideas and information from one individual to another and it must be protected from arbitrary governmental scrutiny.

D. Beepers, Consent Searches, and More

In this final, but by no means all-inclusive section, a number of areas are briefly mentioned where individuals also lose control over their privacy by unknowingly assuming the risk of governmental intrusion. An in-depth analysis of these areas is beyond the scope of this comment. The purpose of presenting the examples is to emphasize the cumulative amount of surveillance permitted under the risk doctrine.

The risk doctrine has been applied to allow the use of electronic tracking devices known as "beepers"\textsuperscript{137} that monitor an individual's movements in public. Relying on the White decision, courts have analogized the beeper to a wired in-former and determined that an individual loses his fourth amendment protection from surveillance when he voluntarily ventures onto the public highways.\textsuperscript{138}


\textsuperscript{136} In a 1975 second circuit decision, the fourth amendment was held not to prohibit the photocopying of the envelopes. The potential conflict with the new electronic mail system is obvious. United States v. Leonard, 524 F.2d 1076 (2d Cir. 1975).

\textsuperscript{137} See generally Dowling, "Bumper Beepers" and the Fourth Amendment, 13 Crime L. Bull. 266 (1977); Comment, Beepers, Privacy and the Fourth Amendment, 86 Yale L.J. 1461 (1977).

\textsuperscript{138} 539 F.2d 32 (9th Cir. 1976).
Assumption of risk analysis is also used in the area of consent searches. When more than one individual has control over a particular place or item of property, the courts have determined that each individual has assumed the risk that the other will allow the police to gain access to the item or place in question.

Risk analysis also appears in decisions regarding administrative searches, jail searches of visitors, and airport searches. The assumption of risk doctrine becomes a volatile weapon that is easily applied in any circumstance where one individual comes into contact with any other person or government agency.

IV. Conclusion

Upon illustrating the cumulative effect of the Court's widespread application of assumption of risk analysis, it becomes apparent that government surveillance must be curtailed. When an individual who values his privacy is threatened in the performance of his daily activities, the power of government has extended too far. The additional realization that in many areas of an individual's life there are no alternatives for avoiding the assumption of surveillance risks, evidences the destructive force of risk analysis. To avoid assuming risks, an individual must withdraw almost completely from participation in society and forego the use of the mails, the telephone, the automobile, and conversation itself. Life must be as transaction free as possible. The result is clearly an Orwellian form of society. This withdrawal not only violates the functional purpose of the fourth amendment but also prevents the preservation of the free and open society to

139. See generally LaFave, Search and Seizure, A Treatise On The Fourth Amendment, § 8.3, 700-01.
141. See, e.g., Almeida Sanchez v. United States, 413 U.S. 266 (1973) (businessman is regulated industry consents, in effect, to restrictions placed on him by the government).
143. United States v. Doran, 428 F.2d 929 (9th Cir. 1973) (passenger assumes the risk that his belongings will be searched).
144. Professor Amsterdam suggests that an individual would have to hide in a dark cellar to escape surveillance. See Amsterdam, supra note 20, at 402-03.
which Americans are committed. Given the rapid technological advances that occur almost daily, and the Court's failure to recognize the potential for abuse in this area, it is imperative that restrictions be placed on governmental access to a person's private life.

Absent full application of the fourth amendment's antecedent justification with magistrate approval, and the specificity protection of the warrant clause, a minimal statutory standard of notification would afford the opportunity to protect one's privacy. The standards set forth in the Financial Privacy Act of 1978 could be adopted to control the use of pen registers, mail covers, and non-content data monitoring.\textsuperscript{146} Admittedly, the notification requirement would render ineffective the government's use of wired informers or secret agents who monitor private conversations, and also negate the usefulness of warrantless beeper installations. As these forms of surveillance intrude into very intimate aspects of an individual's private life, they should be controlled by the more stringent warrant requirements of the fourth amendment and the statutory regulation of Title III.

A dichotomy in constitutional interpretation exists if Katz protects the individual in a public telephone booth from having his words broadcast to the world and yet the same protection is not afforded the individual who has a direct conversation with another in the privacy of his own home. Unless some control is implemented, the number of risks that an individual unknowingly assumes begins to multiply exponentially each day. By necessity, one must reach out and expose his activities to the public. Professor Wayne LaFave, a noted fourth amendment expert, points out that it is precisely because all individuals must frequently reach out beyond their own private sphere to participate in life itself that the Court's reasoning in assumption of risk cases "does great violence to the rationale of the fourth amendment protection that had emerged in Katz."\textsuperscript{146}

We are left with the infamous "assumption of risk" doctrine, more aptly termed: "a hybrid of factual and fictitious elements and of individual and societal judgments."\textsuperscript{147} How-

\begin{itemize}
\item \textsuperscript{145} See supra notes 81-84.
\item \textsuperscript{146} Choper, Kamisar and Tribe, supra note 92, at 140.
\item \textsuperscript{147} Holmes v. Burr, 486 F.2d 55, 71 (9th Cir. 1973)(Hufstedler, J., dissenting).
\end{itemize}
ever, *Katz* also remains a viable alternative. Although the risk analysis decisions have negated its effectiveness in some areas, its power is still evident in the majority holding: "Wherever a man may be, he is entitled to know that he will be free from unreasonable searches and seizures." The erosion of the scope of fourth amendment protections must be halted, either through a more realistic interpretation of *Katz*, or through a statutory notification requirement. It is imperative that unrestrained government surveillance be recognized as an intrusion into the privacy of all individuals, whether innocent or guilty. Without such an awareness, wherever a person may be, he will not be free.

JoAnn Guzik

148. 389 U.S. at 359.

149. Justice Hufstedler, in an excellent dissent in Holmes v. Burr, 486 F.2d 55, clearly states the problem of eroding the scope of the fourth amendment:

A constitutional right continuously diluted becomes no right. Destroying a right protected by the Fourth Amendment because of distaste for the remedy makes little more sense than destroying a patient for failure to respond to chosen medication. If the remedy is wrong, it is time to reexamine the remedy, not to diminish the right.

*Id.* at 74 (Hufstedler, J., dissenting).