



10-1-1973

Electronic Eavesdropping: A Victim's Primer

Notre Dame Law Review Editors

Follow this and additional works at: <http://scholarship.law.nd.edu/ndlr>



Part of the [Law Commons](#)

Recommended Citation

Notre Dame Law Review Editors, *Electronic Eavesdropping: A Victim's Primer*, 49 Notre Dame L. Rev. 162 (1973).

Available at: <http://scholarship.law.nd.edu/ndlr/vol49/iss1/9>

This Note is brought to you for free and open access by NDLScholarship. It has been accepted for inclusion in Notre Dame Law Review by an authorized administrator of NDLScholarship. For more information, please contact lawdr@nd.edu.

ELECTRONIC EAVESDROPPING: A VICTIM'S PRIMER

I. Introduction

On June 17, 1972, five men were arrested in the offices of the Democratic National Committee in the Washington, D.C., Watergate complex.¹ The men were caught by police while in the process of replacing previously installed electronic listening devices and photographing Democratic Party files. Less than a full year later, the Watergate Affair emerged as perhaps the most shocking and damaging² political scandal in United States history, reaching from the lowest and most clandestine ranks of the President's Reelection Campaign Committee to President Nixon's closest advisors, many of whom were forced to resign.

As the facts of the Watergate scandal became known, it became clear that the Democratic National Committee was not the only victim of electronic eavesdropping. At about the same time as the Watergate scandal became public knowledge, a federal district court judge dismissed all charges against Dr. Daniel Ellsberg and Anthony Russo, who had been accused and brought to trial for allegedly stealing and copying the famous "Pentagon Papers." The judge took the action when it was discovered that certain of Ellsberg's telephone conversations had been wiretapped by the FBI.³ The logs of these conversations, which the FBI had told the judge had "disappeared," were eventually discovered in the White House safe of presidential advisor John Erlichmann.⁴

As more and more of the Watergate story unfolded, evidence of widespread wiretapping the bugging became commonplace. On May 16, 1973, the Justice Department announced that Dr. Henry Kissinger, the President's closest foreign affairs advisor, had requested that the FBI wiretap the telephones of several officials of the National Security Council.⁵ At the same time, William D. Ruckelshaus, Acting Director of the FBI, disclosed that wiretaps had been placed on the phones of a total of thirteen government officials and four newsmen during the period 1969 through 1971.⁶ It was learned that presidential advisor John Erlichmann secretly taped his own telephone conversations with the then At-

1 For an extensive, day-by-day analysis of both the details of the Watergate scandal and how they were exposed, see James McCartney's article, *How the Dam Burst*, COLUMBIA JOURNALISM REVIEW, July-August 1973, at 8-22. The same issue has a perceptive analysis/survey of press and television coverage of the Watergate affair prior to the Nixon-McGovern election. E. Diamond, *TV and Watergate: What Was, What Might Have Been*, COLUMBIA JOURNALISM REVIEW, July-August 1973, at 20. Diamond points out that while many newspapers spent an inordinate amount of time congratulating themselves for their part in exposing the scandal, only one newspaper, the Washington Post, devoted any significant space to the story. *Id.* Of some 500 political columns written between June and November, 1972, less than two dozen had dealt with Watergate. Of the 433 Washington-based reporters who could, in theory, have been assigned initially to the Watergate story, only fifteen actually were. *Id.* See also Lewis H. Lapham's perceptive article on the temptation to view the "Watergate press" as a sacred cow in HARPER'S, August 1973 at 43.

2 A Gallup Poll taken during the last week of June, 1973, showed that only 29% of the American people believed President Nixon's statement that he had nothing to do with the Watergate Affair. N.Y. Times, July 8, 1973, at 23, col. 5.

3 *Id.*, May 12, 1973, at 1, col. 8.

4 *Id.*, May 15, 1973, at 1, col. 8.

5 *Id.*, May 17, 1973, at 1, col. 5.

6 *Id.*, May 15, 1973, at 1, col. 8.

torney General of the United States, Richard Kleindienst.⁷ Former White House Counsel John Dean went so far as to suggest before the Senate subcommittee investigating the eavesdropping and spying scandal that the President himself had deliberately asked leading questions of Dean in order to surreptitiously record any incriminating answers Dean might give.⁸ On July 6, 1973, it was reported that Nixon campaign aides had wiretapped the telephone of Mary Jo Kopechne's apartment shortly after she died in an auto accident involving a possible Democratic contender, Senator Edward Kennedy.⁹

The Watergate bugging scandal served to remind many Americans of the incredibly pervasive quality of electronic eavesdropping in an era of science and technology. Microminiaturization has made possible the development of high-quality microphones of match head size. These tiny mikes have been discovered in telephones, doorbell units, clocks, picture frames, cellophane tape dispensers and hundreds of other common household items.¹⁰ Research has developed laser beams that under laboratory conditions can pick up conversations in a room from the outside windowpane.¹¹ A special microphone and transmitter have been built into a light bulb so as to transmit when the light switch is on and stop when the switch is turned off.¹²

Electronic eavesdropping dates back some one hundred years. Almost as soon as the telegraph came into existence, wiretappers were busy intercepting the coded communications.¹³ By 1862, the California Legislature had enacted legislation prohibiting the interception of telegraph messages.¹⁴ During the Civil War, Union and Confederate forces frequently tapped each other's telegraph lines.¹⁵ Less than twenty years after Alexander Graham Bell first exhibited his telephone, the police of New York City were tapping the phones of suspected criminals.¹⁶ In the mid-1930's, an FCC raiding squad uncovered a wiretap apparatus connected to the telephone lines of the Justices of the United States

7 *Id.*, June 30, 1973, at 22, col. 3.

8 NEWSWEEK, July 9, 1973, at 19. Dean may have been right. On July 16, 1973, Alexander Butterfield, a former White House aide, informed the Senate Watergate Committee that President Nixon had listening devices in the White House that automatically tape-recorded both room and telephone conversations. N.Y. Times, July 17, 1973, at 1, col. 8. When the Senate Watergate Committee expressed interest in listening to certain of the tapes, the President immediately ordered the Secret Service to withhold all information about the secretly made recordings. *Id.*, July 18, 1973, at 1, col. 8. When the President refused, on July 23, to release the tape recordings of his conversations about the Watergate scandal with his ex-White House counsel, John Dean, both Archibald Cox, the special prosecutor appointed to investigate Watergate, and the Senate Watergate Committee moved at once to subpoena the tapes. *Id.*, July 24, 1973, at 1, col. 8. Thus was precipitated a "constitutional collision" between the executive and legislative branches. Early efforts to avoid a damaging crisis are reported in the New York Times, July 28, 1973, at 1, col. 6.

9 N.Y. Times, July 6, 1973, at 1, col. 5.

10 A. WESTIN, *PRIVACY AND FREEDOM*, 74 (1967).

11 AMERICAN BAR ASSOCIATION PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE: STANDARDS RELATING TO ELECTRONIC SURVEILLANCE 45 (1971) [hereinafter ABA STANDARDS].

12 A. WESTIN, *supra* note 10, at 74.

13 S. DASH, R. KNOWLTON, AND R. SCHWARTZ, *THE EAVESDROPPERS* 23 (1959) [hereinafter DASH]. For a helpful survey of the history of wiretapping and the law, see the following: A. GASQUE, *WIRETAPPING* (1962) (a history of federal legislation and Supreme Court decisions); F. GREENMAN, *WIRE-TAPPING, ITS RELATION TO CIVIL LIBERTIES* (1938); J. MAGUIRE, *EVIDENCE OF GUILT* (1959); D. TOMPKINS, *WIRETAPPING: A SELECTED BIBLIOGRAPHY* (1955).

14 Statutes of California, 1862, p. 288, CCLXII.

15 *Berger v. New York*, 388 U.S. 41, 46 (1967).

16 N.Y. Times, May 18, 1973, at 1, col. 1.

Supreme Court.¹⁷ In 1967, Internal Revenue Service Commissioner Sheldon Cohen admitted that agents of the IRS had knowingly broken the law in investigating the crimes of others,¹⁸ and even admitted that the IRS had organized a school for eavesdropping.¹⁹ Conference rooms provided by the IRS for attorney-client meetings were bugged,²⁰ and the FBI placed listening devices in the offices of lawyers whose clients were being investigated.²¹

Wiretapping for political purposes began long before Watergate. Telegraph tapping to intercept messages was frequently exposed in newspaper stories of the 1870's.²² The telephones of the Stevenson-For-President campaign headquarters at the 1960 Democratic National Convention were discovered to have been wiretapped.²³ A leader of the right-wing political group, the Minutemen, once told of his organization's expertise in electronically eavesdropping on the meetings of "subversive groups" in the United States.²⁴

While the Watergate and Ellsberg wiretaps and bugs made the front pages of newspapers throughout the world,²⁵ most electronic surveillance, because it is intended to be secret and is usually illegal, is carried on with only the eavesdropper's knowledge. A recent study determined that some 6,500 residents of New York City were wiretapped without their knowledge in 1972.²⁶ All of these taps were authorized by court order. Samuel Dash,²⁷ author of an extensive study of electronic eavesdropping,²⁸ once suggested that the ratio of illegal taps to legal ones may go as high as nine to one.²⁹ It is thus possible that in 1972 over 40,000 New Yorkers were wiretapped.

The arguments against such electronic surveillance extend from issues of search and seizure to the inhibiting of first amendment rights,³⁰ and particularly to notions of the right to privacy.³¹ Supreme Court Justice Brandeis expressed grave concern over such surreptitious electronic surveillance in his famous dissent in the *Olmstead* case:³²

17 DASH, *supra* note 13, at 29.

18 N.Y. Times, July 13, 1967, at 26, col. 1.

19 *Hearings on Invasions of Privacy Before Subcomm. on Administrative Practices and Procedures of Senate Comm. on the Judiciary*, 89th Cong., 1st Sess., at 1212 (1965).

20 *Hearings on Invasions of Privacy Before Subcomm. on Administrative Practices and Procedures of Senate Comm. on the Judiciary*, 90th Cong., 1st Sess., pt. 2, at 122 (1967).

21 N.Y. Times, Dec. 11, 1966, at 148, col. 3.

22 CONG. REC., H.R., 43rd Cong., 1st Sess., 2378 (1874).

23 N.Y. Times, July 12, 1960, at 7, col. 1.

24 A. WESTIN, *supra* note 10, at 115.

25 America is not the only country with eavesdropping problems. The New York Times reported recently on the "bugging" situation in Great Britain. N.Y. Times, July 8, 1973, at 39, col. 1.

Evidence of a new kind of "hands across the sea" approach to wiretapping was disclosed when the West German government reported that it had tapped civilian telephone conversations in West Germany at the request of United States intelligence agencies. A German official who told the press of the results of the tapping said that West German agents did the actual listening work and then passed on their transcripts to the American agents. *Id.*, August 3, 1973, at 7, col. 1.

26 NEW YORK MAGAZINE, July 9, 1973, at 28.

27 Mr. Dash presently serves as Majority Counsel to the Senate subcommittee investigating the Watergate affair.

28 *See* note 13, *supra*.

29 NEW YORK MAGAZINE, July 9, 1973, at 28.

30 ABA STANDARDS, *supra* note 11, at 87.

31 *See* Comment, 17 U.C.L.A. L. REV. 1205 (1970).

32 *Olmstead v. United States*, 277 U.S. 438 (1928).

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security?³³

Twice, the United States Congress has enacted legislation against electronic eavesdropping: against wiretapping in 1934³⁴ and against any form of warrantless electronic eavesdropping ("bugging") in 1968.³⁵ And yet it is clear from the Watergate scandal and other reports that illegal wiretapping and bugging constitute lucrative careers for those willing to risk exposure—that such spying goes on throughout the country, violating the rights of perhaps thousands of Americans. With the number of persons victimized by wiretapping and bugging seemingly increasing, it can be expected that more of these victims will turn to the law for relief. The purpose of this note is to survey the major case law on the subject of electronic surveillance, and to review the current statutory prohibitions against illicit electronic eavesdropping—in short, to provide a primer for the victims of illegal wiretapping and bugging in the United States.

II. Case Law Prior to 1968

The Supreme Court first dealt with the question of electronic eavesdropping in *Olmstead v. United States*.³⁶ Olmstead and several other codefendants had been convicted of conspiring to violate the national prohibition act. The conspiracy had been discovered and exposed through evidence obtained by the interception of the telephone conversations of Olmstead and his fellow conspirators. Government law enforcement officers had intercepted the messages by placing inconspicuous wires on telephone lines leading into the houses of several of the defendants. The Court rejected Olmstead's claim that his fourth amendment rights had been violated, finding that no liberality of construction could cause a conversation passing over a telephone wire to become a "house," or "person," or "paper," or "effect" under the language of the fourth amendment.³⁷ Because the placing of the tap wires had been accomplished without any actual physical trespass to the conspirators' property, the Court held that the wire-tapping was not a search within the meaning of the fourth amendment:

The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only.³⁸

³³ *Id.* at 474.

³⁴ Federal Communications Act of 1934 § 605, ch. 652, § 605, 48 Stat. 1103 (1934), as amended, 47 U.S.C. § 605 (1970).

³⁵ The Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. § 2510-2520 (1970).

³⁶ 277 U.S. 438 (1928).

³⁷ *Id.* at 465.

³⁸ *Id.* at 464.

For the fourth amendment to apply, said the Court, it must be shown that there has been an "official search and seizure of his person, or such a seizure of his papers or his tangible/material effects, or an actual, physical invasion of his house . . . for the purpose of making a seizure."³⁹ The Court refused to find a "search" where there had been no invasion of property rights, and said that there could be no such thing as a "seizure" of conversation.⁴⁰

In 1934, some six years after the *Olmstead* decision, Congress passed the Federal Communications Act. Section 605 of the Act provided that:

. . . no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or the benefit of another not being entitled thereto; and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto . . .⁴¹

In addition, § 501 of the Act imposed a fine or imprisonment or both for willful and knowing violations of its provisions.⁴²

The first case to construe § 605 was *Nordone v. United States*,⁴³ where the Court found the "plain mandate" of the statute to be the prohibition of wiretapping. The Government had argued that § 605 was not intended by Congress to apply to federal law enforcement officers, but the Court held that the statute prohibited the introduction in federal court of evidence directly obtained through wiretapping conducted by *any* person, federal agent or otherwise.⁴⁴ The Court also held that any admission of evidence obtained through wiretapping would constitute the "divulgence" prohibited by the statute.⁴⁵ In *Weiss v. United States*,⁴⁶ the Court held that § 605 applied to intrastate communications, as well as interstate.⁴⁷ The evidence obtained through the wiretapping in that case was held inadmissible.

In *Goldman v. United States*⁴⁸ the Court again applied the "no trespass, no search" principle of *Olmstead* in a case where federal agents had overheard the defendant's telephone conversations by the use of a listening device placed against

39 *Id.* at 466.

40 *Id.* at 465.

41 47 U.S.C. § 605 (1970).

42 47 U.S.C. § 501 (1970).

43 302 U.S. 379 (1937).

44 *Id.* at 381.

45 *Id.* at 382.

46 308 U.S. 321 (1939).

47 *Id.* at 328.

48 316 U.S. 129 (1942).

the wall of the defendant's office. The Court also found that there had been no "interception" within the meaning of § 605.⁴⁹

In *On Lee v. United States*,⁵⁰ a case similar to *Goldman*, the Court rejected the defendant's argument that the use of an informer "wired for sound" who engaged the defendant in incriminating conversations monitored by a government narcotics agent violated both the fourth amendment and § 605. The Court ruled that the defendant had consented to the informer's entry into his place of business, and thus there was no trespass.⁵¹

In a 1957 case, *Rathburn v. United States*,⁵² the Court held that listening to a conversation by use of an extension telephone with the consent of one of the parties was not prohibited by § 605. The Court stated that:

Each party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation. When such takes place there has been no violation of any privacy of which the parties may complain. Consequently, one element of Section 605, *interception*, has not occurred.⁵³

Although the Court had allowed evidence obtained through the wire-tapping activities of state law officers to be admitted in a state court in *Schwartz v. Texas*,⁵⁴ the Court later held in *Benanti v. United States*⁵⁵ that wiretapping by such state officials violated § 605. In *Lee v. Florida*,⁵⁶ decided in 1968, the Court overruled *Schwartz*, holding not only that the "bugging" by state law officers of a defendant's telephone violated § 605 but also that the evidence obtained thereby was wholly inadmissible, even in a state court. Noting that *Mapp v. Ohio*⁵⁷ had applied the strict test of the fourth amendment to the admissibility of evidence in state courts, the Court said that *Mapp* had:

. . . imposed a judicially devised exclusionary rule in order to insure that a state could not adopt rules of evidence calculated to permit the invasion of rights protected by federal . . . law. In the present case the federal law itself explicitly protects intercepted communications from divulgence, in a court or any other place.⁵⁸

In *Silverman v. United States*,⁵⁹ a case decided prior to *Lee*, the Court had already begun to move away from the rigidity of the *Olmstead* and *Goldman* decisions. *Silverman* involved a "bug" rather than a wiretap. Government agents had driven a spike with a microphone attached through a wall and had made contact with a heating duct in the defendant's home, thus allowing the agents to overhear conversations in the house.⁶⁰ The Court found that the

49 *Id.* at 134.

50 343 U.S. 747 (1952).

51 *Id.* at 752.

52 355 U.S. 107 (1957).

53 *Id.* at 111.

54 344 U.S. 199 (1952).

55 355 U.S. 96 (1957).

56 392 U.S. 378 (1968).

57 367 U.S. 643 (1961).

58 392 U.S. at 385.

59 365 U.S. 505 (1961).

60 *Id.* at 506-07.

bugging had involved an "unauthorized physical penetration into the [defendant's] premises."⁶¹ Such a penetration was, in the eyes of the Court, an actual intrusion into a constitutionally protected area⁶² which required reversal of the defendant's conviction. This decision, and another one involving a similar device attached by means of a thumbtack and not a spike,⁶³ recognized that despite *Olmstead* conversations could be seized within the meaning of the fourth amendment, and employed the notion of a constitutionally protected area rather than the traditional *Olmstead-Goldman* notion of a trespass in the real property sense. In 1963, the Court finally held in *Wong Sun v. United States*⁶⁴ that the fourth amendment could "protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'"⁶⁵

In 1967, the Supreme Court invalidated a New York statute prohibiting electronic eavesdropping in *Berger v. New York*.⁶⁶ Government agents had sought and received the issuance of an order permitting the installation of a recording device in the office of an attorney. The order was granted by a New York judge pursuant to § 813(a) of the New York Code of Criminal Procedure. The subsequent electronic surveillance provided evidence used to convict the petitioner of conspiring with others to bribe a public official. The Supreme Court reversed the conviction and found that the New York eavesdropping statute was too broad, lacked the necessary fourth amendment element of particularization,⁶⁷ and authorized the indiscriminate use of electronic devices.⁶⁸ The statute, said the Court, permitted "general searches by electronic devices, the truly offensive character of which was first condemned in *Entick v. Carrington*, 19 How.St.Tr. 1029, and which were then known as 'general warrants.'"⁶⁹ The Court held that the statute's "blanket grant of permission to eavesdrop [was] without adequate judicial supervision in protective procedures," and thus violated the fourth and fourteenth amendments.⁷⁰

Section 813(a) of the New York statute authorized the issuance of an ex parte order for eavesdropping upon the oath or affirmation of a district attorney, an attorney general or a police officer of sergeant's rank or above that there is reasonable ground to believe that evidence of crime could be obtained through the eavesdropping.⁷¹ The oath required that the subjects of the electronic surveillance must be "particularly" described.⁷² The judge from whom the order was requested was allowed, under the statute, to "examine on oath the applicant and any other witness he may produce and shall satisfy himself of the existence of reasonable grounds"⁷³ for the granting of the eavesdrop order. The duration

61 *Id.* at 509.

62 *Id.*

63 *Clinton v. Virginia*, 204 Va. 275, 130 S.E.2d 437 (1963), *rev'd*, 377 U.S. 158 (1964).

64 371 U.S. 471 (1963).

65 *Id.* at 485.

66 388 U.S. 41 (1967).

67 *Id.* at 55.

68 *Id.* at 58.

69 *Id.*

70 *Id.* at 60.

71 *Id.* at 54.

72 *Id.*

73 *Id.*

of the period of surveillance was to be specified in the order, and was generally not to exceed two months, although it could be extended.⁷⁴

The Court held that the New York statute satisfied the fourth amendment requirement that a neutral and detached authority be interposed between the police and the public.⁷⁵ In several other respects, however, the statute was found to be severely wanting. The Court noted that the statute laid down no "requirement for particularity" in the warrant as to what "specific crime has been or is being committed." Nor were the place to be searched or the persons or things to be seized necessarily to be described in particular, as specifically required by the fourth amendment.⁷⁶ The statute's authorization of eavesdropping for up to two months' time, with the further possibility of extension, amounted, said the Court, to "a series of intrusions, searches and seizures pursuant to a single showing of probable cause."⁷⁷ The Court also noted that the statute placed "no termination date on the eavesdrop once the conversation sought" was seized. Nor did the statute provide for the notice found in conventional warrants, but instead permitted "unconsented entry without any showing of [the] exigent circumstances" usually required.⁷⁸

In condemning the overbroad aspects of the New York statute,⁷⁹ the Court in *Berger* depended, to a great extent, on the guidelines it had developed in *Osborn v. United States*,⁸⁰ an eavesdropping case it had decided less than a year before. In *Osborn*, the Court was asked to exclude the evidence of conversations recorded pursuant to a court order. The Court refused to do so and found that the recording, although an invasion of privacy protected by the fourth amendment, was admissible because the judge's order of authorization was based upon a "detailed factual affidavit alleging the commission of a specific criminal offense directly and immediately affecting the administration of justice . . . for the narrow and particularized purpose of ascertaining the truth of the affidavit's allegations."⁸¹ The *Berger* Court implied that the *Osborn* procedure should be followed by law-enforcement officials and authorizing judges in all eavesdropping cases.

The Supreme Court emphasized its adherence to the *Osborn-Berger* standards in *Katz v. United States*,⁸² a case decided a few months after *Berger*, which finally overruled both *Olmstead* and *Goldman*.⁸³ In *Katz* the defendant's conversations on a public telephone had been overheard through the use of a wiretap placed by FBI agents. No warrant had been obtained for the wiretap. The Court reversed *Katz's* conviction, holding that the wiretap evidence had been obtained through an illegal search and seizure. The Court discarded the *Silver-*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *Id.* at 58-59.

⁷⁷ *Id.*

⁷⁸ *Id.* at 60.

⁷⁹ See Comment, 20 SYRACUSE L. REV. 601 (1968), dealing with New York's legislative attempts to overcome the defects of the eavesdropping statute invalidated in *Berger*.

⁸⁰ 385 U.S. 323 (1966).

⁸¹ *Berger v. New York*, 388 U.S. 41, 57 (1967).

⁸² 389 U.S. 347 (1967).

⁸³ "We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." 389 U.S. at 353.

man notion of a "constitutionally protected area" and held that a person was entitled to the protection of the fourth amendment whenever he had a justifiable expectation of privacy:

What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection But what he seeks to preserve as private, even in an area accessible to the public, may be Constitutionally protected.⁸⁴

Noting that the fourth amendment protects people and not places,⁸⁵ the Court completely overruled the *Olmstead* notion of physical trespass:

[W]e have since [*Olmstead*] departed from the narrow view on which (*Olmstead*) rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any "technical trespass under . . . local property law . . ." Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply "areas"—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.⁸⁶

The Court observed that the eavesdropping in *Katz* could easily have met the standards set by *Osborn* and *Berger*:

[T]his surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed . . . could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts . . . took place.⁸⁷

As a result of the *Katz*⁸⁸ and *Berger* decisions, the protection of § 605 of the Communications Act against wiretapping was extended to a fourth amendment prohibition against *all* forms of warrantless electronic surveillance. The *Katz-Berger* warrant standards were the same required for any other search under the fourth amendment: law enforcement officials were to be required, before commencing a search, to present their estimate of probable cause for the detached scrutiny of a neutral magistrate. They were additionally to be compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Finally, they were to be directed, after the search was completed, to notify the authorizing magistrate in detail of all that had been seized.⁸⁹

84 389 U.S. 351-52.

85 *Id.*

86 *Id.* at 353.

87 *Id.* at 354.

88 The *Katz* holding did not apply retroactively to eavesdropping conducted prior to that decision. *Desist v. United States*, 394 U.S. 244 (1969); *Kaiser v. New York*, 394 U.S. 280 (1969).

89 *Katz v. United States*, 389 U.S. 347, 356 (1967).

III. The Omnibus Crime Control and Safe Streets Act of 1968

While law enforcement officials initially denounced the *Berger* and *Katz* decisions as insurmountable roadblocks to effective crime control, these two cases served as both the impetus and basis for the first statutory allowance of wiretapping and bugging on the federal level. As noted, § 605 of the Communications Act had been held to constitute a complete prohibition, without exception, to the interception, divulging or publishing of the content of wiretaps. *Katz* and *Berger* prohibited *warrantless* bugging, but in so doing opened the way for both wiretapping and bugging under warrant. For some thirty years, Congress considered a variety of legislative proposals relaxing the complete prohibition of wiretapping.⁹⁰ By 1968 the widespread concern for "law and order" and the recognition that the electronic eavesdropping laws of the fifty states had been left in disarray by the *Katz* and *Berger* holdings,⁹¹ led Congress to pass the eavesdropping provisions of the 1968 Omnibus Crime Control and Safe Streets Act. The electronic eavesdropping section of the anticrime legislation was basically a combination of two earlier proposals by Senators Hruska and McClellan designed to legalize wiretapping activities by police throughout the country.⁹² The eavesdropping provisions were adopted along with a wide array of other law enforcement aids, from federal aid to local police forces to antigun legislation.⁹³

90 The legislation proposed to allow wiretapping by the Government and introduced prior to 1959 is listed in *Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 86th Cong., 1st Sess., pt. 4, at 781-1031 (1959).

91 At the time of the *Berger* decision, seven states — California, Illinois, Maryland, Massachusetts, Nevada, New York, and Oregon — prohibited surreptitious eavesdropping by mechanical or electronic device. CAL. PEN. CODE §§ 653h-j; ILL. REV. STAT., ch. 38, §§ 14-1 to 14-7 (1965); MD. ANN. CODE, Art. 27, § 125A (1957); MASS. GEN. LAWS, ch. 272, § 99 (Supp. 1966); NEV. REV. STAT. § 200.650 (1963); N.Y. PEN. LAW § 738 (Supp. 1966); ORE. REV. STAT. § 165.540 (1) (c) (Supp. 1965). However, all but Illinois permitted official court-ordered eavesdropping. Some 35 states prohibited wiretapping. ALA. CODE tit. 48, § 414 (1958); ALASKA STAT. § 42.20.100 (1962); ARK. STAT. ANN. § 73-1810 (1957); COLO. REV. STAT. ANN. § 40-4-17 (1963); CONN. GEN. STAT. REV. § 53-140 (1958); DEL. CODE ANN. tit. 11, § 757 (Supp. 1966); FLA. STAT. § 822.10 (1965); HAWAII REV. LAWS § 309 A-1 (Supp. 1963); IDAHO CODE ANN. §§ 18-6704, 6705 (1947); ILL. REV. STAT., ch. 134, § 16 (1965); IOWA CODE § 716.8 (1962); KY. REV. STAT. § 433.430 (1962); LA. REV. STAT. § 14:322 (1950); MD. ANN. CODE art. 35, §§ 92, 93 (1957); MASS. GEN. LAWS, ch. 272, § 99 (Supp. 1966); MICH. STAT. ANN. § 28.808 (1954); MONT. REV. CODES ANN. § 94-3203 (Supp. 1965); NEB. REV. STAT. § 86-328 (1966); NEV. REV. STAT. §§ 200.620, 200.630 (1963); N.J. REV. STAT. § 2A:146-1 (1953); N.M. STAT. ANN. § 40A-12-1 (1964); N.Y. PEN. LAWS § 738 (Supp. 1966); N.C. GEN. STAT. § 14-155 (1953); N.D. CENT. CODE § 8-10-07 (1959); OHIO REV. CODE ANN. § 4931.28 (1954); OKLA. STAT. tit. 21, § 1757 (1961); ORE. REV. STAT. § 165.540 (1) (Supp. 1965); PA. STAT. ANN. tit. 15, § 2443 (1958); R.I. GEN. LAWS ANN. § 11-35012 (1956); S.D. CODE § 13.4519 (1939); TENN. CODE ANN. § 65-2116 (1955); UTAH CODE ANN. § 76-48-11 (1953); VA. CODE ANN. § 18.1-156 (1960 Repl. Vol.); WIS. STAT. § 134.39 (1963); WYO. STAT. ANN. § 37-259 (1957). Of these 35, 27 permitted "authorized" interception of some type.

92 An extensive historical review of the events leading up to the passage of the Omnibus Crime Control and Safe Streets Act can be found in Harris, *Annals of Legislation—The Turning Point*, THE NEW YORKER, Dec. 14, 1968, at 68-179.

93 The bill, as amended, was divided into five titles: Title I, Law Enforcement Assistance; Title II, Admissibility of Confessions, Reviewability of Admission in Evidence of Confessions in State Cases, Admissibility in Evidence of Eyewitness Testimony, and Procedures in Obtaining Writs of Habeas Corpus; Title III, Wiretapping and Electronic Surveillance; Title IV, State Firearms Control Assistance; and Title V, General Provisions.

Title I, Law Enforcement Assistance, authorizes the establishment of a three-member Law Enforcement Assistance Administration within the Department of Justice under the general authority of the Attorney General to administer grant programs to states and units of

Title III of the Omnibus Act superseded § 605 of the Communications Act; and unlike that previous statutory prohibition made no distinction between wiretapping and other forms of electronic surveillance.⁹⁴ Generally, Title III prohibits all forms of electronic surveillance except by duly authorized law enforcement officers engaged in the investigation or prevention of specific crimes. Section 2511 prohibits the *interception* of wire or oral communications unless one party to the communication has consented to the interception. The section also prohibits the *disclosure* or use of such illegally intercepted communications. A willful violation of § 2511 is a criminal offense punishable by a fine of not more than \$10,000 and/or imprisonment not to exceed five years.⁹⁵

The manufacture, distribution, sale, possession, or advertising of devices whose design "renders them primarily useful for the purpose of surreptitious interception of wire or oral communication" is prohibited by § 2512; the penalty for violation is again a fine of up to \$5,000 and/or five years in prison.⁹⁶ Section 2513 authorizes the seizure and forfeiture to the United States of the eavesdropping devices prohibited by § 2512.⁹⁷

Under § 2514 a U.S. Attorney, with the approval of the Attorney General, is authorized to grant immunity to a witness to compel testimony in any case involving a violation of the Act or involving a violation of any offense for which federal warrants for electronic surveillance may be issued.⁹⁸

Section 2516 authorizes the Attorney General or an Assistant Attorney General to apply for a surveillance order to investigate any of the following federal offenses: murder, kidnapping, sabotage, espionage, treason, extortion, robbery, bribery, counterfeiting, fraudulent bankruptcy, the use or sale of dangerous drugs, the obstruction of justice, presidential assassination, labor racketeering, labor embezzlement, interstate transportation of stolen property, and conspiracy to commit any of the foregoing offenses. The principal prosecutor of a state or local government may, if authorized by a state statute, apply for a surveillance order to investigate murder, kidnapping, gambling, bribery, extortion, narcotics traffic or other crimes dangerous to life, limb, or property and punishable by imprison-

local government to strengthen and improve law enforcement.

Title II adds three new sections to chapter 223, title 18, United States Code, relating to the admissibility into evidence of voluntary confessions in criminal prosecutions in federal courts, the reviewability by federal courts of state court rulings admitting confessions found to be voluntary, and the admissibility into evidence of eyewitness testimony.

Title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officials engaged in the investigation of specified types of major crimes after obtaining a court order, with exceptions provided for interceptions by employees of communications facilities whose normal course of employment would make necessary such interception, and personnel of the Federal Communications Commission in the normal course of employment.

Title IV seeks to aid in making it possible to keep firearms out of the hands of those not legally entitled to possess them because of age, criminal background, or incompetency, and to assist law enforcement authorities in the states and their subdivisions in combating crime in the United States.

Title V contains a legislative separability clause.

94 The two *are* different. For a discussion of various types of devices and the distinctions between them, *see* NEW YORK MAGAZINE, July 9, 1973, at 28-33.

95 18 U.S.C. § 2511 (1970).

96 18 U.S.C. § 2512 (1970).

97 18 U.S.C. § 2513 (1970).

98 18 U.S.C. § 2514 (1970).

ment for more than one year. The offense must be specified in a state statute authorizing such surveillance.⁹⁹

Sections 2518 and 2510(9)(a) authorize judges of federal district courts and federal courts of appeal to issue surveillance orders. Judges of state courts of general criminal jurisdiction may, under § 2510(9)(b), issue surveillance orders if they are authorized to do so under state statute. Any judge who issues a surveillance order must, under § 2518(3), have probable cause to believe that (1) a particular offense has been, is being, or is about to be committed; and (2) particular communications relating to the offense will be overheard. The issuing judge must also find that the normal investigative procedures have been tried and failed, are unlikely to succeed if tried, or are simply too dangerous.¹⁰⁰

Section 2516(1) provides that a federal order may be executed only by the FBI or by the federal agency having responsibility for investigating the offense named in the order.¹⁰¹ A state order may, under § 2516(2), be executed only by investigative or law enforcement officers having the responsibility for investigating the offense named in the order.¹⁰² Evidence of crimes not named in a surveillance order may not be introduced in evidence unless judicial approval is received subsequent to the interception under provisions of § 2517(5).¹⁰³

Section 2518(5) provides that a surveillance order may be issued for a period no longer "than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days." Extensions of an eavesdropping order may be granted under § 2518(5) only upon a new showing of probable cause.¹⁰⁴

In certain emergency situations specially designated investigative or law-enforcement officers may intercept communications without a surveillance order. Under § 2518(7), however, an application for a judicial order approving the interception must be filed within 48 hours.¹⁰⁵

Section 2518(8)(a) requires that intercepted communications must, if possible, be recorded on tape or some other device. Such recordings are required to be protected from possible editing or alteration. The judge issuing the surveillance order shall have the tapes made available to him and shall seal them. Applications and orders must also be sealed by the judge.¹⁰⁶

Within 90 days after an application for a surveillance order has been denied or the termination of the period of an approved order and any extensions thereof, § 2518(8)(d) requires that persons named in an order or application, "and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice," shall be served with an inventory giving notice of the order or application and the period of surveillance, if any. Such notice may be postponed upon a showing of good cause before a judge.¹⁰⁷

Unlawfully intercepted communications are excluded under § 2515 from

99 18 U.S.C. § 2516 (1970).

100 18 U.S.C. §§ 2518, 2510(9) (1970).

101 See note 99, *supra*.

102 *Id.*

103 18 U.S.C. § 2517 (1970).

104 18 U.S.C. § 2518 (1970).

105 *Id.*

106 *Id.*

107 *Id.*

evidence in any federal or state court, grand jury, administrative or legislative proceeding.¹⁰⁸ Under § 2518(10) the parties to an intercepted communication or the person against whom the interception was directed may challenge the validity of a surveillance order, and the Government may appeal from an order granting motion to suppress such evidence.¹⁰⁹

Judges issuing electronic eavesdropping orders must file a report with the Administrative Office of the United States Courts within 30 days after the expiration of a surveillance order under § 2519(1).¹¹⁰ This report must identify the officer or agency applying for the order, the offense named in the order, the length of the surveillance period, and the type of facilities involved in the interception. Under the same section prosecutors must also file reports in January of each year with the Administrative Office of the United States Courts. These reports must include the same information required in the judges' reports and must also contain information on the number of arrests, trials and convictions resulting from the interceptions, the utility of the interception, the frequency of both incriminating and innocent conversations overheard, and the manpower used in the eavesdropping period. The Administrative Office of the United States Courts, to whom these reports are given, must file summaries and analyses of the reports with the Congress in April of each year.¹¹¹

Finally, under § 2520, any person whose communication is unlawfully intercepted, used, or disclosed has a civil cause of action against the illegal eavesdropper.¹¹² The victim of such illicit surveillance is entitled to recover actual damages or liquidated damages at the rate of \$100 per day for each day of the eavesdropping or \$1,000, whichever is greater, and punitive damages. Reasonable attorneys' fees and other costs of litigation are also recoverable.¹¹³

IV. Title III—The Case Law

Although the specific question of Title III's constitutionality has not yet been decided by the Supreme Court, it has been considered on numerous occasions by the lower federal courts. With one exception, the federal courts ruling on the validity of Title III have concluded it is constitutional.¹¹⁴ The cases involving the application of Title III divide into cases involving: (1) the "national security" powers of the President; (2) the suppression of wiretap evidence in

108 18 U.S.C. § 2515 (1970).

109 18 U.S.C. § 2518 (1970).

110 18 U.S.C. § 2519 (1970).

111 *Id.*

112 18 U.S.C. § 2520 (1970).

113 *Id.*

114 See *United States v. Cox*, 462 F.2d 1293 (8th Cir. 1972); *United States v. Cox*, 449 F.2d 679 (10th Cir. 1971), *cert. denied*, 406 U.S. 934 (1972); *United States v. Focarile*, 340 F. Supp. 1033 (D. Md. 1972); *United States v. LaGorga*, 336 F. Supp. 190 (W.D. Pa. 1971); *United States v. King*, 335 F. Supp. 523 (S.D. Cal. 1971); *United States v. Lawson*, 334 F. Supp. 612 (E.D. Pa. 1971); *United States v. Becker*, 334 F. Supp. 546 (S.D. N.Y. 1971); *United States v. Perillo*, 333 F. Supp. 914 (D.Del. 1971); *United States v. Leta*, 332 F. Supp. 1357 (M.D. Pa. 1971); *Donlon v. United States*, 331 F. Supp. 979 (D. Del. 1971); *United States v. Scott*, 331 F. Supp. 233 (D.D.C. 1971); *United States v. Cantor*, 328 F. Supp. 561 (E.D. Pa. 1971); *United States v. Sklaroff*, 323 F. Supp. 296 (S.D. Fla. 1971); *United States v. Escandor*, 319 F. Supp. 295 (S.D. Fla. 1970), *rev'd on other grounds, sub nom.*, *United States v. Robinson*, 468 F.2d 189 (5th Cir. 1972). *Contra*, *United States v. Whitaker*, 343 F. Supp. 358 (E.D. Pa. 1972). The *Whitaker* decision has been appealed.

criminal trials; and (3) actions brought to recover damages under the provisions of 18 U.S.C. § 2520.

A. "National Security" Wiretaps

Several of the wiretaps exposed in recent months were considered by the Government to be in the interest of "national security." Since Franklin Roosevelt, Presidents have authorized such wiretaps to varying degrees.¹¹⁵ In 1971 Senator Edward Kennedy disclosed the use of national security wiretaps to a Senate subcommittee. He found that "warrantless devices accounted for an average of 78 to 209 days of listening per device, as compared with a 13-day per device average for those devices installed under court order."¹¹⁶

The single most important national security wiretap case to date dealing with the provisions of Title III has been *United States v. United States District Court*.¹¹⁷ In that case, the Government charged the defendants with conspiring to destroy government property. In response to the defendants' pretrial motion for disclosure of electronic surveillance information, the Government filed an affidavit by the Attorney General stating that he had approved the wiretaps for the purpose of "gather[ing] intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." On the basis of this affidavit and surveillance logs, the Government claimed that the surveillance, though warrantless, was lawful as a reasonable exercise of presidential power to protect the national security. The district court found the surveillance violative of the fourth amendment and issued an order for disclosure of the overheard conversations. The court of appeals upheld the district court, and the Supreme Court held that neither the President nor his Attorney General could authorize electronic surveillance of domestic subversives without obtaining prior judicial approval. Justice Powell, writing for the unanimous Court, dismissed the Government's contention that the requirements of the fourth amendment were not applicable in domestic cases involving the national security. The Court could find no justification for the Executive's asserted authority in either Title III or in the President's inherent power as Chief of State.¹¹⁸

In examining the language of Title III the Court looked to § 2511(3),

¹¹⁵ Roosevelt wrote his Attorney General, Robert Jackson, that he was authorized and directed to authorize the use of bugs and wiretaps by his agents in the investigation of persons "suspected of subversive activities against the Government." 117 CONG. REC. 6480 (daily ed. May 10, 1971). President Truman's Attorney General, Tom Clark, requested that he be given the authority to use electronic surveillance in cases of domestic subversives. Truman gave Clark such "authority." 117 CONG. REC. 6480 (daily ed. May 10, 1971). Lyndon Johnson and his Attorney General (Ramsey Clark, the son of Tom Clark) both frowned on such wiretaps to a great extent, and Clark forbade wiretapping and bugging except in cases involving foreign subversives. Memorandum from Attorney General Ramsey Clark, June 16, 1967, in 117 CONG. REC. 6480 (daily ed. May 10, 1971).

¹¹⁶ Letter from Senator Edward Kennedy to Members of the Subcomm. on Administrative Procedure and Practices of the Senate Judiciary Comm., Dec. 17, 1971. For statistics dealing with court-ordered wiretaps, see ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS (1972).

¹¹⁷ 407 U.S. 297 (1972).

¹¹⁸ *Id.* at 321.

upon which the Government based its argument regarding the constitutional right of the President to approve such warrantless searches. Section 2511 reads, in part, that:

[Nothing] contained in this chapter [shall] be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.¹¹⁹

Although the Court said it found an "implicit" recognition in such language that the President does have certain powers in the specified areas to defend the nation from attempts to overthrow the Government, the Court found that the language was "essentially neutral" insofar as it pertained to the power of the President to order warrantless electronic eavesdropping:

Section 2511(3) certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution.¹²⁰

Reviewing the language of Title III in its totality, the Court found that:

In view of these and other interrelated provisions delineating permissible interceptions of particular criminal activity upon carefully specified conditions, it would have been incongruous for Congress to have legislated with respect to the important and complex area of national security in a single brief and nebulous paragraph. This would not comport with the sensitivity of the problem involved or with the extraordinary care Congress exercised in drafting other sections of the Act. We therefore think the conclusion inescapable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances.¹²¹

In seeking to determine the intent of Congress in legislating on the matter, the Court noted Senator Hart's comments during the debate preceding enactment of the legislation:

Mr. HART However, we are agreed that this language should not be regarded as intending to grant any authority, including authority to put a bug on, that the President does not have now.

In addition, Mr. President, *as I think our exchange makes clear, nothing in section 2511(3) even attempts to define the limits of the President's national security power under present law which I have always found*

119 18 U.S.C. § 2511(3) (1970). See note 95, *supra*.

120 407 U.S. at 303.

121 *Id.* at 306.

*extremely vague . . . Section 2511(3) merely says that if the President has such a power, then its exercise is in no way affected by Title III.*¹²²

Thus, it was clear to the Court that if the President did in fact have the authority to approve warrantless electronic surveillance, it would have to be found in the Constitution for it clearly did not exist in Title III:

One could hardly expect a clearer expression of congressional neutrality. The debate above explicitly indicates that nothing in § 2511(3) was intended to *expand* or to *contract* or to *define* whatever presidential surveillance powers existed in matters affecting the national security. *** viewing § 2511(3) as a congressional disclaimer and expression of neutrality, we hold that the statute is not the measure of the executive authority asserted in this case. Rather, we must look to the constitutional powers of the President.¹²³

The Court found no such power.

In his concurring opinion Justice White argued that the Court should not have dealt with the constitutional issue, and that the decision should have been based solely on § 2511 of Title III.¹²⁴ Within that framework Justice White found that the Attorney General's affidavit seeking to justify the wiretap was wholly deficient:

It is apparent that there is nothing whatsoever in this affidavit suggesting that the surveillance was undertaken within the first branch of the § 2511(3) exception, that is, to protect against foreign attack, to gather foreign intelligence or to protect national security information. The sole assertion was that the monitoring at issue was employed to gather intelligence information "deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." . . .

Neither can I conclude from this characterization that the wiretap employed here fell within the exception recognized by the second sentence of § 2511(3); for it utterly fails to assume responsibility for the judgment that Congress demanded: that the surveillance was necessary to prevent overthrow by force or other unlawful means or that there was any other clear and present danger to the structure or existence of the Government. The affidavit speaks only of attempts to attack or subvert; it makes no reference to force or unlawfulness; it articulates no conclusion that the attempts involved any clear and present danger to the existence or structure of the Government.

The shortcomings of the affidavit when measured against § 2511(3) are patent. Indeed, the United States in oral argument conceded no less. The specific inquiry put to Government counsel was: "Do you think the affidavit, standing alone, satisfies the Safe Streets Act?" The Assistant Attorney General answered "No, sir. We do not rely upon the affidavit itself . . ."¹²⁵

122 114 CONG. REC. 14751 (1968) (emphasis added).

123 407 U.S. at 308.

124 Justice White's argument was based on the doctrine of *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288, 346-47 (1936) (concurring opinion), that "courts should abjure constitutional issues except where necessary to decision of the case before them." 407 U.S. at 340. Also, because the wiretap was unlawful under the Act, the fruits of the search were inadmissible in court proceedings against the defendant and, thus, the necessity for discussion of the constitutional issues was obviated. *Id.*

125 407 U.S. at 340-41.

If the Court majority had applied Justice White's view, Title III's stringent requirements for the required magisterial approval of electronic surveillance would have been securely established as governing the kind of governmental intrusion ultimately disapproved of in *United States v. United States District Court*. As it was, the Court's decision helped to clarify the language of Title III, and affirmed the applicability of its provisions to even the "well-intentioned" electronic eavesdropping carried on by governmental agencies.

B. Suppression of Wiretap Evidence Under 18 U.S.C. § 2518

Under Title III's § 2515 no part of the contents of an illegally intercepted communication or any evidence derived therefrom may be received in any court, before a grand jury, or similar governmental body.¹²⁶ This sanction is designed to compel compliance with the overall requirements of Title III. Further, § 2518(10) provides that any "aggrieved person" may move to suppress such unlawfully procured evidence.¹²⁷ Thus, § 2518 provides the remedy for the right created by § 2515.

In *Alderman v. United States*¹²⁸ petitioners had been convicted of conspiring to transmit murderous threats in interstate commerce. Subsequent to their conviction, they discovered that the place of business of one of the petitioners had been subject to electronic surveillance by the Government. The surveillance had been warrantless, but the Government argued that "no overheard conversation in which any of the petitioners participated [was] relevant to [the] prosecution."¹²⁹ The Court vacated and remanded the case for retrial holding that a petitioner is entitled to the suppression of evidence violative of the fourth amendment, and that if any surveillance is found to be unlawful, the Government must disclose to the petitioner the records of the overheard conversations:

Although [the Government's argument] may appear a modest proposal, especially since the standard for disclosure would be "arguable" relevance, we conclude that surveillance records as to which any petitioner has standing to object should be turned over to him without being screened *in camera* by the trial judge. Admittedly, there may be much learned from an electronic surveillance which ultimately contributes nothing to probative evidence. But winnowing this material from those items which might have made a substantial contribution to the case against a petitioner is a task which should not be entrusted wholly to the court in the first instance. It might be otherwise if the trial judge had only to place the transcript or other record of the surveillance alongside the record evidence and compare the two for textual or substantive similarities . . . But a good deal more is involved. An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all

126 18 U.S.C. § 2515 (1970).

127 18 U.S.C. § 2518 (1970).

128 394 U.S. 165 (1969).

129 *Id.* at 168.

the relevant circumstances. Unavoidably, this is a matter of judgment, but in our view the task is too complex, and the margin for error too great, to rely wholly on the *in camera* judgment of the trial court to identify those records which might have contributed to the Government's case.¹³⁰

The Court, however, also held that such suppression can be successfully urged only by those whose rights have been violated by the search itself and not those "Who are aggrieved solely by the introduction of damaging evidence."¹³¹ And, while records of the illegal surveillance must be turned over to the defendants, they will "not have an unlimited license to rummage" in the Government's files.¹³²

The Government's violation of Title III does not taint all the fruits of surveillance. In *United States v. King*¹³³ the defendants had been charged with conspiring to smuggle marijuana into the United States. The Government based its case almost completely on evidence obtained through a 45-day, around-the-clock wiretap on one of the defendants' phones. The court order authorizing the wiretap was confined in scope to communications concerning specific facts surrounding the conspiracy. The Government made no attempt to minimize the communications intercepted and, based on this lack of minimization, the defendants moved to suppress all of the wiretap evidence on the grounds that the Government had violated the authorizing judicial order.

Although the Court agreed the Government failed to meet the requirements of minimization, it refused to suppress all the evidence, and held that only the evidence not subject to interception would be suppressed.¹³⁴

The *King* precedent has been followed in a number of cases involving the suppression of wiretap evidence. In *United States v. Cox*¹³⁵ the Court held that even if wiretap surveillance violated the minimization requirements, not all of the evidence obtained need be suppressed:

... 18 U.S.C. § 2517 manifests an intent to utilize *all* the evidence obtained by eavesdropping, and § 2517(5) expressly permits the use in court of evidence obtained by wiretap of a crime other than the crime upon which the court order was premised. Clearly Congress did not intend that evidence directly within the ambit of a lawful order should be suppressed because the officers, while awaiting the incriminating evidence, also gathered extraneous conversations. The nonincriminating evidence could be suppressed pursuant to 18 U.S.C. § 2518(10)(a), but the conversations the warrant contemplated overhearing would be admitted.¹³⁶

The *King/Cox* holdings have not been universally applied. In *United States v. Scott*,¹³⁷ the court suppressed the entire contents of the illicit wiretap as well as any evidence derived therefrom. The purpose of the suppression, said

130 *Id.* at 182.

131 *Id.* at 171-72.

132 *Id.* at 185.

133 335 F. Supp. 523 (S.D. Cal. 1971).

134 *Id.* at 545.

135 462 F.2d 1293 (8th Cir. 1972).

136 *Id.* at 1301.

137 331 F. Supp. 233 (D.D.C. 1971).

the Court, was to serve as a deterrent against the Government ignoring the minimization requirements of either Title III or any individual court order:

If this court were to allow the Government agents to indiscriminately intercept every conversation made and to continue monitoring such calls when it becomes clear that they are not related to the "authorized objectives" of the wiretap and in violation of the limiting provisions of the order such order would become meaningless verbiage and the protections to the right or privacy outlined in *Berger* and *Katz* would be illusory.¹³⁸

Another argument for suppression of wiretap evidence has shown mixed results. In *United States v. Askins*¹³⁹ the defendants' motion to suppress was based upon the Government's alleged failure to comply with § 2516's requirement that either the Attorney General or a specially designated Assistant Attorney General authorize the prosecuting attorney to request the eavesdropping order. The court found that while the Attorney General himself had not signed the authorization order, the name of the designated Assistant Attorney General had been signed by a Justice Department official. The Court followed solid precedent in the matter,¹⁴⁰ and ruled that the letter over the signature of the Assistant Attorney General was but a ministerial action and could not alter the fact that the authorization had been granted in compliance with § 2516.

Only a few days after *Askins* was decided, a federal court of appeals in *United States v. Giordano*¹⁴¹ held that the procedure approved in *Askins* was "violative of the separation of powers doctrine and not to be tolerated." In affirming the order of the district court for the suppression of the wiretap evidence, the Court looked to the intention of Congress in enacting Title III:

Congress enacted the various sections of Title III for a purpose. It wanted only specially designated persons of a certain stature within the Justice Department to initiate applications; it directed that the identity of the individual be transmitted to the authorizing magistrate so that he could be certain on whom he was relying; and it wanted the name of the authorizing individual stated in the judicial order so that interested parties might later be able to trace the line of responsibility. We cannot relegate provision after provision to oblivion by terming each a mere "technicality"—or else we leave the statute a shadow of itself, an apparition without substance.¹⁴²

[It is appropriate] to recall Justice Brandeis' famous admonition given nearly forty-five years ago in *Olmstead v. United States*, 277 U.S. 438, 485, 48 S.Ct. 564, 575, 72 L.Ed. 944 (1928) (dissenting), that when "government becomes a lawbreaker, it breeds contempt for law." Similarly, when government consistently tramples upon those parts of the law that do not

138 *Id.* at 248.

139 351 F. Supp. 408 (D. Md. 1972).

140 See *United States v. Ceraso*, 467 F.2d 647 (3d Cir. 1972); *United States v. Cox*, 462 F.2d 1293 (8th Cir. 1972); *United States v. Pisacano*, 459 F.2d 259 (2d Cir. 1972); *United States v. Whitaker*, 343 F. Supp. 358 (E.D. Pa. 1972); *United States v. Iannelli*, 339 F. Supp. 171 (W.D. Pa. 1972); *United States v. Doolittle*, 341 F. Supp. 163 (M.D. Ga. 1972); *United States v. Aquino*, 338 F. Supp. 1080 (E.D. Mich. 1972); *United States v. LaGorga*, 336 F. Supp. 190 (W.D. Pa. 1971).

141 469 F.2d 522 (4th Cir. 1972).

142 *Id.* at 530.

suit its momentary purpose and seeks to justify its conduct by sophistic argumentation, neither respect for the law nor societal order is promoted.¹⁴³

Section 2518 has also been invoked in a motion to suppress evidence gained through a wiretap of conversations between a husband and wife. In *United States v. Kahn*¹⁴⁴ the Government had obtained a court order for the wiretapping of Irving Kahn. Several conversations between Kahn and his wife were intercepted, and the evidence derived from these interceptions led to the indictment of both Kahn and his wife on charges of violating the Illinois state gambling law. The Kahns filed motions to suppress the wiretap evidence pursuant to 18 U.S.C. 2518(1)(a). The Kahns alleged, *inter alia*, that the wiretaps of their conversations violated the marital privilege under the ninth amendment, common law, and 18 U.S.C. § 2517(4). The district court judge suppressed all conversations between the Kahns as being within the marital privilege doctrine, applied through 18 U.S.C. § 2517(4), and the Government appealed.

The Court of Appeals found that while society has an interest in protecting the privacy of marriage, where both spouses are substantial participants in illegal activity, even the most expansive of the marital privileges would not prevent testimony.¹⁴⁵ The court would not allow evidence of such activity to be suppressed because of the marital relationship, and the evidence was to be admitted.

C. *Private Causes of Action Under 18 U.S.C. § 2520*

There is to date a surprising paucity of private civil suits brought under the provisions of Title III's § 2520. Perhaps this reflects the success of the eavesdroppers in keeping their surveillance secret, but perhaps it also indicates that some of the victims who discover that they have been tapped or bugged would rather not press the matter especially if the tap or bug was placed by the Government. A suit against the Government risks public disclosure of the contents of the wiretap logs, and some victims of wiretapping are evidently not willing to take that risk. Of the 13 government officials wiretapped at the request of Henry Kissinger, only one, Morton Halperin, has sued.¹⁴⁶ Daniel Ellsberg has indicated that he intends to sue several individuals, including the President,¹⁴⁷ for the wiretapping that led to the dismissal of charges against him in the Pentagon Papers trial. The past Chairman of the Democratic National Committee, Lawrence F. O'Brien, has filed suit against the Re-Election Committee for the Watergate bugging.¹⁴⁸

143 *Id.* at 531.

144 471 F.2d 191 (7th Cir. 1972).

145 *Id.* at 194.

146 On June 13, 1973, Dr. Morton Halperin, whose telephone had been wiretapped by the Government from November, 1971, to May of 1973, filed suit in the United States District Court for the District of Columbia against Henry Kissinger, John Mitchell, H. R. Halderman, John Erlichmann, General Haig, William Ruckelshaus and "John Doe, Richard Roe and other unknown agents of the FBI." The suit sought money damages, and declaratory and injunctive relief to suppress the contents of the wiretaps. Halperin Complaint, Civil Action No. 1187-73, United States District Court for the District of Columbia.

147 N.Y. Times, May 12, 1973, at 14, col. 5.

148 For a description of the Democrats' reaction, both "official" and personal, see G. HART, *RIGHT FROM THE START—A CHRONICLE OF THE MCGOVERN CAMPAIGN* (1973).

Throughout the course of Congressional debate on Title III, the twofold purpose of the electronic eavesdropping provisions was emphasized. The statute was intended not only to delineate on a uniform basis circumstances and conditions under which the interception of communications by the Government might be authorized, but also to protect the privacy of wire and oral communications¹⁴⁹ by providing criminal penalties, civil recourse for damages, and a denial of admissibility to unlawfully intercepted evidence in civil and criminal proceedings.¹⁵⁰ Thus, while the statutory basis for civil action against persons¹⁵¹ unlawfully intercepting or disclosing wire and oral communications is clear, the reported cases indicate sparse usage of the available remedy.

In *Alderman v. United States*,¹⁵² the Supreme Court for the first time took notice of Title III's enactment. Discussing the rights of the defendants who had moved to suppress wiretap evidence, the Court said:

We do not deprecate Fourth Amendment rights. The security of persons and property remains a fundamental value which law enforcement officers must respect. Nor those who flout the rules escape unscathed. In this respect we are mindful that there is now a comprehensive statute making unauthorized electronic surveillance a serious crime. The general rule under the statute is that official eavesdropping and wiretapping are permitted only with probable cause and a warrant. Without experience showing the contrary, we should not assume that this new statute will be cavalierly disregarded or will not be enforced against transgressors.¹⁵³

In the 1971 case of *Kinoy v. Mitchell*¹⁵⁴ the plaintiff brought action against Attorney General John Mitchell and other officials of the federal government for damages caused by their alleged illegal and unauthorized electronic surveillance of Kinoy's telephone and also to quash subpoenas that had been served on the plaintiff. The Court held that if the Government had conducted unauthorized or illegal electronic surveillance in violation of Kinoy's fourth amendment rights, a cause of action existed under both 18 U.S.C. § 2520 and the fourth amendment:

Congress has specifically granted to persons whose wire or oral communications are intercepted, disclosed or used in violation of Chapter 119 of Title 18 of the United States Code, a civil cause of action for money damages against those who intercept, disclose or use such communications. 18 U.S.C. § 2520. Congress intended that (Title III), which prohibits certain wiretapping and electronic surveillance be as pervasive as the fourth amendment constitutional standards set out in *Berger v. New York*, 388 U.S. 41 . . . and *Katz v. United States*, 389 U.S. 347 . . .¹⁵⁵

Thus, while the Court dismissed four causes of action charging the abuse of grand

149 1968 U.S. CODE CONG. AND ADM. NEWS, at 2153.

150 *Id.* at 2156.

151 "Persons" is defined in the Act specifically to include agents of the federal government. 18 U.S.C. § 2510(6) (1970).

152 394 U.S. 165 (1969).

153 *Id.* at 175.

154 331 F. Supp. 379 (S.D.N.Y. 1971).

155 *Id.* at 382.

jury procedure and bad faith usage of the subpoena process, it refused to dismiss the fifth cause of action charging the Government with violation of Title III and seeking damages under § 2520. The Court noted that the plaintiff could prevail under such a suit "if [it was proved] that defendants conducted illegal wiretapping of [the] plaintiff's telephone."¹⁵⁶ There is no further reported adjudication of the Kinoy claim for civil damages.

In *Abramson v. Mitchell*¹⁵⁷ plaintiffs in an appeal from a lower court decision sought damages for an unauthorized wiretap on their phone. The Court noted that the statutory defense of good faith reliance on a court order does not serve as a complete bar to a civil damage action. It might happen, said the court, that the application for the wiretap itself was defective even though it stated probable cause for a search.¹⁵⁸ The Court reversed the trial court's dismissal of the case and remanded it for another trial; there has as yet been no reported judicial determination of plaintiff's action for damages under 18 U.S.C. § 2520.

In *United States v. La Gorga*,¹⁵⁹ another case involving questionable government wiretapping activities, a federal district court ordered the production of transcripts and tapes of the clearly irrelevant conversations of nondefendants whose conversations had been monitored. The Court did not accept the defendants' argument that all evidence should be suppressed because there had been little attempt to minimize the interception of irrelevant material, but was reluctant to "disparage the objections to loss of privacy which become very understandable . . . when one reads the irrelevant conversations which [were intercepted]."¹⁶⁰ While the Court would not suppress all the evidence, it felt that:

. . . such annoyance as might be caused by the interception of calls of innocent persons in this case should not be permitted to continue any longer. We will suppress only the evidence pertaining to the irrelevant conversations and order that the transcripts and portions of the tape of those interceptions be impounded.

Furthermore, an additional inventory shall be prepared by the Government and served upon all individuals not in the defendants' households whose irrelevant conversations were monitored.

We believe that in taking this action due respect will be accorded the Congressional intent to provide a specific remedy of civil damages in § 2520 to those whose communications may have been intercepted in violation of the law. If the aggrieved parties wish to file a suit for damages, then the alleged offending tapes may be released for use as evidence.¹⁶¹

To date there has been no reported civil action brought for the overextensive wiretapping found in *La Gorga*.

In *Meredith v. Gavin*,¹⁶² the plaintiff sought damages under § 2520 against

156 *Id.*

157 459 F.2d 955 (8th Cir. 1972).

158 *Id.* at 957.

159 336 F. Supp. 190 (W.D. Pa. 1971).

160 *Id.* at 196.

161 *Id.* at 197.

162 446 F.2d 794 (8th Cir. 1971).

an insurance company whose agent had secretly taped telephone conversations between himself and the plaintiff. The plaintiff argued that the recording of his conversations was an "interception" within the meaning of § 2510 (4) and therefore constituted a violation of the statute. Plaintiff also argued that if the interception was not a violation of Title III, its subsequent use and disclosure were a violation, and that he was therefore entitled to a directed verdict as to liability and minimum damages of \$1,000 as provided under § 2520.

The Court held that the insurance company agent, as a party to a conversation, could protect himself and his credibility by recording the conversation, unless his purpose was evil; *i.e.*, to commit or attempt a criminal or tortious act, or injure an unsuspecting participant in some vague but illegitimate fashion.¹⁶³ The Court found no such evil purpose and affirmed the trial court's judgment that there was no liability for the agent's actions under § 2511(2)(d), and that no damages could be recovered under § 2520.

In *United States v. Cox*,¹⁶⁴ a case similar to *La Gorga*, the Court held that evidence was not to be suppressed merely because government agents failed to minimize the interception of conversation irrelevant to their investigation. This did not mean that those whose irrelevant conversations were overheard did not have a remedy:

If appellants, and the unindicted persons whose conversations were overheard, have any remedy under Title III other than the suppression of conversations outside the warrant's scope, it lies in § 2520 as a civil suit against the investigating officers alleging that they exceeded their authority.¹⁶⁵

All of the courts presented with the matter have reaffirmed the availability of § 2520 to victims of unlawful wiretapping. In some instances, as in *La Gorga*, the courts have gone out of their way to instruct potential § 2520 litigants in the purposes of § 2520. It remains true, however, that § 2520, as effective a sanction as exists for victims of wiretapping and bugging, has seldom been invoked.

V. Conclusion

It seems clear that the Government and others have unlawfully and extensively wiretapped and bugged American citizens, in complete disregard of Title III of the Omnibus Crime Control and Safe Streets Act. Congress clearly intended that this "dirty business," as Mr. Justice Holmes referred to electronic surveillance in *Olmstead v. United States*, be severely restricted and supervised by judicial authority. Congress also intended to punish those who violated the rights of their fellow citizens and made them victims of illicit invasions of privacy. The sanctions for such disregard of the law of the land are properly harsh and readily available; they should be applied at every opportunity.

Staff

¹⁶³ *Id.* at 798.

¹⁶⁴ 462 F.2d 1293 (8th Cir. 1972).

¹⁶⁵ *Id.* at 1301-02.