Fordham International Law Journal

Volume 6, *Issue* 3 1982 *Article* 5

Foreign Intelligence Surveillance: Intelligence Gathering of Prosecution?

Christine A. Burke*

*

Foreign Intelligence Surveillance: Intelligence Gathering of Prosecution?

Christine A. Burke

Abstract

This Note considers the permissible uses of information secured through a FISA surveillance in light of the fourth amendment issue raised by Falvey. It concludes that when information is sought for purposes of national security or foreign affairs, the nature of the investigation and the compelling government interest in obtaining the information require fourth amendment standards in some respects different and lower than in ordinary criminal investigations.

FOREIGN INTELLIGENCE SURVEILLANCE: INTELLIGENCE GATHERING OR PROSECUTION?

INTRODUCTION

During 1980, the Federal Bureau of Investigation (FBI) began to investigate an international terrorist organization believed to be operating in New York.[1] As part of its investigation, the FBI obtained a warrant on April 3, 1981 authorizing the electronic surveillance[2] of two United States citizens, Thomas Falvey and George Harrison,[3] pursuant to the Foreign Intelligence Surveillance Act of 1978[4] (FISA or Act).[5] The surveillance continued until June 19 or 20 1981;[6] Falvey and Harrison were then arrested and charged with smuggling arms and equipment from the United States to the Provisional Irish Republican Army (IRA) in Ireland.[7]

The government sought to use tapes of the intercepted telephone conversations at trial.[8] Pursuant to FISA requirements, the government obtained the Attorney General's approval and informed the defendants and the court of its intention to use those tapes.[9] The government moved for an order under 50 U.S.C. §

---

1. United States v. Falvey, 540 F. Supp. 1306, 1308 (E.D.N.Y. 1982).

2. *Id.* The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811 (Supp. II 1978), contains four separate definitions of electronic surveillance. The definitions vary depending upon the type of communications or activities subject to surveillance, *id.* § 1801(f)(3), (4), the type and location of the facility or premises to be monitored, *id.*, and whether a United States citizen or legal resident alien is a partcipant in the communications or activities under investigation. *Id.* § 1801(f)(1), (2).

3. 540 F. Supp. at 1308.

4. 50 U.S.C. §§ 1801-1811.

5. 540 F. Supp. at 1308.

6. *Id.*

7. *Id.* The defendants Thomas Falvey, Michael Flannery, George Harrison, Patrick Mullin and Daniel Gormley were indicted for conspiracy and numerous offenses relating to the purchase of arms in violation of 18 U.S.C. § 371 (1976)(conspiracy to commit offense or to defraud the United States), 26 U.S.C. §§ 5841, 5842, 5845 (1976)(relating to the registration or identification of firearms), and 26 U.S.C. § 2778 (1976)(control of arms exports and imports). 540 F. Supp. at 1307.

8. 540 F. Supp. at 1308.

9. Pursuant to 50 U.S.C. § 1806(b) (Supp. II 1978), the government obtained the advance authorization of the Attorney General to use the information in a criminal proceeding. 540 F. Supp. at 1308. That provision is designed to ensure that the Attorney General has an opportunity to prevent the disclosure in litigation of information that might jeopardize national security interests. *See* H. REP. No. 1720, 95th Cong., 2d Sess., *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 4048, 4060 [hereinafter cited as HOUSE CONFERENCE REPORT]. Prior to trial, the government must notify the court and the person against whom the evidence will be offered of its intention to disclose the information. 50 U.S.C. § 1806(c).

1806(f)[10] declaring that the surveillance had been conducted according to FISA specifications and that the evidence therefore would be properly admissible at trial.[11]

The defendants responded with a motion to suppress the fruits of the FISA surveillance on the grounds that FISA on its face and as applied in this case, violated the first, fourth, fifth, sixth and ninth amendments and articles I and III of the Constitution.[12] The court denied the defendants' motion and admitted the evidence.[13] The court held that the surveillance had been conducted in accordance with the provisions of the statute[14] and that the statute was constitutional.[15] *United States v. Falvey* was the first decision to consider the constitutionality of FISA.[16]

---

10. The section provides that whenever a court or other authority is notified that the information obtained pursuant to the surveillance will be offered as evidence or otherwise disclosed at trial, the court will "review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). Once such an affidavit is submitted, issues relating to the FISA surveillance can be resolved only in a United States district court. If the case is already pending in federal district court, it remains there for resolution of FISA issues. *Id.*

11. 540 F. Supp. at 1308.

12. *Id.* The only issue to be discussed in this Note will be the issue raised under the fourth amendment. For the first amendment issue raised under FISA, see *id.* at 1314. For the fifth and sixth amendment arguments, see *id.* at 1315. For the article I and III issues, see *id.* at 1313 n.16.

13. *Id.* at 1316.

14. Specifically, the court found that the President authorized the Attorney General to approve the application for the surveillance. *Id.* The application was made by a federal officer and approved by the Attorney General. *Id.* The application contained the necessary statements and the certifications were not clearly erroneous. *Id.* There was probable cause to believe the targets, Falvey and Harrison, were agents of a foreign power, and this finding was not based soley on the basis of activities protected by the first amendment. *Id.* There was probable cause to believe that the facilities targeted were to be used by a foreign power. *Id.* The minimization procedures employed were properly drawn. *Id.* Although the defendants lost on the motion to suppress, they were subsequently acquitted at the jury trial.

15. *Id.*

16. 540 F. Supp. 1306 (E.D.N.Y. 1982). A second case that ruled on the constitutionality of FISA is United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982). In *Belfield*, the defendants were charged with conspiracy to murder, accessory after the fact, grand larceny, unauthorized use of a vehicle and perjury in connection with the assassination of Akbar Tabatabai, president of the Iran Freedom Foundation. *Id.* at 141-42. Prior to the trial, defendants requested disclosure of any electronic surveillance covering them. *Id.* at 142. The government answered that each appellant was overheard on separate occasions during the course of the electronic surveillance authorized by the United States FISA Court. *Id.* The legality of the surveillance was determined ex parte after examination in camera. *Id.* The defendants challenged the procedures on both statutory and constitutional grounds. *Id.* The court of appeals held that the in camera, ex parte proceeding did not violate FISA provisions,

The most serious constitutional issue raised by *Falvey* is whether evidence obtained pursuant to a FISA warrant may be used in the prosecution of a United States citizen without violating the fourth amendment. This Note considers the permissible uses of information secured through a FISA surveillance in light of the fourth amendment issue raised by *Falvey*. It concludes that when information is sought for purposes of national security or foreign affairs, the nature of the investigation and the compelling government interest in obtaining the information require fourth amendment standards in some respects different and lower than in ordinary criminal investigations.[17]

I. *FOURTH AMENDMENT RIGHTS: ADJUSTMENT OF THE PROCEDURES ACCORDING TO THE GOVERNMENT INTEREST INVOLVED*

When the government conducts any type of search and seizure, the fourth amendment requires that government interests be balanced against the individual's privacy interests.[18] Generally, the fourth amendment protects the individual from unreasonable searches and seizures by requiring first, a warrant, and second, that the issuance of the warrant be based on probable cause.[19]

The purpose of the warrant process is to interpose a neutral figure between the citizen and the law enforcement official to

---

nor did it violate the defendants' fifth and sixth amendment rights. *Id. See also* United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982).

17. *See infra* notes 69-76, 99-104 and accompanying text.

18. In Berger v. New York, 388 U.S. 41 (1967), the Court held:

> The effect of the Fourth Amendment is to put the courts of the United States . . . under limitations and restraints as to the exercise of such power . . . and to forever secure the people . . . against all unreasonable searches and seizures under the guise of law. This protection reaches all alike, whether accused of a crime or not, and the duty of giving to it force and effect is obligatory upon all . . . . The tendency of those who execute the criminal laws of the country to obtain conviction by means of unlawful seizures . . . should find no sanction in the judgments of the courts which are charged at all times with the support of the Constitution and to which people of all conditions have a right to appeal for the maintenance of such fundamental rights.

Id. at 50 (quoting Weeks v. United States, 232 U.S. 383, 391-92 (1914)).

19. The fourth amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

guarantee that the privacy of the individual will be disturbed only after certain prescribed standards, including probable cause, have been met.[20] In the area of criminal investigation, the Supreme Court has consistently stated that only exigent circumstances[21] or consent[22] will excuse approval by the impartial magistrate. In criminal investigations, the magistrate must find probable cause to believe that a specific crime has been or is being committed before he may issue a warrant.[23] The probable cause requirement is intended "to safeguard citizens from rash and unreasonable interferences with privacy and unfounded charges of crime," and also to "give fair leeway for enforcing the law in the community's protection."[24] "The rule of probable cause," declared the Court, "is a practical, nontechnical conception affording the best compromise that has been found for accommodating these often opposing interests."[25] Thus, the fourth amendment balances privacy interests against prosecutorial interests by requiring prior judicial authorization and a strong showing of probable cause.

---

20. *See* Coolidge v. New Hampshire, 403 U.S. 443 (1971); Johnson v. United States, 333 U.S. 10 (1948).

21. The Supreme Court has held that in certain situations exigent circumstances will permit warrantless searches. United States v. Chadwick, 433 U.S. 1 (1977)(police may search a movable vehicle for which the individual has a lessened expectation of privacy provided probable cause and exigent circumstances are present); Chimel v. California, 395 U.S. 1 (1969) (police officer may conduct a search incident to lawful arrest in order to protect himself and prevent destruction of the evidence); Terry v. Ohio, 392 U.S. 1 (1968)(stop and frisk may be permitted where there is an immediate threat to the officers' safety); Schmerber v. California, 384 U.S. 757 (1966)(police may conduct a search without a warrant if there is probable cause to believe that evidence in or on the individual's body is likely to disappear or be destroyed).

22. The Supreme Court has held that a valid consent to search obviates the need to obtain a warrant or to show that the police conduct was premised on probable cause. Schneckloth v. Bustamonte, 412 U.S. 218 (1973). *See generally* 2 W. LAFAVE, SEARCH AND SEIZURE § 8.1 (1978).

23. *Berger*, 388 U.S. at 59. *See also* Beck v. Ohio, 379 U.S. 89 (1964). In *Beck*, the Court held that ommission of a warrant "bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment." *Id.* at 96.

24. Brinegar v. United States, 338 U.S. 160, 176 (1949). The nature or concept of probable cause remains substantially the same as it was articulated by the Supreme Court in *Brinegar* and Carroll v. United States, 267 U.S. 132 (1925). In *Carroll*, the Court held that probable cause exists when "the facts and circumstances within [the arresting officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief" that an offense is being or has been committed. *Id.* at 162.

25. *Brinegar*, 338 U.S. at 176.

The fourth amendment compromise between competing interests need not always be maintained in precisely the same way.[26] For example, when the government gathers information for foreign affairs and national security purposes, it is concerned with the survival of the nation, an interest of higher priority than the prosecution of domestic crime. The government's interest in obtaining timely, accurate information concerning the intentions and activities of foreign powers and international terrorist organizations does not preempt fourth amendment rights but does require a balancing of interests different from the balancing in criminal investigations. That weighing of interests in intelligence gathering cases may not always require prior judicial authorization and a strong showing of probable cause.

Intelligence investigations detect and evaluate two types of information: information "relating to the capabilities, intentions and activities of foreign powers, organizations or persons,"[27] and "information gathered and activities conducted to protect against espionage and other clandestine activities, sabotage, international terrorist activities or assassinations."[28]

Fourth amendment protections still apply to foreign affairs and national security cases. The Court stated in *United States v. Curtiss-Wright Export Corp.*,[29] that the presidential power in foreign affairs is "a power which . . . like every other governmental power must be exercised in subordination to the applicable provisions of the Constitution."[30] In *United States v. United States District Court*[31] *(Keith)*, the Court held that national security interests

---

26. There are certain investigative techniques that incorporate a different probable cause test than the standard ordinarily used for arrests and searches. In Camara v. Municipal Court, 387 U.S. 523 (1967), the Court engaged in a "balancing" of the "need to search against the invasion which the search entails" in adjusting the probable cause standard for housing inspection warrants. *Id.* at 537. This balancing approach was subsequently used in Terry v. Ohio, 392 U.S. 1 (1968), in which the Court permitted a "stop and frisk" upon information that fell short of probable cause to make a full fledged arrest and full search of the person. *Id.* at 27. For a more complete analysis of these investigative techniques, see *infra* notes 156-164 and accompanying text. *See generally* 1 W. LAFAVE, SEARCH AND SEIZURE, § 2.1 (1978).

27. Exec. Order No. 12,036, § 4-205, 3 C.F.R. 112, 133 (1979), *reprinted in* 50 U.S.C. § 401 (Supp. II 1978).

28. *Id.* § 4-202, 3 C.F.R. at 133 (1979), *reprinted in* 50 U.S.C. § 401 (Supp. II 1978).

29. 299 U.S. 304 (1936).

30. *Id.* at 320. *See also* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

31. 407 U.S. 297 (1972). The case is referred to as *Keith* because Judge Damon R. Keith presided over the case in the district court. United States v. Sinclair, 321 F. Supp. 1074 (E.D. Mich. 1971).

did not render fourth amendment requirements inoperative and would not justify warrantless electronic surveillance of a domestic organization.[32]

II. *HISTORY OF ELECTRONIC SURVEILLANCE*

Despite the highly intrusive nature of electronic surveillance, both the judiciary and Congress were hesitant to recognize fourth amendment protections in that area. Those two branches were even more reticent to apply fourth amendment protections to national security and foreign affairs cases.[33] The Supreme Court first addressed the applicability of fourth amendment protections to electronic surveillance in the 1927 case of *Olmstead v. United States*.[34]

In *Olmstead*, the Court held that warrantless electronic surveillance did not violate the fourth amendment's prohibition against unreasonable search and seizure because such surveillance did not physically enter the constitutionally protected areas of the house or the office.[35] Six years later, Congress placed the first restrictions on the use of electronic surveillance by enacting the Federal Communications Act of 1934.[36] Section 605 of the act made it a crime for any person to intercept and divulge or publish the

---

32. The Court held that the use of "surveillance [is not] a welcome development even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law abiding-citizens." 407 U.S. at 312. The Court continued that although "physical entry of the home is the chief evil against which . . . the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance . . . . Broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate Fourth Amendment safeguards." *Id.* at 313.

33. S. REP. No. 604, 95th. Cong., 2d Sess. 6-7, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS, 3908, 3909 [hereinafter cited as SENATE JUDICIARY COMMITTEE REPORT.]. For a detailed history of the development of electronic surveillance, see Note, *The Foreign Intelligence Surveillance Act: Legislating a Judicial Role in National Security Surveillance*, 78 MICH. L. REV. 1116 (1980); Note, *The Foreign Intelligence Surveillance Act of 1978*, 13 VAND. J. TRANSNAT'L L. 719 (1980).

34. 277 U.S. 438 (1928).

35. *Id.* at 466. By a five-to-four decision, the Supreme Court removed electronic surveillance, unaccompanied by physical trespass, from the purview of constitutional supervision for nearly forty years. The Court did not apply the fourth amendment's requirement that invasions of privacy occur only after a magistrate has issued a warrant based on probable cause, despite Justice Brandeis' warning that "writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping." *Id.* at 476 (Brandeis, J., dissenting).

36. Federal Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1103-04 (codified at 47 U.S.C. § 605 (1976)).

contents of wire and radio communications.[37] The Supreme Court applied the statute to wiretapping by state and federal officials as well as by private persons in *Nardone v. United States* (*Nardone I*).[38] It further held that communications intercepted in violation of the act were inadmissible in federal courts.[39] Finally, in *Berger v. New York*[40] and *Katz v. United States*,[41] the Supreme Court recognized that warrantless electronic surveillance conducted in criminal investigations violated the fourth amendment.[42]

Neither section 605, the *Nardone I* decision, nor the *Berger* and *Katz* cases had an impact on the use of electronic surveillance for purposes of national security. The Supreme Court exclusionary rule applied only in criminal proceedings. Moreover, in 1940, President Roosevelt stated in a memorandum to the Attorney General that section 605 and the *Nardone I* decision did not prohibit warrantless electronic surveillance involving the defense of the nation.[43]

---

37. 47 U.S.C. § 605. The relevant provisions state:

> No person not being authorized by the sender shall intercept any (wire or radio) communications and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto.

Id.

38. 302 U.S. 379 (1937).

39. In *Nardone I*, the Court found § 605 binding on law enforcement agents and barred the introduction of wiretap records. *Id.* at 383. In Nardone v. United States, 308 U.S. 338 (1939)(*Nardone II*), the Court barred the introduction of evidence derived from the wiretap. *Id.* at 340-43. The Justice Department soon adopted the view that since § 605 made it unlawful to "intercept" and "divulge" communications, the act did not prohibit wiretapping by agencies of the government if the information intercepted was disseminated only within the government for law enforcement purposes. *See* Donner, *Electronic Surveillance: The National Security Game*, CIV. LIB. REV., Summer 1975, at 15, 19.

40. 388 U.S. 41 (1967).

41. 389 U.S. 347 (1967).

42. The *Berger* case involved the constitutionality of a New York statute which authorized eavesdropping for periods of up to 60 days based on a sworn statement that there was reasonable ground to believe that evidence of a crime would be obtained. 388 U.S. at 55-56. The Court struck down the statute because, among other things, the 60 day authorization permitted a series of searches and seizures based on one finding of probable cause. *See infra* notes 55-62 and accompanying text.

In 1968, when the Court decided *Katz*, it finally recognized that the "underpinnings of *Olmstead* . . . 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. The Court held that government officers must obtain a warrant from a neutral magistrate before employing electronic surveillance in the course of any state or federal criminal investigation. *Id.* at 356.

43. Confidential Memorandum from Franklin D. Roosevelt to Robert H. Jackson (May 21, 1940), *reprinted in* Zweibon v. Mitchell, 516 F.2d 594, 673 app. (D.C. Cir. 1975).

Later presidents expanded the scope of national security surveillance.[44] Even the *Berger* and *Katz* decisions disclaimed any intent to extend their holdings to cases "involving national security."[45]

In response to the *Katz* and *Berger* cases, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968.[46] Title III of the act allows electronic surveillance only in cases involving specified serious crimes and imposes a warrant requirement for such surveillance.[47] Title III, however, disclaims any congressional intent to modify the President's authority "to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities."[48]

The Supreme Court did not rule on the constitutionality of warrantless electronic surveillance for national security purposes

---

44. *See* SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 755, 94th Cong., 2d Sess., bk. II, at 36-38, 60-61, 105-06, 121-22 (1976). Although abuses of warrantless electronic surveillance for national security purposes first came to public attention during the Watergate investigations of the Nixon Administration, the Church Committee concluded that such abuses predated the presidency of Richard Nixon. *Id.* at 12. The Church Committee Report stated:

> Since the early 1930's intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of a judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, a Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security . . . .

Id.

45. *Katz*, 389 U.S. at 358 n.23. Three Justices briefly expressed their views on the national security exception in concurring opinions. Justice White stated that the President's inherent article II powers permitted warrantless electronic surveillance for national security purposes. *Id.* at 364 (White, J., concurring). Justice Douglas, with whom Justice Brennan concurred, argued that the President and Attorney General could not act as disinterested neutral magistrates because their duties to "investigate and prevent breaches of national security" made it impossible for them to be impartial. *Id.* at 359-60 (Douglas, J., concurring). *See also Berger*, 388 U.S. 41.

46. Pub. L. No. 90-351, 82 Stat. 197 (1968)(codified at 18 U.S.C. §§ 2510-2520 (1976)).

47. 18 U.S.C. §§ 2510-2520. *See* S. REP. NO. 1097, 90th Cong., 2d Sess. 66-76 (1968) *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2153-63 [hereinafter cited as TITLE III SENATE REPORT]. Title III established procedures for government officials to follow in order to secure warrants for electronic surveillance in criminal investigations. 18 U.S.C. §§ 2510-2520. In contrast to § 605 of the Communications Act of 1934, 47 U.S.C. § 605 (1976), which prohibited all persons from intercepting wire and radio communications in most circumstances, title III set standards for court approval of that type of surveillance. 18 U.S.C. §§ 2510-2520.

48. 18 U.S.C. § 2511(3).

until 1972. Then, in *Keith*, the Court held that the fourth amendment required prior judicial authorization for the electronic surveillance of American citizens suspected of national security breaches.[49] The Court was not confronted with, and did not address, the constitutionality of warrantless electronic surveillance in cases involving a foreign power or its agent.[50] That open question prompted Congress to enact the Foreign Intelligence Surveillance Act of 1978.[51] The Act prescribes standards and procedures for the

---

49. 407 U.S. at 321-24. The *Keith* case arose from a criminal proceeding in the United States District Court for the Eastern District of Michigan. The United States charged three defendants with conspiracy to destroy government property in violation of 18 U.S.C. § 371. One of the defendants, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan. 407 U.S. at 299. Plamondon sought disclosure of the government's electronic surveillance records and a hearing to determine whether the government had used information from warrantless wiretaps to support the indictment. *Id.* at 299-300. The government claimed that the warrantless surveillance was a lawful exercise of presidential power to protect national security. *Id.* at 301. District Judge Damon Keith ruled that the surveillance violated the fourth amendment and that records of the wiretaps had to be disclosed. United States v. Sinclair, 321 F. Supp. 1074, 1079-80 (E.D. Mich. 1971). Both the United States Court of Appeals for the Sixth Circuit and the Supreme Court affirmed the district court order. United States v. United States District Court, 444 F.2d 651, 664-69 (6th Cir. 1971), *aff'd*, 407 U.S. 297, 321-24 (1972). *See infra* notes 69-76 and accompanying text.

50. 407 U.S. at 321-22 n. 20. There has been tremendous confusion in case law and statute as to the distinction between domestic and foreign intelligence gathering. In United States v. United States District Court, 407 U.S. 297 (1972), the Court analyzed the domestic aspects of national security but did not address "the issues which may be involved with respect to activities of foreign powers or their agents." *Id.* at 322 (footnote omitted). *Keith* added to the confusion surrounding national security. The Court emphasized that it was difficult to distinguish between domestic and foreign threats to the structure and existence of the government. *Id.* at 309 n.8. The Court acknowledged that title III of the Omnibus Crime Control and Safe Streets Act of 1968 uses "national security" to refer only to the activities of foreign powers. *Id.* § 2511(3). Nevertheless, the Court continued to apply the term national security to both domestic and foreign intelligence operations. *Keith*, 407 U.S. at 309 n.8. In Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (en banc), *cert. denied*, 425 U.S. 944 (1976), the court extended the holding in *Keith* and its warrant requirement to a wiretap of a domestic organization that was not involved with a foreign power or foreign agent. *Id.* at 613-14. In a lengthy footnote, the court attempted to distinguish between domestic security and foreign security. *Id.* at 613 n.42. The court, however, concluded " 'national security' will generally be used interchangeably with 'foreign security' except where the context makes it clear that it refers to both 'foreign security' and 'internal security.' " *Id.* On remand, the district court established a different categorization and distinguished "domestic security," "domestic national security," and "foreign security" surveillances. Zweibon v. Mitchell, 444 F. Supp. 1296, 1299 n.3 (D.D.C. 1978), *rev'd in part and remanded on other grounds*, 606 F.2d 1172 (D.C. Cir. 1979).

51. Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-1811 (Supp. II 1978)). Three federal appellate courts have ruled on the constitutionality of warrantless electronic surveillance for foreign intelligence. The Third and Fifth Circuits have held that the executive branch has inherent constitutional power under article II to conduct such

authorization of electronic surveillance in foreign intelligence and counterintelligence investigations.[52] Due to the extreme secrecy and protracted nature of such investigations, the procedures and probable cause standards embodied in the Act differ from the corresponding requirements for criminal investigations under title III.

III. *VARYING REQUIREMENTS OF PROBABLE CAUSE*

A. *Title III and Domestic Criminal Surveillance*

Under ordinary law enforcement procedures not involving electronic surveillance, a warrant will not issue unless there is probable cause to believe that a specific crime has been, is being or is about to be committed.[53] Furthermore, a judicial warrant must be supported by an oath or affidavit particularly describing the place to be searched and the persons or things to be seized.[54] The Court applied those standards to the use of electronic surveillance in *Berger v. New York*.[55] New York's wiretapping statute had permitted electronic surveillance if there were reasonable grounds to believe that evidence of a crime would be obtained.[56] The Court held that the "reasonable ground" requirement of the statute was not equivalent to the probable cause standard of the fourth amendment.[57] While the Court declared that " '[t]he requirements of the

---

surveillance. United States v. Butenko, 494 F.2d 593 (3d Cir.) (en banc), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974). In a plurality opinion, the Circuit Court for the District of Columbia indicated that, absent exigent circumstances, the President must obtain a warrant for all national security surveillance, domestic as well as foreign, conducted within the United States. *Zweibon*, 516 F.2d at 651. *See infra* note 76.

52. 50 U.S.C. § 1801(e).

53. The Supreme Court has held that: "Probable cause under the Fourth Amendment exists where the facts and circumstances within the affiant's knowledge, and of which he has reasonably trustworthy information, are sufficient unto themselves to warrant a man of reasonable caution to believe that an offense has been or is being committed." Berger v. New York, 388 U.S. 41, 55 (1967). *See also* Brinegar v. United States, 338 U.S. 160, 175-76 (1949); Husty v. United States, 282 U.S. 694, 700-01 (1931); Carroll v. United States, 267 U.S. 132, 162 (1925).

54. U.S. CONST. amend. IV. *See also* FED. R. CRIM. P. 41. Rule 41 of the *Federal Rules of Criminal Procedure* governs the issuance, content, execution and return of federal search warrants. *Id.* Rule 41 requires: (1) a pre-issuance determination of probable cause; (2) issuance only upon oath or affirmation in support of the probable cause showing; and (3) particularity of description in the warrant of the place to be searched and the persons or things to be seized. *Id.*

55. 388 U.S. 41 (1967).

56. *Id.* at 54-55.

57. *Id.* at 55.

fourth amendment are not inflexible, or obtusely unyielding to the legitimate needs of law enforcement,'[58] it is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded."[59] The Court concluded that law enforcement investigations which employ covert electronic surveillance require prior judicial authorization of the surveillance,[60] particularity in the application and order,[61] and a showing of probable cause that a specific crime has been or is being committed.[62]

Congress followed the dictates of *Berger* when it enacted title III of the Omnibus Crime Control and Safe Streets Act of 1968.[63] Title III provides that the magistrate must find that there is probable cause to believe that a particular crime has been or is being committed.[64] The statute effectuates that standard by requiring that the application contain a "full and complete statement of the facts . . . relied upon by the applicant, to justify his belief that (a wiretap) order should be issued."[65] That statement must include "details as to the particular offense that has been, is being, or is about to be committed."[66] The statute requires that the application specify the identity of the targeted person, the nature and location of the facilities subject to surveillance and include a particular description of the communications sought.[67] Title III adequately provided for the constitutional requirements of judicial authorization, particularity and a finding of probable cause set out by the Court in *Berger*.[68]

---

58. *Id.* at 63 (quoting Lopez v. United States, 373 U.S. 427, 464 (1963) (Brennan, J., dissenting)).

59. 388 U.S. at 63.

60. According to the Court, New York's wiretapping statute did satisfy the fourth amendment's requirement that a detached and neutral magistrate be interposed between the police and the public. *Id.* at 54.

61. *Id.* at 55. New York's statute was incompatible with the fourth amendment's requirement of particularity. *Id.* The Court recognized that the need for particularity and evidence of reliability was especially great in the case of electronic eavesdropping because it involves an intrusion of privacy that is broad in scope. *Id.* at 55-56.

62. *Id.* at 54-55.

63. 18 U.S.C. §§ 2510-2520 (1976). *See* TITLE III SENATE REPORT, *supra* note 47, at 2153-63.

64. 18 U.S.C. § 2518(3)(a).

65. *Id.* § 2518(1)(b).

66. *Id.*

67. *Id.* § 2518(1)(b)(ii)-(iv).

68. Although the Supreme Court has never decided the constitutionality of title III as a whole, it has held certain sections of the statute constitutional. *See* United States v. Giordano,

B. *Probable Cause:* Keith *and National Security Surveillance*

In *Keith*, the Court noted that the presence of national security considerations added elements to both sides of the fourth amendment balance not present in ordinary criminal investigations.[69] The Court stated that, in national security cases, prior determination by a magistrate is particularly important because "[n]ational security cases . . . often reflect a convergence of First and Fourth amendment values not present in cases of 'ordinary' crime. . . . The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' "[70] In addition, the Court noted that the fourth amendment incorporates the historical judgment that unreviewed executive discretion may yield too readily to the pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.[71]

While recognizing that the fourth amendment imposed a warrant procedure for electronic surveillance in national security cases,[72] the Court acknowledged that domestic threats to national security posed practical and policy considerations distinct from those involved in ordinary criminal cases.[73] The Court noted that warrant applications and orders may "vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection."[74] The opinion stated that Congress is not constitutionally obligated to maintain a probable cause standard that called for evidence of criminal activity. The Court noted that

> [t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many

---

416 U.S. 505 (1974); United States v. Chavez, 416 U.S. 562 (1974). Every appellate court which has considered the issue has found the statute constitutional. *See* United States v. Sklaroff, 506 F.2d 837 (5th Cir.), *cert. denied*, 423 U.S. 874 (1975); United States v. Martinez, 498 F.2d 464 (6th Cir.), *cert. denied*, 419 U.S. 1056 (1974); United States v. Tortorello, 480 F.2d 764 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973); United States v. Cafero, 473 F.2d 489 (3d Cir.), *cert. denied*, 417 U.S. 918 (1973).

69. 407 U.S. at 315-17.

70. *Id.* at 313-14.

71. *Id.* at 317 (footnote omitted).

72. *Id.* at 320.

73. *Id.* at 320-21.

74. *Id.* at 323.

> types of crime. . . . Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime. . . . It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of (Title III) but should allege other circumstances more appropriate to domestic security cases . . . .[75]

The *Keith* decision limited its discussion to the domestic aspects of national security surveillance. However, the opinion contains nothing to suggest that the same analysis would not be applicable to cases of electronic surveillance for foreign intelligence and counterintelligence purposes.[76]

---

75. *Id.* at 322-23.

76. The distinction between domestic and foreign security is untenable. The government itself, up to and including the arguments in *Keith*, asserted that the area was indivisible. It also maintained that if such distinction did exist, domestic organizations posed a greater threat to the national security. *See* NATIONAL LAWYERS GUILD, RAISING AND LITIGATING ELECTRONIC SURVEILLANCE CLAIMS IN CRIMINAL CASES § 8.3(a) (1977). The government has argued that "foreign and domestic affairs are inextricably intertwined and . . . any attempt to legally distinguish the impact of foreign affairs from the matters of internal subversive activities is an exercise in futility." United States v. Hoffman, 334 F. Supp. 504, 506 (D.D.C. 1971). The futility of distinguishing between these two categories and the abuses which arise from such a categorization are illustrated in a set of cases, each dealing with the identical set of wiretaps of the Jewish Defense League. *Compare* United States v. Huss, 482 F.2d 38 (2d Cir. 1973) *and* United States v. Smilow, 472 F.2d 1193 (2d Cir. 1973) (wiretap categorized as surveillance involving the domestic aspects of national security) *with* Zweibon v. Mitchell, 363 F. Supp. 936 (D.D.C. 1973) (same tap categorized as surveillance involving foreign threats to national security), *rev'd and remanded*, 516 F.2d 594 (D.C. Cir. 1975)(en banc), *cert. denied*, 425 U.S. 944 (1976). Despite the fact that the distinction is not useful and generally confusing, several federal appellate courts have maintained the distinction between the domestic and foreign threats to national security. Two of the circuit courts have found the *Keith* analysis inapplicable to cases involving electronic surveillance for investigations involving foreign threats to the national security. In United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Court of Appeals for the Fifth Circuit concluded that the President had authority "over and above the Warrant Clause of the Fourth Amendment" to conduct foreign intelligence surveillance. *Id.* at 426. The following year, in United States v. Butenko, 494 F.2d 593 (3d Cir. 1974) (en banc), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1975), the Third Circuit held that prior approval of electronic surveillance was not necessary. Post hoc determination of the legality of the particular surveillance was adequate. *Id.* at 605. In contrast to the Third and Fifth Circuits, the Circuit Court of Appeals for the District of Columbia, in Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (en banc), *cert denied*, 425 U.S. 944 (1976), concluded that in the absence of exigent circumstances, all foreign intelligence surveillances must be conducted pursuant to a judicial warrant. *Id.* at 661.

IV. *ELECTRONIC SURVEILLANCE FOR INTELLIGENCE GATHERING*

The Foreign Intelligence Surveillance Act regulates all electronic surveillance conducted within the United States for intelligence gathering purposes.[77] The statute classifies these intelligence activities as positive foreign intelligence and counterintelligence investigations.[78] It further classifies the object of a FISA surveillance as a United States person, a foreign person or a foreign power.[79] The FISA standards of specificity and probable cause differ according to the nature of the investigation and its target.[80]

A. *Foreign Intelligence Investigations*

Pure foreign intelligence investigations may intentionally target only foreign powers,[81] and foreign persons acting as agents of a foreign power.[82] Such investigations aim solely at acquiring infor-

---

77. 50 U.S.C. § 1801 (Supp. II 1978).

78. 50 U.S.C. § 1801(e)(2)(B). The statute uses foreign intelligence to define both positive foreign intelligence relating to national defense and foreign affairs, and counterintelligence relating to clandestine intelligence activities, sabotage and international terrorism. However, the the legislative history defines information relating to national defense and foreign affairs as foreign intelligence. SENATE JUDICIARY REPORT, *supra* note 33, at 3978. Information relating to clandestine intelligence activities, sabotage, espionage and international terrorism is referred to as counterintelligence information. *Id.* at 3979.

79. 50 U.S.C. § 1801(a), (b), (c).

80. If the target of the surveillance is a "foreign power" or an "agent of a foreign power," who is not a "United States person," there is no requirement of evidence of criminality. 50 U.S.C. § 1804(a)(4)(A). However, before a "United States person" may be targeted for surveillance as an agent of a foreign power, the government must establish probable cause to believe that the person's activities "involve" or "may involve" a violation of federal criminal law. *Id.* § 1805(a)(3)(A); *id.* § 1801(b)(2).

81. A foreign power is defined as:

(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign based political organization, not substantially composed of United States persons; or
(6) an entity that is directed and controlled by a foreign government or governments.

50 U.S.C. § 1801(a)(1)-(6).

82. An agent of a foreign power is defined as:

(1) any person other than a United States person, who—

mation relating to the capabilities, activities and intentions of foreign powers, organizations or persons.[83] With the exception of emergency surveillance[84] and limited surveillance of an "official foreign power,"[85] all foreign intelligence must be authorized by a warrant issued by a judge of the special FISA court.[86]

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States . . . or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowlingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

50 U.S.C. § 1801(b).

83. Section 401 of title 50 defines foreign intelligence as information relating to the capabilities, intentions and activities of foreign powers, organizations or persons. 50 U.S.C. § 401. The definition of foreign intelligence contained in FISA is less explicit but in accord with § 401. FISA defines foreign intelligence as information with respect to a foreign power that relates to the national defense or security of United States or to the conduct of foreign affairs. 50 U.S.C. § 1801(e)(2).

84. If the Attorney General determines that the basis for a FISA warrant exists but because of an emergency the surveillance must be conducted before an application can be made, the Attorney General may authorize the surveillance and notify a FISA court judge that he is doing so. Emergency surveillance is permitted for 24 hours at the maximum. 50 U.S.C. § 1805(e).

85. The President may authorize the Attorney General to approve a FISA surveillance for up to one year without a court order. 50 U.S.C. § 1802(a)(1). The certification must state that the surveillance is targeted against a "means of communication used exclusively between or among" official foreign powers or against non-verbal "technical intelligence . . . from property or premises under the open and exclusive control of" an official foreign power. *Id.* § 1802(a)(1)(A)(i)-(ii).

86. *Id.* § 1803. The Chief Justice must publicly appoint seven district court judges from seven of the United States judicial circuits. *Id.* § 1803(a). The district judges will have exclusive jurisdiction to receive FISA applications and issue FISA warrants. *Id.* The Chief Justice must also designate an appeals court of three judges to hear government appeals if the district court denies the first order. *Id.* § 1803(b). If the appeals court affirms the lower court's denial of the FISA warrant, the government may petition the Supreme Court for a writ of certiorari. *Id.*

An application for a foreign intelligence warrant must meet the following technical requirements. It must identify the federal officer making the application, confirm the authority conferred upon the Attorney General by the President, and include the Attorney General's approval of the application.[87] In addition, the application must describe the means by which the surveillance is to be effected and whether physical entry is required.[88]

1. Specificity

The specificity requirements embodied in FISA closely parallel those of ordinary criminal investigations. The warrant application and order must specify the target of the surveillance, describe in detail the information sought and clarify the period of time during which the surveillance may be conducted.[89] The application must also include a certification by a designated official of the executive branch stating that the purpose of the intelligence is to obtain foreign intelligence information of a specific type which could not be obtained through normal investigative techniques.[90] However, in determining whether the stated purpose of the surveillance will be achieved, the magistrate cannot go beyond the facts described in the certification to evaluate the necessity of the surveillance.[91] The application must also specify minimization procedures which limit the interception, acquisition and dissemination of conversations of United States persons who are not the authorized targets of the surveillance.[92] If, for example, an American spoke with a foreign

---

87. *Id.* § 1804(a)(1)-(2).

88. *Id.* § 1804(a)(8). The warrant itself must also state the means by which the surveillance is to be effected and whether physical entry is required. *Id.* § 1805(b)(1)(D).

89. The applications for court orders are governed by § 1804. *Id.* § 1804(a)(3), (6), (10). Requirements for the issuance of the court orders are contained in § 1805. *Id.* § 1805(b)(1)(A)-(E).

90. *Id.* § 1804(a)(7)(A)-(D). S. REP. No. 701, 95th Cong., 1st Sess., *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3973, 4020-21 [hereinafter cited as SENATE INTELLIGENCE COMMITTEE REPORT].

91. In determining whether the articulated purpose will be achieved by the wiretapping, the magistrate cannot go beyond the certification to evaluate the necessity of the surveillance. The judge must take the reasons for the surveillance asserted in the application as true. SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3978.

92. Minimization procedures provide safeguards for the acquisition, retention and dissemination of information about a United States person only, whether they are the intentional target of the surveillance or whether they are overheard accidentally. 50 U.S.C. § 1801(h). Section 1801(h)(1) includes the most explicit definition of minimization. It requires that "specific procedures be adopted . . . that are reasonably designed in light of the purpose

official who was under surveillance for purposes unrelated to the conversation,[93] the minimization procedures would limit the recording of those communications in order to avoid unnecessary intrusion.[94]

The statute's requirement of particularity in the application and order comports with constitutional mandates.[95] In *Keith*, the Supreme Court held that the application and order for domestic security surveillance could be less specific as to the identity of its targets and the nature of the information sought than the application and order required for criminal investigations.[96] By incorporating specificity requirements followed in criminal investigations, Congress mandated a higher standard than the Court did in *Keith*.[97]

2. Probable Cause

In order for a foreign intelligence surveillance to be approved, the judge must find that the application establishes probable cause to believe that the target of the surveillance is a foreign power or a

---

and technique of the particular surveillance, to minimize the acquistion and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons . . . ." *Id.* § 1801(h)(1). Minimizing acquisition under FISA is equivalent to minimizing interception of the information. SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 4009. Minimizing retention requires the government to destroy the information where feasible, and render it essentially non-usuable if destruction is not feasible. *Id.* Minimizing dissemination involves restricting access to the information while its relevancy is determined. Once it is determined that the information is relevant, dissemination is restricted to agencies, and to those officials within an agency with a need to know. *Id.* at 4010. For an extensive analysis of minimization procedures, see Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Jobs*, 12 RUTGERS L.J. 405 (1981).

93. *See* SENATE COMMITTEE INTELLIGENCE REPORT, *supra* note 90, at 4008. In assessing the minimization effort, the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they could to avoid unnecessary intrusion." *Id.* at 4008-09.

94. *Id.* at 4009-10.

95. *See* U.S. CONST. amend. IV.

96. 407 U.S. at 322.

97. 388 U.S. 41. The Congress went beyond the *Keith* requirements to satisfy the standards established for surveillance in Berger v. New York, 388 U.S. 41 (1967). In *Berger*, the Court required that the warrant particularly describe the conversations or communications to be intercepted and not merely furnish the name or identity of persons whose conversations were to be seized. *Id.* at 55-59. *Berger* also held that the duration of surveillance needed to be explicitly stated in the application as well. *Id.* For a complete discussion of the *Berger* requirements, see *supra* notes 55-62 and accompanying text.

foreign person acting as an agent of a foreign power. FISA, in contrast to criminal investigations, does not require a showing of criminal activity before electronic surveillance can be used in a foreign intelligence investigation.[98]

The purpose of the probable cause standard in a criminal investigation is to ensure that government intrusions occur only when there are articulable facts and evidence indicating criminal activity.[99] However, where the government's need to intrude on individual privacy is based on national security intelligence gathering, the Supreme Court recognized in *Keith* that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[100]

Elimination of the probable cause showing of criminal activity for foreign intelligence surveillance comports with the Supreme Court's holding in *Keith*.[101] Although most often formulated in terms of an officer's probable cause to believe that criminal activity has or will take place, the standard may be modified when the government interest compels an intrusion based on something other than a reasonable belief of criminal activity.[102] The government undertakes electronic surveillance for foreign intelligence purposes with no suspicion that evidence of criminal activity may be discovered. Requiring the government agents to show that they have a

---

98. 50 U.S.C. § 1805(a)(3)(A).

99. *Berger*, 388 U.S. at 59.

100. *Keith*, 407 U.S. at 323. The gathering of information about foreign powers and their relations with this country serves an important purpose. *See, e.g.*, United States v. Clay, 430 F.2d 165, 172 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971). "Undoubtedly, certain kinds of foreign security information surpass in value to the Government any information about ordinary crime or domestic subversion: information concerning the likelihood of preemptive nuclear attack, for example, or the theft of vital military secrets." Note, *Foreign Security Surveillance*, 87 HARV. L. REV. 976, 984 (1974).

101. *Keith*, 407 U.S. at 322-23.

102. SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3978-79. Only a small percentage of intelligence investigations conducted against foreign powers are aimed at gathering evidence of criminal activity. Many intelligence professionals believe that criminal prosecutions should never be brought against hostile agents because doing so will only result in their replacement by other, unknown agents. Moreover, criminal proceedings will not only confirm the accuracy of classified information that has been passed to a foreign power, but may also reveal some of the material to a far wider audience. *See* SENATE SELECT COMM. ON INTELLIGENCE, 95TH CONG., 2D SESS., REPORT ON NATIONAL SECURITY SECURITY SECRETS AND THE ADMINISTRATION OF JUSTICE (Comm. Print 1978).

reasonable belief that criminal activity will be unearthed ignores the overriding purpose of the surveillance.

FISA provisions regulating surveillance in positive foreign intelligence investigations comport with fourth amendment guarantees. The statute requires prior approval by a district court judge based upon a description of specific targets and a showing of probable cause appropriate to the nature of the investigation.[103] The executive branch must take into account the characteristics of the foreign power, the identity of the foreign agent, the risks involved in the surveillance, and the relevance of the information sought to the fulfillment of proper intelligence needs.[104] FISA also requires prior judicial authorization and probable cause that the target is a foreign power or a foreign agent. The elimination of a probable cause showing of criminal activity is entirely appropriate in the foreign intelligence context where the use of the intercepted communications is for informational purposes only and where the absence of criminal activity is irrelevant to the purpose of the surveillance.

B. *Counterintelligence Investigations*

Counterintelligence investigations are distinct from foreign intelligence investigations in scope and purpose. Counterintelligence surveillances intentionally target "United States persons"[105] as well as foreign persons and powers. The purpose of such investigations is to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping and terrorists acts committed by or on behalf of foreign powers.[106]

Information gathering and law enforcement tend to merge in counterintelligence investigations, in contrast to foreign intelligence investigations which target information about the intentions and capabilities of foreign powers. FISA establishes procedures for the use of counterintelligence information in subsequent criminal prosecutions against United States citizens and resident aliens.[107] The intentional targeting of United States persons and the overlap with

---

103. 50 U.S.C. §§ 1804(a)(4), 1805(a)(3)(A).

104. SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3979.

105. 50 U.S.C. § 1801(i). A United States person is defined as a citizen of the United States, a legal resident alien, an unincorporated association substantially composed of citizens or resident aliens, or a United States corporation incorporated in this country. *Id.*

106. *Id.* § 1801(b)(2)(A)-(D).

107. *Id.* § 1806(a)-(j).

law enforcement requires a careful balancing of the government's need to gather intelligence information and its interest in preventing the commission of serious crimes against fourth amendment privacy interests.

All electronic surveillance conducted for counterintelligence investigations requires prior judicial authorization with the exception of emergency surveillance.[108] The technical requirements of the warrant procedure, such as disclosing the identity of the federal officer making the application and confirming the authority conferred by the President on the Attorney General, are identical to the technical procedures for foreign intelligence surveillances.[109] The application must also include a certificate stating that the purpose of the surveillance is to obtain counterintelligence information of a specific type that cannot be obtained by normal investigative techniques. In contrast to foreign intelligence investigations, the judge is authorized to evaluate the sufficiency of the factual statement to insure that it is not clearly erroneous.[110]

1. Specificity

As with foreign intelligence probes, the warrant application and order must specify the target of the surveillance, describe in detail the information sought and clarify the period of time during which the surveillance may be conducted.[111] These provisions of FISA fulfill the requirements of the fourth amendment, reaching beyond the standards for national security investigations established in *Keith* to satisfy the requirements for domestic criminal investigations in *Berger*.[112]

2. Probable Cause

A United States citizen or resident alien may be classified as a foreign agent and hence, intentionally targeted in a FISA surveil-

108. For a discussion of emergency surveillance, see *supra* note 84 and accompanying text.

109. *See supra* notes 87-88 and accompanying text.

110. If the target of the surveillance is a United States person, the judge may evaluate whether the statements in the certification are clearly erroneous. 50 U.S.C. § 1805(a)(5). The statements will relate to the foreign intelligence information and the need of the surveillance. *Id.* The judge can request further information from the applicant to make this determination. *Id.* § 1804(d).

111. The application procedures are governed by 50 U.S.C. § 1804(a)-(d). The warrant procedures are governed by 50 U.S.C. § 1805(a)-(d).

112. For a detailed discussion of the *Berger* requirements, see *supra* notes 55-62 and accompanying text.

lance, if he knowingly engages in various clandestine activities for a foreign power and if the activities "involve or may involve" a violation of criminal law.[113] FISA divides such activities into four categories: "clandestine intelligence gathering activities,"[114] "other clandestine activities,"[115] "sabotage, terrorism or preparation therefor,"[116] and aiding, abetting, or conspiring with an agent of a foreign power.[117] By establishing that the target's activities fall into one of these subdivisions, the government officer asserts the target is

---

113. 50 U.S.C. § 1801(b)(2).

114. The statute does not precisely define clandestine intelligence gathering. However, the application must show that the target is aware that he is acting for or on behalf of a foreign power's intelligence network. SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3990. In addition, the activities in question must be ones which involve or may involve a violation of the criminal law. *Id.* at 3990-91. Most often the laws in question will be the criminal espionage statutes: 18 U.S.C. §§ 792-799; *id.* § 951 (1976); 42 U.S.C. §§ 2272-2278(b) (1976); 50 U.S.C. § 855 (1976). *Id.* SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3990-91. The definition would also include the collection of industrial or technological information which, if disclosed to a hostile foreign nation might threaten national security. *Id.* In such situations the activity might violate federal law prohibiting the interstate transportation of stolen property pursuant to 18 U.S.C. § 2314 (1976). *Id.* SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3990-91. The activity may include covert actions designed by an intelligence service of a foreign power to influence events in this country. *Id.* But such covert actions must involve a present or imminent violation of federal criminal law such as 18 U.S.C. § 201 (1976) (bribery of public officials and witnesses). SENATE INTELLEGENCE COMMITTEE REPORT, *supra* note 90, at 3993-95.

115. 50 U.S.C. § 1801(b)(2)(B). Under this category, the person must not only have a knowing and substantial connection with the foreign power, but he must be acting pursuant to the direction of a foreign intelligence service or network. *See* SENATE INTELLIGENCE COMMITTEE REPORT, *supra* note 90, at 3993-95.

116. 50 U.S.C. § 1801(c), (d). The statute defines sabotage as "activities that involve a violation of chapter 105 of title 18, or would involve such a violation if committed against the United States." 50 U.S.C. 1801(d). For the activities that violate chapter 105 of title 18, see 18 U.S.C. §§ 2151-2157 (1976).

International terrorism is defined as activities that

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) appear to be intended—
  (A) to intimidate or coerce a civilian population;
  (B) to influence the policy of a government by intimidation or coercion; or
  (C) to affect the conduct of a government by assassination or kidnapping; and
(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate, or the locale in which their perpetrators operate or seek asylum.

50 U.S.C. § 1801(c)(3).

117. 50 U.S.C. § 1801(b)(2)(D). This section requires the government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding and abetting is engaged in the described activities as an agent

acting as an agent of a foreign power and is involved in activities which may violate the criminal law.

V. *ANALYSIS*

A. *Insufficiency of the Probable Cause Standard for Counterintelligence Investigations*

When surveillance is used solely to collect foreign intelligence or counterintelligence for informational purposes only, a showing of criminal activity is simply irrelevant. Accordingly, fourth amendment procedures may be adjusted to omit a showing of criminal activity usually required to justify a search.[118] Even where the government targets a United States citizen simply to obtain information concerning clandestine intelligence activities such as espionage, sabotage, kidnapping or assassination, FISA's "may involve" a criminal violation standard[119] gives sufficient fourth amendment protection when the information is not used in the prosecution of that citizen. However, when the purpose of the counterintelligence surveillance is to gather incriminating evidence, the government has a dual interest: preventing breaches in national security and prosecuting the individual. Thus, the appropriate balance between the government's interests and individual privacy lies nearer to routine criminal investigation standards. Accordingly, when the government institutes electronic surveillance of a United States person and intends to use evidence derived from that surveillance to prosecute him,[120] the government should be required to demonstrate that there is probable cause to believe the individual committed or is committing a specific crime.

---

of a foreign power and that his own conduct is assisting or furthering such activities. SENATE INTELLIGENCE COMMITTEE REPORT, *supra note* 90, at 3997.

118. In *Keith*, the Court recognized that domestic security surveillance may involve policy and practical considerations that differ from those involved in the surveillance of ordinary crime. 407 U.S. at 322. The exact targets of the surveillance are more difficult to identify than in ordinary criminal surveillance, and the focus of the surveillance may be less precise as well. *Id. See supra* notes 69-76 and accompanying text.

119. See *supra* notes 113-17 and accompanying text for a discussion of the "may involve" probable cause standard.

120. Intent to prosecute can be deduced from the timing and subsequent use of the information. The courts and law enforcement officials acknowledge that prosecutorial purpose is a common element in counterintelligence investigations. *See infra* notes 125-27.

B. Falvey: *Misuse of FISA*

The *Falvey* case is a clear example of the use of counterintelligence information as evidence in a criminal prosecution. The timing of the surveillance indicated prosecutorial intent. According to the Appellant's Brief, by December 23, 1980, a criminal investigation was directed at George Harrison.[121] It was not until April 3, 1981, however, that the government instituted electronic surveillance of defendants Falvey and Harrison pursuant to FISA.[122] The surveillance continued until June 19th or 20th of that same year when the defendants were arrested.[123] The government used the information intercepted as evidence to support the subsequent arrest and indictment of the defendants for offenses relating to the alleged purchase of arms and ammunition for shipment to the Irish Republican Army.[124]

The use of intelligence information for prosecutorial purposes is not unique to *Falvey*. Courts and law enforcement officials have indicated that intelligence investigations of United States citizens often involve prosecutorial purposes.[125] Indeed, the court in *United States v. Humphrey*[126] recognized that the government would rarely engage in electronic surveillance of a citizen without plans to prosecute at some time.[127]

The defendants argued that FISA was misused in their case because the government was primarily gathering incriminating evidence by the time the surveillance was instituted.[128] Accordingly, the defendants asserted that the government should therefore have complied with procedures of title III requiring a probable cause

---

121. Brief for Appellant at 31, United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) [hereinafter cited as Brief for Appellant].

122. 540 F. Supp. at 1308.

123. *Id.*

124. *Id.* at 1307.

125. United States v. Truong Dinh Hung, 629 F.2d 908, 916 n.5 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982) (statement of Griffin Bell, Att'y Gen: "Let me say that every one of these counterintelligence investigations involved . . . [or] involves crime in an incidental way. You never know when you might turn up with something you might want to prosecute.").

126. 456 F. Supp. 51 (E.D. Va. 1978).

127. *Id.* at 56.

128. *Id.* at 1313. In the brief, the appellants argued that FISA could not properly authorize seizure of the conversations where the purpose of the surveillance was criminal investigation. Accordingly, the requirements of and prohibitions contained in title III should prevail. Brief for the Appellant, *supra* note 121, at 33.

showing of a specific crime before the warrant was issued.[129] In dismissing the defendant's assertion, the court conceded that the argument was "not without appeal."[130]

The FISA probable cause standard for counterintelligence investigations of United States persons is insufficient when the purposes of the investigation include criminal prosecution. First, FISA's "may involve a criminal violation" standard permits surveillance based on the mere possibility of criminal activity, a standard that violates conventional criminal procedure.[131] Second, the statute does not indicate the particular offenses for which surveillance may be instituted. To regulate electronic surveillance for use in criminal prosecution, a statute should enumerate the specific crimes for which the surveillance may be used.

Standard fourth amendment law requires a probable cause showing of the commission or imminent commission of a particular offense.[132] By requiring that the government only establish conduct that "may involve a criminal violation,"[133] FISA's probable cause standard lacks both the specificity and imminence needed for the issuance of a warrant in a criminal investigation. The "may involve" standard permits surveillance upon a finding of probable cause to believe in the mere possibility rather than the existence of criminal activity. FISA requires that the government only assert generalized rather than specific criminal activity. Finally, the statute permits the government to allege that the criminal activity will take place in the indefinite rather than the immediate future. Thus, a FISA application and order not only require less information

---

129. 540 F. Supp. at 1313.

130. *Id.* In *Falvey*, the court recognized that several courts have ruled that, while warrantless electronic surveillance was permissible to obtain foreign intelligence information, in no case was it permitted as an excuse for, or with the intention of obtaining evidence of criminal activity. *Id.* at 1313. *See* United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982); United States v. Butenko, 494 F.2d 593 (3d Cir. 1974)(en banc), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1975). Although well aware in both *Truong* and *Butenko* of the importance of an executive informed of accurate information concerning national security, neither court was willing to forego traditional fourth amendment requirements of prior judicial authorization and probable cause when circumstances indicate that the government is indeed looking for incriminating evidence and not information vital to the defense of the nation. *Truong*, 629 F.2d at 912-13; *Butenko*, 494 F.2d at 606.

131. *See supra* notes 18-26, 53-68 and accompanying text.

132. *See supra* notes 18-26 and accompanying text.

133. 50 U.S.C. § 1801(b)(2)(B).

pertaining to the criminal activity involved, but also permit surveillance upon mere speculation that at some point in the indefinite future the individual may violate the law.

In addition to the vague phrasing of the probable cause standard, FISA does not contain a listing of specific criminal laws. FISA is not primarily a tool for prosecuting crime;[134] the statute merely explains the proper focus of foreign intelligence and counterintelligence investigations without specifying the related national security offenses. A statute authorizing electronic surveillance for prosecutorial purposes should be limited to a list of crimes for which surveillance is an appropriate investigative device.[135] If FISA is used to obtain evidence for a criminal prosecution, the government will be able to employ electronic surveillance without limiting its use to the investigation of particular, serious offenses.

Use of electronic surveillance to fulfill prosecutorial needs requires a probable cause showing of the commission or imminent commission of a specific crime listed in the statute because of the highly intrusive nature of electronic surveillance. In investigations not involving electronic surveillance, a warrant authorizes one single, overt entry and search of specific premises.[136] In contrast, electronic surveillance usually involves the interception of many conversations over an extensive period of time.[137] Electronic surveillance thus results in a general search of private conversations.[138]

The Supreme Court has recognized that investigative activities that are especially intrusive require a higher probable cause threshold. In *Camara v. Municipal Court*,[139] the Court noted that the

---

134. *See* SENATE JUDICIARY REPORT, *supra* note 33, at 3957.

135. *See infra* notes 144-54 and accompanying text.

136. C. FISHMAN, WIRETAPPING AND EAVESDROPPING § 6 (1978).

137. Although the minimization procedures apply to limit the interception of wire communications, electronic surveillance looms as the ultimate invasion of privacy. *Id.* § 7. When the police execute a warrant, they are looking for a particular item and must limit their search accordingly. *Id.* However, the government must necessarily listen to numerous conversations in their entirety in order to determine whether or not they are significant. *Id.* §§ 6-7. Under the authority of a single warrant, the government may conduct a series of surrepticious intrusions. *Id.*

138. *See Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the of the Select Comm. on Intelligence of the United States Senate*, 95th Cong., 2d Sess. 112 (1978). Even when a tap is placed on a person suspected of engaging in criminal activity, it offends the fourth amendment because it necessarily results in a general search of all private conversations, incriminating or not. *Id.*

139. 387 U.S. 523 (1967).

degree of justification for a search depended on the scope of the invasion.[140] In *Berger v. New York*,[141] Justice Stewart noted in his concurring opinion:

> I would hold that the affidavits on which the judicial order issued in this case did not constitute a showing of probable cause adequate to justify the authorizing order. The need for particularity and evidence of reliability in the showing required when judicial authorization is sought for the kind of electronic eavesdropping involved in this case is especially great. The standard of reasonableness embodied in the Fourth Amendment demands that the showing of justification match the degree of intrusion. By its very nature electronic eavesdropping for a 60-day period, even of a specified office, involves a broad invasion of constitutionally protected area. Only the most precise and rigorous standard of probable cause should justify an intrusion of this sort.[142]

Justice Stewart concluded that the evidence "was constitutionally insufficient to constitute probable cause to justify an intrusion of the scope and duration that was permitted in this case."[143]

C. *Title III: The Appropriate Standard*

When the government institutes electronic surveillance for prosecutorial purposes, it should meet the standards of title III for three reasons. First, Congress intended title III as a prosecutorial tool in contrast to FISA which was not primarily intended for use in criminal investigations.[144] Second, the scope of title III covers the use of electronic surveillance in investigations relating to espionage and sabotage.[145] Third, title III recognizes the extremely intrusive nature of electronic surveillance and requires a stringent standard of probable cause.[146]

Title III governs and was intended to govern the use of electronic surveillance to gather evidence for criminal prosecutions.[147]

---

140. *Id.* at 535-36.

141. 388 U.S. 41 (1967).

142. *Id.* at 69.

143. *Id.* at 70.

144. *See* TITLE III SENATE REPORT, *supra* note 47, at 2157-58; SENATE JUDICIARY REPORT, *supra* note 33, at 3957.

145. 18 U.S.C. § 2516(a) (1976).

146. *Id.* § 2518(3)(a)-(d). Before the judge will issue a warrant, he must be satisfied that "there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in § 2516 of this chapter." *Id.* § 2518(3)(a).

147. *Id.* §§ 2510-2520. *See* TITLE III SENATE REPORT, *supra* note 47, at 2157-58, 2185-88.

Section 2516 of title III enumerates the specific criminal violations that may necessitate the use of electronic surveillance as a part of the investigative process.[148] That substantial list includes: espionage, treason, kidnapping, presidential assassination, interstate transport of stolen property and sabotage. Thus, title III would have applied to the crimes suspected in the *Falvey* case[149] and to others that fall within the counterintelligence category.[150] FISA is concerned with threats to national security that emanate from a foreign power and implicate foreign persons and United States persons.[151] To the extent that FISA is used to obtain information for its informational value only, its standards are sufficient for surveillance of foreign citizens and powers, and United States persons.[152] Using FISA as a prosecutorial tool substitutes unintended and inadequate standards for the appropriate standards of title III. Thus, where the government intentionally targets United States persons to gather evidence for prosecution, the use of title III implements congressional intent and safeguards fourth amendment freedoms.[153] Furthermore, conducting electronic surveillance according to title III standards is appropriate because it recognizes the extremely intrusive nature of the surveillance. Title III does not permit the use of electronic surveillance unless the warrant application establishes probable cause to believe a specific offense listed in section 2516 of the act, has been, is being, or is about to be committed.[154]

The Supreme Court has sanctioned searches and seizures without a finding of probable cause in certain prescribed circumstances.[155] However, the rationale allowing those departures from

---

148. 18 U.S.C. § 2516.

149. Several provisions appear applicable: unlawful use of explosives, theft from interstate shipment, interstate transportation of stolen property, racketeer influenced and corrupt organizations or indeed, espionage or sabotage. *Id.* § 2516(1)(a), (c).

150. FISA counterintelligence investigations may involve the following violations under § 2516: espionage, treason, kidnapping, presidential assassination, sabotage, or bribery of public officials.

151. The definition of "foreign agent" indicates that the surveillance is to be directed at a foreign person who "acts in the United States as an officer or employee of a foreign power," or against any person who "acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States." 50 U.S.C. § 1801(b)(1) (Supp. II 1978). For a complete definition of a foreign power, see *supra* note 81.

152. *See supra* notes 99-103 and accompanying text.

153. For a discussion of the appropriate fourth amendment procedures for the use of electronic surveillance in criminal investigations, see *supra* notes 55-68, 144-52.

154. 18 U.S.C. § 2518(1)(b) (1976).

155. *See infra* notes 156-64 and accompanying text.

fourth amendment requirements is inappropriate when the government employs electronic surveillance in criminal investigations. The Court carved out exceptions for the permissible departure from a finding of probable cause in *Camara v. Municipal Court*[156] and *Terry v. Ohio*.[157] In *Camara* the Supreme Court sanctioned the use of area warrants for municipal authorities to conduct housing code investigations.[158] *Camara* approved the use of an area wide search warrant without proof of particular violation because the inspections were neither "personal in nature nor aimed at discovery of evidence of a crime."[159] They involved a rather limited invasion of the citizens' privacy and were justified because of the necessity of locating and abating hazards to public health.[160] In *Terry v. Ohio*,[161] the Court concluded that a police officer could conduct a "stop and frisk" based on something less than probable cause of criminal activity.[162] The Court held that a stop and frisk for weapons could take place if there was reasonable suspicion of criminal activity.[163] Use of a stop and frisk under circumstances admittedly short of probable cause was permitted because of the public interest in protecting the police officer and the limited scope of the search.[164]

The reasoning used in *Camara* and *Terry* is inapplicable to investigations that use electronic surveillance for counterintelligence purposes. Both cases involved limited invasions of privacy, either as part of a regulatory scheme or as a means of protecting the safety of the police officer. In contrast to those limited invasions, electronic surveillance is perhaps the most intrusive form of search and seizure. It is a more drastic interference than the searches and seizures conducted pursuant to a routine search warrant. Since no one can accurately predict when the incriminating evidence will be communicated, the surveillance must continue for a significant duration in contrast to the limited temporal intrusion granted by an ordinary search warrant for tangible things.

---

156. 387 U.S. 523 (1967).
157. 392 U.S. 1 (1968).
158. 387 U.S. at 535-36.
159. *Id.* at 537.
160. *Id.* at 533.
161. 392 U.S. (1968).
162. *Id.* at 27.
163. *Id.*
164. *Id.*

CONCLUSION

Surveillance for counterintelligence purposes inevitably and inextricably involves a policy of criminal law enforcement.[165] When the purpose of a counterintelligence investigation is to gather incriminating evidence for prosecution, the standard of probable cause must reflect the balance between the government's interest in prosecution and the individual's right to be free from unreasonable searches and seizures. The probable cause standard must reflect the preeminence of the individual's right to privacy in a criminal investigation which employs such intrusive measures as electronic surveillance. Thus, when the use of electronic surveillance is part of a counterintelligence investigation that intends criminal prosecution, the surveillance should be conducted in compliance with the standards and requirements of title III.

Christine A. Burke

---

165. Note, *The National Security Interest and Civil Liberties*, 85 HARV. L. REV. 1130, 1263-64 (1972). *See* United States v. Truong Dinh Hung, 629 F.2d 908, 916 n.5 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982); United States v. Humphrey, 456 F. Supp. 51, 56 (E.D. Va. 1978); *see also supra* notes 125-27 and accompanying text.