Vanderbilt Journal of Transnational Law

Volume 13
Issue 3 *Issue 4 - Fall 1980*

Article 2

1980

The Foreign Intelligence Surveillance Act of 1978

Kim L. Kelley

NOTES

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

TABLE OF CONTENTS

I. INTRODUCTION

In 1978 Congress enacted[1] and President Carter signed into law[2] the Foreign Intelligence Surveillance Act of 1978 [FISA].[3] The Act established the exclusive means by which foreign intelli-

1. S. 1566, 95th Cong., 2d Sess., 124 CONG. REC. 5994 (1978): (Apr. 20, considered and passed Senate); H.R. 1266, 95th Cong., 2d Sess., 124 CONG. REC. 9102 (1978): (Sept. 6, considered and passed House, amended); S. 1566, 95th Cong. 2d Sess., 124 CONG. REC. 14798 (1978): (Sept. 12, Senate disagreed with House amendments); S. 1566 95th Cong., 2d Sess., 124 CONG. REC. 17882 (1978): (Oct. 9, Senate agreed to conference report); H.R. 5708, 95th Cong., 2d Sess., 124 CONG. REC. 17882: (Oct. 12, House agreed to conference report).

2. Foreign Intelligence Surveillance Act of 1978, 14 WEEKLY COMP. OF PRES. DOC. 1853 (Oct. 25, 1978).

3. Foreign Intelligence Surveillance Act of 1978, § 101, 50 U.S.C.A. § 1801 (Supp. 1979).

gence surveillance within the United States could be conducted. It was a completion of the statutory schemata governing domestic electronic eavesdropping created via Title III of the Omnibus Crime Control Act of 1968 [hereinafter Title III].[4] Congress enacted the FISA to clarify and delineate the proper interface between the dictates of the fourth amendment and foreign intelligence eavesdropping within the country.[5] It was a legislative response to a void in this area of the law.[6]

Since enactment, the post-Watergate atmosphere which spawned impetus for FISA has given way to a mood more receptive to intelligence agencies and their activities.[7] Further, since the statute provides for mandatory periodic Congressional scrutiny of its implementation and ramifications,[8] it is important to review and analyze this Act.

This note will explore the constitutional background of the executive practice of conducting warrantless electronic foreign intelligence surveillance, and the legislative history of the Act. It will then examine the more important provisions of the statute, while concurrently comparing these to comparable terms of Title III. Constitutional issues or problems raised by the Act and its provisions will then be discussed. Finally, possible amendments to the Act will be explored.

II. CONSTITUTIONAL BACKGROUND

Originally, wiretapping escaped the fourth amendment[9] prohibition against "unreasonable searches and seizures" because normally such surveillance did not physically penetrate the constitutionally protected areas of either the house or the office.[10] This

4. Omnibus Crime Control Act of 1968, Title III § 80Z, 18 U.S.C. § 2510 (1976).

5. H.R. REP. No. 1283-Pt. 1, 95th Cong., 2d Sess. 20-22 (1978).

6. S. REP. No. 604-Pt. 1, 95th Cong., 2d Sess. 6-7, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS, 3909, 3908.

7. NEWSWEEK, Jan. 28, 1980, at 31.

8. 50 U.S.C.A. § 1808(b) (Supp. 1979).

9. U.S. CONST. amend. IV: "The right of the people to be secure in their person, 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."

10. Olmstead v. United States, 277 U.S. 438 (1928). The Supreme Court also reasoned that telephonic messages were intangibles, and as such the interception

doctrine, delimiting the scope of a search,[11] gave law enforcement officials carte blanche to engage in warrantless electronic wiretapping.[12] Congress sought to bridle this discretion by enacting Section 605 of the Federal Communications Act of 1934 [hereinafter Section 605].[13]

Section 605 ostensibly prohibited interception and dissemination of any communications received by nonconsensual wiretaps,[14] but it failed to specify the exclusionary rule as a remedy for violations perpetrated by government officials.[15] The Supreme Court, interpreting Section 605, held that the contents of communications seized in violation of the Act should be excluded from any federal criminal trial,[16] as should any evidence derived from a prohibited wiretap.[17]

In 1940, President Roosevelt interpreted Section 605 and the

---

of those intangibles did not constitute a search for fourth amendment purposes. *Id.* at 464.

11. W. LAFAVE, SEARCH AND SEIZURE § 2.1(a) (1978). The trespassory intrusion into a constitutionally protected area doctrine was firmly delineated in Clinton v. Virginia, 377 U.S. 158 (1964); Silverman v. United States, 365 U.S. 505 (1961); Goldman v. United States, 316 U.S. 129 (1940); Olmstead v. United States, 277 U.S. 464-65 (1928).

12. B. SEVERN, THE RIGHT TO PRIVACY 107 (1973). The Court, in Olmstead v. United States, did invite Congress to statutorily extend the exclusion remedy to wiretap evidence to be used in federal criminal trials. 277 U.S. 438, 465-66 (1928).

13. Federal Communications Act of 1934, § 605, 47 U.S.C. § 605 (1976), as amended by Pub. L. No. 90-351, § 803, 82 Stat. 223 (1968). The relevant provisions state that: "[N]o 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 . . . and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or 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 benefit or for the benefit of another not entitled thereto."

14. *Id.*

15. J. CARR, THE LAW OF ELECTRONIC SURVEILLANCE 7 (1977).

16. Nardone v. United States, 302 U.S. 379 (1937). The Supreme Court failed to extend the exclusionary rule to evidence obtained by state authorities in violation of Section 605, and used in state criminal trials. Schwartz v. Texas, 344 U.S. 199 (1952). This rule was expressly overturned by Lee v. Florida, 392 U.S. 378 (1967).

17. Nardoné v. United States, 308 U.S. 338 (1939).

resultant Supreme Court cases[18] as not prohibiting nonconsensual wiretaps for national defense purposes.[19] He authorized Attorney General Jackson to initiate this type of surveillance, but to limit investigations "insofar as possible to aliens."[20] Arguably, this directive did not address the propriety of trespassory buggings[21] for national defense purposes.[22] In 1946, Attorney General Clark's

---

18. Nardone v. United States, 302 U.S. 379 (1937).

19. Memorandum to Attorney General Jackson from President Roosevelt, May 12, 1940, reprinted in Zweibon v. Mitchell, 516 F.2d 594, 673-74 (D.C. Cir. 1975), *cert. denied,* 425 U.S. 944 (1976).

> I have agreed with the broad purpose of the Supreme Court decision relating to wire-tap in investigations. The court is undoubtably sound in regard to the use of evidence secured over tapped wires in the prosecution of citizens in criminal cases and is also right in its opinion that under ordinary and normal circumstances wire-tapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.
>
> However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.
>
> It is, of course, well known that certain other nations have been engaged in the organization of propaganda of so called "fifth columns" in other countries and in preparations for sabotage, as well as in actual sabotage.
>
> It is too late to do anything about it after sabotage, assassinations and "fifth column" activities are completed.
>
> You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information direct[ed] to the conversation or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies. You are further requested to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.

Two months earlier, Attorney General Robert H. Jackson announced a return to the policy of forbidding wiretapping by federal agents as mandated by Section 605. Donner, *Electronic Surveillance: The National Security Game,* 2 Summer 1975 CIV. LIB. REV. 15, 18-20.

20. *Id.*

21. Bugging as distinguished from wiretapping is not limited to the interception of a specific telephonic line or wire. A bug is a miniature electronic device which overhears, broadcasts, transmits, or records conversations or activities in the targeted area. Thus, bugs must be installed in the desired area and this usually requires physical trespass. J. CARR, *supra* note 15; Zweibon v. Mitchell, 516 F.2d 594, 617-18 (D.C. Cir. 1975); Donner, *supra* note 19, at 20. Trespassory bugging was not sanctioned by Section 605, but instead fell under the mandate of the Olmstead decision. Olmstead v. United States, 277 U.S. 438 (1928).

22. Zweibon v. Mitchell, 516 F.2d 594, 617-18 (D.C. Cir. 1975).

memorandum, as adopted by President Truman,[23] expanded the scope of permissible nonconsensual electronic surveillance to cases of suspected subversive activities against the government and to cases "affecting domestic security, or where human life is in jeopardy."[24] Furthermore, the distinction between wiretapping and trespassory bugging was blurred by the Truman directive which referred only to "special investigative measures."[25] The executive expansion of the Section 605 foreign security exception went unchecked by the legislature largely due to the pervasive fear of communist espionage and subversive activities.[26] At the same time, courts lacked the opportunity to review the Justice Department's actions as the surveillances were typified as investigatory, intragovernmental, and non-evidentiary in nature.[27]

Subsequent Attorney Generals adopted the expansive guidelines of Clark's memorandum and the ancillary bugging procedures developed by prior administrations.[28] President Johnson, however, circumscribed the executive power by authorizing warrantless electronic surveillance, upon approval by the Attorney General, for the collection of intelligence affecting the national security.[29] The cited authorities for the asserted executive powers

---

23. President Truman's Response to Attorney General Clark's Memorandum, July 17, 1947, *reprinted in* Zweibon v. Mitchell, 516 F.2d 594, 674 (D.C. Cir. 1975).

24. Memorandum to President Truman from Attorney General Clark, July 17, 1946, *reprinted in* Zweibon v. Mitchell, 516 F.2d 594, 674 (D.C. Cir. 1975).

25. *Id.* Prior precedent within the Justice Department allowed electronic bugging without prior approval of the Attorney General for national security purposes. Donner, *supra* note 19, at 20-21. Such bugging avoided prohibition under the Olmstead Doctrine, even though trespassory, because it was only used outside of court for the protection of the national security. Donner, *supra* note 19, at 24.

26. *See* Brownell, *The Public Security and Wire Tapping*, 39 CORN. L. Q. 201; Gasque, *Wiretapping: A History of Federal Legislation and Supreme Court Decisions*, 15 S.C.L. REV. 610-11 (1963).

27. Attorney General Jackson originally proffered that the Section 605 prohibition against interception and divulgence only precluded courtroom use of wiretap surveillance. Note, *The Fourth Amendment and Judicial Review of Foreign Intelligence Wiretapping; Zweibon v. Mitchell*, 45 GEO. WASH. L. REV. 59 (1976); Donner, *supra* note 19, at 19-20.

28. Donner, *supra* note 19, at 24; Brownell, *supra* note 16, at 199-200.

29. Memorandum for the Heads of Executive Department and Agencies from President Johnson, June 30, 1965, *reprinted in* Zweibon v. Mitchell, 516 F.2d 594, 674-75 (D.C. Cir. 1975). This policy was effectuated within the Justice Department by Memo No. 493, Memorandum to All United States Attorneys from

of domestic security and foreign intelligence surveillance were the inherent presidential power in the area of foreign relations,[30] the President's powers as commander-in-chief of the armed forces,[31] the power to protect the country from foreign encroachment,[32] the President's duty to protect the Constitution,[33] and the President's law enforcement duties.[34] The first three of these rationales clearly support executive authorization of foreign intelligence surveillance, while the remaining two have been used to justify domestic intelligence surveillance.[35]

The Supreme Court, in *Katz v. United States*,[36] overturned the

---

Ramsey Clark, Acting Attorney General, November 3, 1966, *reprinted in part in* Zweibon v. Mitchell, 516 F.2d 594, 675 (D.C. Cir. 1975).

30. The Constitution states that the President "shall receive Ambassadors and other public Ministers." U.S. CONST. art. II, § 3. This clause has been broadly interpreted, so as to make the President the sole mouthpiece in the area of foreign relations. LIBRARY OF CONGRESS CONGRESSIONAL RESEARCH SERVICE, THE CONSTITUTION OF THE UNITED STATES OF AMERICA: ANALYSIS AND INTERPRETATION 537 (7th ed. 1974). The Court emphatically declared:

> The President, both as Commander-in-Chief and as the nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret. Nor can the courts sit *in camera* in order to be taken into executive confidences. But even if courts could require full disclosure, the very nature of the executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution on the political department of government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.

Chicago & S. Air Lines, Inc. v. Waterman Steamship Corp., 333 U.S. 103, 111 (1948).

31. U.S. CONST. art. II, § 2, cl. 1; United States v. Butenko, 494 F.2d 593, 602-03 (3rd Cir. 1974), *cert. denied*, 415 U.S. 960 (1974); United States v. Clay, 430 F.2d 165 (5th Cir. 1970).

32. United States v. Brown, 484 F.2d 426 (5th Cir. 1973).

33. U.S. CONST. art. II, § 1 cl. 8; United States v. United States District Court, 407 U.S. 297, 310-11 (1971).

34. U.S. CONST. art. II, § 3.

35. Note, *Present and Proposed Standards for Foreign Intelligence Electronic Surveillance*, 71 N.W.U.L. REV. 112 n. 16 (1976).

36. 389 U.S. 347 (1967).

Olmstead trespass doctrine and found warrantless electronic surveillance an unreasonable search under the fourth amendment.[37] However, the court specifically reserved judgment on whether alternative safeguards might be substituted for the usual judicial warrant process in cases involving national security.[38] In 1968, Congress enacted Title III[39] which superceded Section 605. Title III generally requires law enforcement officers to obtain court authorization prior to the initiation of any wiretapping or bugging.[40] Yet, Congress exempted Presidential powers of eavesdropping in the areas of foreign intelligence, domestic security from attack of foreign powers, and domestic security from internal subversion from the purview of Title III.[41] Implicit within these exceptions and ostensibly corroborated in the legislative history[42] appeared to be a Congressional recognition of the then broad Presidential powers to engage in warrantless eavesdropping in the enumerated

37. *Id.* at 353.

38. *Id.* at 358 n. 23.

39. Omnibus Crime Control and Safe Street Act, Title III, Pub. L. No. 90-351, 82 Stat. 212 (Codified at 18 U.S.C. §§ 2510-2520) (1978).

40. 18 U.S.C. § 2516 (1976). Section 2516 lists the crimes for which eavesdropping to obtain information is permissible with the required court authorization as provided in 18 U.S.C. § 2518 (1976). This act does provide for warrantless interception of oral or wire communication where one party consents to such interception, 18 U.S.C. § 2511(2)(c) (1976), and in limited emergency situations 18 U.S.C. § 2518(7) (1976).

41. 18 U.S.C. § 2511(3) (1976) states:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter 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 the authority of the President in the exercise of the foregoing powers may be received in evidence at any trial hearing, and shall not be otherwise used or disclosed except as necessary to implement that power.

42. S. REP. No. 1097, 90th Cong., 2d Sess. *reprinted in* [1968] U.S. CODE CONG. & AD. NEWS 2112, 2153.

areas, limited only by internal executive safeguards.[43]

The Supreme Court rejected this interpretation in 1971 for domestic national security cases.[44] In *United States v. United States District Court*[45] [hereinafter *Keith*], the Court held that the fourth amendment requires prior judicial approval for the use of electronic surveillance for purely national security cases, and that Congress had left untouched Presidential power in cases involving the activities of a foreign power.[46] Yet, the Supreme Court failed to rule upon and specify the permissible scope of the asserted Presidential power of the use of warrantless electronic surveillance for the purpose of collecting foreign intelligence information.[47]

Therefore, a number of circuit courts of appeal ruled upon these questions when the issues were presented. The Fifth Circuit, in *United States v. Brown,* held that warrantless electronic surveillance for the purposes of obtaining foreign intelligence information was within the domain of permissible Presidential powers.[48] The Third Circuit, in *United States v. Butenko,* came to

---

43. Memorandum from President Johnson, *supra* note 19.

44. United States v. United States District Court, 407 U.S. 297, 303 (1971). The Court found that the wording of 18 U.S.C. § 2511(3) (1976) and its legislative history is merely a recognition of certain areas of asserted Presidential powers and it was not a legislative accession to such powers. The Court gave special attention to the Senate debate prior to that body's vote. *Id.* at 306-07; United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974).

45. 407 U.S. 297 (1971).

46. The Court limited its inquiry to cases where the Attorney General authorized surveillance "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the government." The Court took this language directly from the affidavit of the Attorney General in support of the surveillance. *Id.* at 308-09. The Court, balancing the governmental interest in protecting domestic security with the individual interest of privacy and freedom of expression, found warrantless domestic security surveillance unreasonable under the fourth amendment. A crucial factor in this determination is whether a warrant requirement would frustrate the government's legitimate efforts. *Id.* at 314-15. They found the fourth amendment mandates a warrant issued by a neutral and disinterested magistrate in such cases. *Id.* at 317.

47. *Id.*

48. United States v. Brown, 484 F.2d 418, 425-26 (5th Cir. 1973), *cert. denied,* 415 U.S. 960. The Fifth Circuit had previously held in 1970 that a warrantless wiretap authorized by the Attorney General was constitutionally permissible. United States v. Clay, 430 F.2d 165 (5th Cir. 1970), *cert. denied,* 394 U.S. 310.

the same conclusion,[49] but reasoned that the strong governmental interest in the continuous flow of information necessary for the operation of the executive's foreign policy apparatus outweighed the protection offered by the warrant procedure against possible abuse of Executive authority.[50] The Ninth Circuit also found that Executive warrantless electronic surveillance was constitutionally permissible, stating simply that "[f]oreign security wiretaps are a recognized exception to the general warrant requirement."[51] Yet, no circuit delineated clearly the parameters of this foreign intelligence exception to the warrant requirement.

Only one circuit, when availed of the opportunity to decide the issue, failed to sanction broad executive foreign intelligence powers. The Court of Appeals for the District of Columbia Circuit, in *Zweibon v. Mitchell*,[52] rejected the propriety of warrantless foreign intelligence electronic surveillance. It held that the fourth amendment required the issuance of judicial warrant prior to the wiretapping of a domestic organization which was "neither an agent of nor acting in collaboration with a foreign power,"[53] despite the government's claim that the wiretap was a legitimate exercise of the executive's foreign intelligence obligation.[54] The plurality opinion, authored by J. Skelly Wright,[55] rejected the government's contention that the subject matter of foreign intelligence surveillance preempted traditional fourth amendment anal-

---

49. United States v. Butenko, 494 F.2d 593 (3rd Cir. 1975), *cert. denied*, 419 U.S. 881.

50. *Id.* at 605. The court did not say that the Presidential powers in the area of foreign affairs pre-empted fourth amendment analysis. *Id.* at 603. Rather, the court balanced the benefit of prior judicial authorization against the burden of requiring such a procedure on the intelligence collection apparatus.

51. United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977), *cert. denied*, 434 U.S. 890 (1979).

52. 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

53. *Id.* at 613-14.

54. *Id.* at 614.

55. J. Skelly Wright authored the court's opinion in which Circuit Judges Leventhal and Robinson concurred and Chief Judge Bazelon concurred in part, but dissented to the court's mistake of law analysis for a civil suit brought for the violation of the plaintiff's fourth amendment rights. Circuit Judges McGowan and Robb concurred in the court's result, but felt that it could be reached on the basis of Title III, without necessitating the court's fourth amendment analysis. Judge Wilkey concurred only upon the constitutional grounds and dissented on the statutory (Title III) grounds. Judge MacKinnon filed a dissenting opinion.

ysis.[56] The court then stated that a warrantless search is presumed to be unreasonable, but such a presumption may be rebutted if the government has a legitimate need for foreign intelligence eavesdropping and the permissible goal of such surveillance would be frustrated by the warrant process.[57] Wright found that although there was a legitimate governmental need in acquiring foreign intelligence information, absent exigent circumstances, the obtaining of a warrant would not unduly interfere in the government's collection of the information.[58]

Chief Judge Bazelon concurred in this fourth amendment analysis, but dissented from Wright's contention that the Attorney General, as defendant of the civil suit, could effectively assert a mistake of law defense if he could show a good faith and reasonable belief that it was constitutional to order installation of the

---

56. The court examined two lines of authority for the government's argument; prior Presidential practice in the area of foreign intelligence eavesdropping and Supreme Court cases heralding broad Presidential powers in the conduct of foreign affairs. The court concluded that neither line supported the notion that the Executive's power in this area is exempt from judicial review or that such acts are outside the scope of constitutional limitations. Wright reasoned that since Roosevelt, Truman, and Johnson's memoranda were made when the *Olmstead* trespass doctrine was viable and each directive only related to wiretapping (which was normally outside the scope of the *Olmstead* doctrine), then all three Presidential orders failed to alter the fourth amendment warrant requirement. *Id.* at 617-18. The opinion then divided the Supreme Court cases into "three overlapping subclasses: (1) cases finding that our political relations with foreign governments are non-justiciable; (2) cases recognizing that the President has certain 'inherent' powers in the field of foreign affairs which are not dependent upon Congressional authorization; and (3) cases recognizing an evidentiary privilege shielding information pertaining to military or diplomatic secrets from disclosure in open court." *Id.* at 619. Wright went on to distinguish or show the inapplicability of each of these subclasses to the issue of foreign intelligence surveillance. *Id.* at 620-27.

57. *Id.* at 632-33.

58. *Id.* at 641-51. The court discussed five factors which might justify abrogation of the warrant requirement for foreign intelligence eavesdropping: (1) judicial competence; (2) the danger of security leaks which might endanger the lives of the informants and which might seriously harm the national security; (3) the fact that such surveillance is of the ongoing intelligence-gathering type and that, since criminal prosecutions are less likely, fourth amendment protections are not as essential as in a normal criminal context; (4) the possibility that the delay involved in the warrant procedure might result in substantial harm to the national security; and (5) the fact that the administrative burden on the courts or the executive branch which would result from such a requirement would be enormous.

warrantless wiretaps involved in the case.[59] Both Robinson and Leventhal joined in the entire Wright opinion.[60]

Judge McGowan concurred in the judgment, but felt that the result could be reached without necessitating Wright's fourth amendment analysis.[61] He found that the wiretap surveillance of sixteen members of the Jewish Defense League[62] did not fit within the Congressional disclaimer to limit any possible Presidential eavesdropping powers of Title III, 18 U.S.C. § 2511(3),[63] and thus the surveillance fell within the purview of Title III.[64] He urged that the statute's exemption of surveillance "necessary to protect the Nation against . . . hostile acts of a foreign power,"[65] only became operative if the surveillance was "directed against agents of or collaborators with the foreign powers whose hostile acts are feared."[66] This was not the situation in the instant case because the only contemplated hostile act of a foreign power was the possible reaction of the U.S.S.R. to the Jewish Defense League's actions.[67] Judge Robb filed a similar concurring opinion which found that the warrantless eavesdropping related to possible domestic crimes enumerated in Title III and thus was violative of the statute.[68]

Judge Wilkey agreed with the plurality opinion that the eavesdropping fell within the meaning of the 18 U.S.C. § 2511(3) disclaimers for foreign affairs or domestic security surveillance.[69]

---

59. *Id.* at 675-81.

60. *Id.* at 601.

61. *Id.* at 681.

62. Plaintiff-appellants were sixteen members of the Jewish Defense League (J.D.L.), a domestic group, whose focus of activity was aimed at international affairs. They were especially concerned with Russia's restrictive emigration policy concerning Soviet Jewry. The government maintained that since the J.D.L. held demonstrations and were implicated in acts of violence aimed at Soviet officials in the United States, surveillance of this group was within "the Presidential authority relating to the nation's foreign affairs and was deemed essential to protecting the nation and its citizens from hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States." *Id.* at 607.

63. *Id.* at 683-85.

64. *Id.* at 686.

65. 18 U.S.C. § 2511(3) (1976).

66. Zweibon v. Mitchell, 516 F.2d 594, 684 (D.C. Cir. 1975).

67. *Id.* at 685-86.

68. *Id.* at 688.

69. *Id.* at 689.

Yet, he maintained that the surveillance was only subject to constitutional strictures; thus via *Keith* Title III procedural requirements and damages are not necessarily applicable.[70] He then went on to reject the government's claim that since the surveillance involved a foreign power "the reasonableness standard of the fourth amendment is met without a warrant," as an overly broad interpretation of a possible foreign affairs exemption.[71] He reasoned that any fourth amendment warrant requirement exemption must be based upon overriding governmental interests and that the typical interests proffered to support a foreign affairs exemption were of attenuated import when the subjects of the surveillance were not foreign agents or collaborators.[72] In concluding this line of reasoning, Wilkey distinguished four catagories of surveillance: (1) surveillance for ordinary criminal cases directly governed by Title III; (2) domestic security wiretaps which the Supreme Court in *Keith* found to be outside of the scope of Title III, but constitutionally warranting prior judicial approval; (3) surveillance "whose primary purpose is to protect our relations with other countries" which also constitutionally requires prior judicial approval; and (4) surveillance directed at foreign agents and collaborators which might justify dispensing with prior judicial approval.[73]

Judge MacKinnon agreed with Wilkey's opinion except he found a probable cause determination inapplicable to foreign intelligence surveillance whose purpose was not to collect information relevant to a criminal prosecution.[74] Thus, six justices appeared to reach the conclusion that the fourth amendment mandates some sort of prior judicial oversight for foreign intelligence electronic surveillance when the target is neither a foreign agent nor a collaborator. The Supreme Court has yet to rule on the interface of the fourth amendment warrant requirement with electronic surveillance for foreign intelligence collection purposes within the United States.

---

70. *Id.* at 689-99.

71. Wilkey stated: "Weighing the Government's rationale for a sweeping 'foreign affairs' exemption to the warrant requirement against the inroads such an exemption would make on important Fourth and First Amendment values, I must first conclude that a waiver of such breadth is unjustified." *Id.* at 700.

72. *Id.* at 701-05.

73. *Id.* at 705.

74. *Id.* at 706-07.

III. LEGISLATIVE HISTORY

The unearthing of Executive abuse of warrantless electronic surveillances in the name of national security during the Watergate investigations catalyzed interest in circumscribing the Executive's power in this area.[75] This resulted in numerous and varied congressional hearings on the abuse under the guise of foreign intelligence surveillance[76] and no less than four legislative attempts prior to 1977 to bridle the asserted Executive power.[77] Senator Church's Senate Select Committee to Study Government Operations with Respect to Intelligence Activities was particularly vocal in its criticism of intelligence agencies' abuse of surveillance authority.[78] It reported frequent warrantless wiretappings and buggings of United States citizens who were neither engaged in criminal activities, a threat to national security, nor reasonable targets for the gathering of foreign intelligence information.[79] The Committee cited the vague standards governing electronic surveillance and the failure of Congress to act in the area of foreign intelligence surveillance as contributing factors to the problem.[80] Yet, all of these investigations also realized the countervailing interest

---

75. S. REP. No. 604-Pt. 1, 95th Cong., 1st Sess. 7, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3908.

76. *Hearings on S. 3197 Before the Subcommittee on Intelligence and the Rights of Americans of the Senate Select Committee on Intelligence, Electronic Surveillance within the United States for Foreign Intelligence Purposes,* 94th Cong. 2d Sess. (1976); *Hearings before the Subcommittee on Criminal Laws and Procedure of the Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1976,* 94th Cong., 1st Sess. (1975); *Subcommittee on Surveillance of the Senate Committee on Foreign Relations and the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, Warrantless Wiretapping and Electronic Surveillance,* 94th Cong., 1st Sess. (1975); *Joint Hearings before the Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, Warrantless Wiretapping and Electronic Surveillance,* 93rd Cong., 2d Sess. (1974).

77. S. 3917, Foreign Intelligence Surveillance Act of 1976, 94th Cong., 2d Sess. (1976); S. 743, National Security Surveillance Act of 1975, 94th Cong., 1st Sess. (1975); S. 4062, Freedom from Surveillance Act of 1974, 93rd Cong., 2d Sess. (1974); S. 2820, Surveillance Practices and Procedures Act of 1973, 93rd Cong., 1st Sess. (1973).

78. *See,* SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE, ANNUAL REPORT TO THE SENATE, 95th Cong., 1st Sess., 12-16 (committee print, 1977).

79. S. REP. No. 604-Pt. 1 *supra* note 75, at 7-8.

80. *Id.* at 8.

of the government is assembling adequate intelligence to protect the nation.[81]

In an attempt to balance this countervailing interest and provide a statutory procedure for judicial authorization of electronic foreign intelligence eavesdropping, Senator Edward M. Kennedy introduced Senate bill number 1566 on May 18, 1977.[82] According to the Senate Select Committee on Intelligence Report on the Foreign Intelligence Surveillance Act of 1978, "[t]he basic premise of the bill is that a court order for foreign intelligence electronic surveillance can be devised that is consistent with the 'reasonable search' requirement of the Fourth Amendment."[83] Further, Congress views the statute as a legislative clarification and advancement of constitutional law in an area of uneven and inconclusive judicial development.[84]

The statute provided for mandatory procedure for the Attorney General to attain court approval for electronic foreign intelligence information collection in the United States, except for surveillance of communications of a foreign power not likely to involve a United States person.[85] The bill was a continuation and amendment of Senate bill number 3917 [hereinafter S. 3917], the Foreign Intelligence Surveillance Act of 1976, which was also introduced by Senator Kennedy.[86] S.3917 received bipartisan Congressional support, the endorsement of two Senate commitees,[87] and an endorsement by the Ford administration, but it failed to reach the floor of the Senate before the Ninety-fourth Congress adjourned.[88] It appears likely that many legislators were reluctant to enact a bill which reserved a residuum of untouched Presidential power in the area and which would probably result in

---

81. *Id.* at 9.

82. *Id.*

83. S. REP. No. 701, 95th Cong., 2d Sess. 9, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS 3904, 3977.

84. S. REP. No. 604-Pt. 1, *supra* note 75, at 15.

85. 50 U.S.C.A. § 1802 (b) (Supp. 1979).

86. S. 3197 Foreign Intelligence Surveillance Act of 1976, 94th Cong., 2d Sess. (1976).

87. Both the Senate Subcommittee on Criminal Laws and Procedure of the Committee on the Judiciary and the Senate Select Committee on Intelligence held hearings on the Foreign Intelligence Surveillance Act of 1976.

88. *See, Foreign Intelligence Surveillance Act of 1978; Hearings on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence,* 95th Cong., 2d Sess. 2.

further confusion about the future exercise of this residuum power.

Unlike its precursor, Senate bill number 1566, [hereinafter S. 1566] required warrant authorization for electronic eavesdropping of any international communications of a United States citizen located within the country. Second, S. 1566 required court review of the Attorney General's certification of the necessity of eavesdropping on a United States citizen to acquire the desired foreign intelligence information. Finally, it went beyond the scope of S. 3917 in that it asserted that its procedures were the exclusive mechanism by which foreign intelligence surveillance could be conducted within the country.[89] These amendments result from some Senators' reservations voiced during the committee hearings on S. 3917 and also represented subsequent consultation with Justice Department officials.[90]

Like its predecessor, the 1978 act received broad-based support, including endorsements by Attorney General Griffin Bell and President Carter.[91] Hearings on the Act were held by the Senate Subcommittee on Criminal Laws and Procedure of the Judiciary Committee,[92] the Senate Subcommittee on Intelligence and the Rights of Americans of the Intelligence Committee,[93] and the House Subcommittee on Legislation of the Intelligence Committee.[94] These hearings yielded alterations, the most important of which was the redrafting of the definition of "agent of a foreign power" to lessen the possibility of a warrant issuing against a citizen or resident alien without probable cause of involvement in a criminal activity.[95]

In addition to Senator Kennedy's bill, introduced by Mr.

---

89. *Id.* at 2-3.

90. *Id.* at 2.

91. *Id.* at 12-13. (endorsement of Attorney General Griffin B. Bell and quoting President Carter's endorsement); *See also* S. REP. No. 604-Pt. 1, *supra* note 75, at 4.

92. *Foreign Intelligence Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. of the Judiciary*, 95th Cong., 1st Sess. (1977).

93. *Hearings on S. 1566, supra* note 89.

94. *Foreign Intelligence Electronic Surveillance: Hearing on H.R. 5794, H.R. 9754, H.R. 7308, and H.R. 5632 Before the House Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess. (1977).

95. S. REP. No. 604-Pt. 1, *supra* note 75, at 4.

Rodino[96] in the House and bearing the bill number of H.R. 7038, three other proposals were before the House subcommittee. The Railsback and Kastenmeir bills also provided for the safeguard of a prior judicial warrant in foreign security cases.[97] The Railsback bill was very similar to FISA.[98] The Kastenmeir bill provided that a warrant could issue upon a mere showing that there was reason to believe foreign intelligence information could be obtained, but it greatly restricted the scope of activity that the court warrant could authorize.[99] The McClory bill sought only a three step internal executive control procedure for authorization of electronic surveillance to obtain foreign intelligence information.[100] After comparing the alternative proposals and evaluating the testimony of eighteen witnesses, the House Permanent Select Committee on Intelligence recommended passage of S. 1566.[101] The Senate considered and passed this bill on April 20, 1978.[102] The House passed its own version on September 7, 1978 and sent its amendments to the Senate.[103] After the House conference report was filed, both bodies passed the amended bill and President Carter

---

96. *Hearings on H.R. 5794, H.R. 9745, H.R. 7308 and H.R. 5632, supra* note 95, at 2 (Railsback bill was H.R. 5794 and Kastenmeir bill was H.R. 5632).

97. *Id.*

98. *Id.*

99. *Id.* at 2, 67.

100. *Id.* at 275 (Appendix B reprint of H.R. 9745). McClory felt that since different circumstances necessitated foreign intelligence surveillance than necessitated searches and seizures for strictly law enforcement purposes prior judicial authorization was inappropriate. He felt that certification by the President, the Attorney General, and the Assistant to the President for National Security Affairs both protected individuals from abuse of this power and satisfied the mandates of the fourth amendment. The certificate had to specify among other things: (1) the target of the electronic surveillance; (2) the facts and circumstances which support the belief that foreign intelligence information would be obtained; (3) the minimization procedures; (4) if the target were a foreign power, the nature of the information sought; (5) statements that foreign intelligence information is being sought; (6) other procedures could be fruitless; (7) the period of the proposed surveillance; and (8) the means by which the surveillance was to be effectuated. *Id.* at 3 and 272-75.

101. H.R. REP. No. 1283-Pt. 1, 95th Cong. 2d Sess. 1 (1978).

102. 124 CONG. REC. S5994-6019 (daily ed. April 20, 1978).

103. 124 CONG. REC. H9237-9273 (daily ed. Sept. 7, 1978).

signed it into law.[104]

IV. The Foreign Intelligence Surveillance Act of 1978

A. *Scope of the Act*

The boundaries of FISA are primarily delimited by the statute's definitions of foreign intelligence information,[105] electronic surveillance,[106] foreign power,[107] and agent of a foreign power.[108] A prerequisite to the Act's applicability is that either the sender, the intended recipient, or both must be located within the United States.[109] Communications wholly outside the United States, even though they involve United States citizens, are not covered by FISA or Title III,[110] and international communications of a citizen within the country are covered only if the interception was made by intentionally targeting the person.[111] The interception of the communication content[112] must be made by an electronic, mechanical, or other surveillance device.[113] One party consensual eavesdropping is excluded from the statute's purview.[114]

FISA regulates only surveillance that falls within one of the five partially overlapping categories that define activities or areas the knowledge of which constitutes foreign intelligence information. These categories include information regarding: (1) foreign military capabilities or actions which would directly affect the national security; (2) sabotage or international terrorism by a foreign power or its agents; (3) spying by foreign intelligence networks; (4) national defense or the security of the United

---

104. Foreign Intelligence Surveillance Act of 1978, 14 Weekly Comp. of Pres. Doc. 1853 (Oct. 25, 1978).

105. 50 U.S.C.A. § 1801(e) (Supp. 1979).

106. 50 U.S.C.A. §1801(f) (Supp. 1979).

107. 50 U.S.C.A. §1801(a) (Supp. 1979).

108. 50 U.S.C.A. §1801(b) (Supp. 1979).

109. 50 U.S.C.A. §1801 (f)(1)-(4) (Supp. 1979); S. Rep. No. 701, *supra* note 84, at 33-38.

110. Title III regulates primarily domestic electronic surveillance and prior to 1978 it specifically excepted foreign intelligence surveillance. FISA is primarily an addendum to the coverage of Title III. Congress provided conforming amendments to Chapter 119 of Title 18, United States Code as part of FISA to assure the integration of the two statutes.

111. 50 U.S.C.A. §1801 (f) (1) (Supp. 1979).

112. Pen registers are not within the purview of this statute.

113. 50 U.S.C.A. §1801 (f) (1)-(4) (Supp. 1979).

114. 50 U.S.C.A. §1801(e) (2)-(4) (Supp. 1979).

States; and (5) conduct of United States foreign policy.[115] Inclusion in this genre, and thus within the Act's provisions, further depends on whether the information sought concerns a United States person (a citizen or legal alien) or not.[116] If it does, then the information must not merely relate to one of the five categories of foreign intelligence information, but rather it must be *necessary* to the collection of information specified by the category.[117] Since this statute in conjunction with Title III represents a complete statutory interpretation of the parameters of permissible electronic eavesdropping within the country,[118] it provides a stricter standard of fourth amendment review for foreign intelligence surveillance involving a United States person than a non-United States person.

Finally, the target of the surveillance covered in the Act must be believed to be a foreign power or an agent of a foreign power.[119] The drafters of the statute broadly defined foreign power to include: (1) an official foreign government and its components; (2) a foreign faction (not officially recognized) not substantially composed of United States persons; (3) entities acknowledged to be controlled by a foreign government; (4) a foreign based terrorist group; (5) a foreign based group, not substantially composed of United States persons; and (6) a commercial entity directed and controlled by a foreign government, but not merely an enterprise that is under a contractual duty to a foreign government.[120] The common denominator of these six categories is that control of the entity must be with a group of non-United States persons.

The target of the statute's surveillance may also be an agent of a foreign power. This definition includes officers and employees of a foreign power who are not United States persons.[121] There is a legislative presumption that non-resident aliens working for a foreign power in this country are likely sources of foreign intelligence information.[122] The definition also includes non-United States persons who act for foreign powers engaged in clandestine

115. 50 U.S.C.A. §1801 (e) (1)-(2) (Supp. 1979).
116. 50 U.S.C.A. §1801 (i) (Supp. 1979).
117. 50 U.S.C.A. §1801 (e) (1)-(2) (Supp. 1979).
118. S. REP. No. 701, *supra* note 83, at 5.
119. 50 U.S.C.A. §1804 (a) (4) (b) (Supp. 1979).
120. 50 U.S.C.A. §1801 (a) (1)-(6) (Supp. 1979).
121. 50 U.S.C.A. §1801 (b) (1) (A) (Supp. 1979).
122. S. REP. No. 701, *supra* note 83, at 19.

intelligence collection operations of the United States, "when the circumstances of such person's presence in the United States, indicates that such person may engage in such activities in the United States."[123] Thus, a foreign visitor acting for a foreign government or employed by a foreign government may be subjected to surveillance under FISA without showing that he has or may commit any criminal offense.[124] The definition also includes any person who knowingly engages in activities constituting spying against the United States interest, sabotage,[125] international terrorism and preparation for such terrorism, or aiding and abetting any such activities.[126] Thus, for a citizen or resident alien to be the target of permissible FISA surveillance, there will generally be suspicion of the violation of a criminal statute. This is akin to the protection afforded all persons subject to surveillance pursuant to Title III.[127] Title III requires a full and a complete statement of the facts and circumstances demonstrating probable cause that a listed offense has, is, or is about to be committed.[128]

B. *§ 1802 (a) Limited Executive Authorized Electronic Surveillance*

FISA permits the executive branch to engage in domestic warrantless eavesdropping for the purpose of assembling foreign intelligence information only in extremely limited circumstances and only after scrutiny of systematic internal checks and limitations. Upon an intelligence agency's application for § 1802 (a) surveillance, the Attorney General must ascertain and certify in a sworn document that three conditions exist.[129] First, the target of the eavesdropping must be either a "means of communication used exclusively between or among foreign powers" or technical non-vocal data emanating from property exclusively controlled by a foreign power.[130] Second, that no substantial likelihood of acquisition of a communication to which a United States person is a

123. 50 U.S.C.A. §1801 (b) (1) (B) (Supp. 1979).
124. S. REP. No. 702, *supra* note 83, at 20.
125. Sabotage is defined by reference to 18 U.S.C., Chapter 105. 50 U.S.C.A. § 1801 (d) (Supp. 1979).
126. 50 U.S.C.A. § 1801 (c) (Supp. 1979).
127. 18 U.S.C. § 2516 (1) (a) (1976).
128. 18 U.S.C. § 2518 (1) (b) (1976).
129. 50 U.S.C.A. § 1802 (a) (1) (Supp. 1979).
130. 50 U.S.C.A. § 1802 (a) (1) (A) (i)-(ii) (Supp. 1979).

party exists.[131] Last, that the proposed surveillance fits within previously adopted and Congressionally ratified[132] procedures which assure minimal acquisition, retention, and dissemination of private information concerning United States persons.[133] This written certification is sealed and submitted to a designated court and is opened only upon challenge of the legality of the surveillance or if the government later applies for a warrant for the same surveillance.[134] Bugging under this section is limited in duration to one year.[135] Title III does not have a similar statutorily prescribed procedure for executive issued surveillance without judicial review.

C. *Foreign Intelligence Surveillance Pursuant to Court Authorization, § 1802 (b) - § 1805 (d)*

FISA institutes a system of internal (executive) and external (judicial) checks upon the implementation of permissible foreign intelligence electronic surveillance. In some respects the internal procedural protections afforded United States citizens and resident aliens and the resultant administrative encumbrances in attaining judicial authorization are greater than those of Title III. FISA surveillance requires review by a presenting officer, the Attorney General, and the Assistant to the President for National Security Affairs.[136] An initial control in the process requires that a federal officer, in writing and upon his oath, submit an application for an order allowing eavesdropping for the purpose of collecting foreign intelligence information.[137] If the officer cannot swear to his personal knowledge of any of the listed criteria in the application, he must obtain an affidavit of an investigating or other officer who is cognizant of the basis of those assertions or of the assertions of the informer.[138]

---

131. 50 U.S.C.A. § 1802 (a) (1) (B) (Supp. 1979).

132. The act provides that the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall review a report from the Attorney General on the compliance with and effectuation of minimization procedures and further supply notification of any changes in such procedure. 50 U.S.C.A. § 1802 (a) (1) (Supp. 1979).

133. 50 U.S.C.A. § 1801 (h) (Supp. 1979).

134. 50 U.S.C.A. § 1802 (a) (3) (Supp. 1979).

135. 50 U.S.C.A. § 1802 (a) (1) (Supp. 1979).

136. 50 U.S.C.A. § 1804 (a) and (a) (7) (Supp. 1979).

137. 50 U.S.C.A. § 1804 (a) (Supp. 1979).

138. S. REP. No. 701 *supra* note 82, at 49. If informers are to be used the

Every application for authorization of foreign intelligence surveillance must contain an averment to or proof of the following: (1) the identity of the presenting federal officer;[139] (2) evidence of the authority of the Attorney General granted by the President and approval of the application pursuant to this authority;[140] (3) the identity of the targeted person, if known, or a description of the targeted person, if known, or a description of the targeted entity;[141] (4) the facts which support the reasonable belief that the target of the surveillance is either a foreign power or an agent of a foreign power and that the facilities or premises to be invaded are likely to be used by such a defined person or entity;[142] (5) "a statement of the proposed minimization procedures;"[143] (6) a report of any prior application for surveillance of the targeted person, facilities, or premises;[144] and (7) a statement of the expected or required duration of the bugging.[145] Every application must also contain an appended certification by the Assistant to the President for National Security Affairs which attests to the fact that: (a) he believes that the information sought is foreign intelligence information; (b) the actual purpose of the electronic eavesdropping is to get such information; (c) other surveillance techniques would be unfruitful; and (d) the information sought fits one of the five categories deliniating foreign intelligence surveillance and the certification designates the category.[146]

These are the requisite criteria for an application for judicial ratification of eavesdropping on a foreign government where the targeted facility is in the United States and controlled by the foreign government.[147] Each of these application criteria has a counterpart in Title III except that there is nothing akin to the

---

Spinelli v. United States, 394 U.S. 410 (1969) standards of proving the basis of the informer's knowledge and his reliability must be demonstrated.

139. 50 U.S.C.A. § 1804 (a) (1) (Supp. 1979).

140. 50 U.S.C.A. § 1804 (a) (2) (Supp. 1979).

141. 50 U.S.C.A. § 1804 (a) (3) (Supp. 1979).

142. 50 U.S.C.A. § 1804 (a) (4) (Supp. 1979).

143. 50 U.S.C.A. § 1804 (a) (9) (Supp. 1979).

144. *Id.*

145. 50 U.S.C.A. § 1804 (a) (10) (Supp. 1979).

146. 50 U.S.C.A. § 1804 (a) (7) (A)-(D) (Supp. 1979). The third criterion is met either by showing that prior non electronic surveillance techniques proved useless or that under the circumstances one would expect such methods to prove fruitless.

147. 50 U.S.C.A. § 1804 (b) (Supp. 1979).

auxilliary screening provided by the detailed certification of the Presidential Assistant,[148] nor is there a recitation of the Attorney General's authority in Title III.[149] Although the minimization procedure generally parallels 18 U.S.C. § 2518 (5) of Title III in that both are designed to diminish unnecessary acquisition of private and non-utilitarian overheard information and dissemination, the procedures under FISA are more detailed, only apply to United States persons, and must be specified in the application.[150]

If the electronic eavesdropping is not targeted at a foreign government facility, then the application must also include: "A detailed description of the nature of the information sought or the activities to be subject to the surveillance";[151] a statement of how the surveillance is to be effectuated and whether or not physical entry upon the targeted premises to install an electronic device is required;[152] and a statement of when multiple eavesdropping devices are to be used, a cataloging of each device, its proposed coverage, and individualized minimization procedures.[153] Finally, the certification by the Presidential Assistant must also include a statement which justifies the conclusions that the targeted information is foreign intelligence in character and that such information could not be reasonably obtained by alternative methods.[154] Title III does not require the applicant to divulge how the surveillance will be effectuated nor does it mandate a cataloging for

148. Although Title III does not have a secondary Executive review procedure analogous to the FISA certification procedure, it does not mandate investigation of similar questions prior to the issuance of a judicial warrant. 18 U.S.C. § 2518 (3) (1976). These determinations under Title III are made by the judge reviewing the application on the basis of the facts submitted and any other evidence the judge requested the applicant to supply. 18 U.S.C. § 2518 (1)-(3).

149. 18 U.S.C. § 2518 (1) (a) (1976), (identification of the presenting officer); 18 U.S.C. § 2518 (1) (b) (iv) (1976), (identity of targeted person); 18 U.S.C. § 2518 (1) (b) (i) (1976), (belief that criminal activity targeted, paralleling belief that the target is a foreign power or foreign agent); 18 U.S.C. § 2518 (1) (e) (1976), (prior applications for surveillance); 18 U.S.C. § 2518 (1) (d) (1976), (statement of the proposed duration of surveillance).

150. 50 U.S.C.A. § 1801 (h) (Supp. 1979).

151. Compare 50 U.S.C. § 1804 (a) (5) (Supp. 1979) and 18 U.S.C. § 2518 (5) (1976).

152. 50 U.S.C.A. § 1804 (a) (6) (Supp. 1979).

153. 50 U.S.C.A. § 1804 (a) (8) (Supp. 1979).

154. 50 U.S.C.A. § 1804 (a) (11) (Supp. 1979).

multiple eavesdropping devices within a single surveillance.[155] FISA then requires an equal, if not more thorough, application for surveillance than Title III and most importantly requires a two-step Executive review process prior to judicial submission of the application. These added internal safeguards may prove cumbersome, especially in times of international turmoil when the need for intelligence is acute and immediate.[156]

Subsequent to this two-step Executive review process, the application is then presented to one of the seven United States District Court judges appointed by the Chief Justice of the Supreme Court to hear FISA cases.[157] Significant judicial review is limited to a determination of: (1) whether there is probable cause the person who is the target of the eavesdropping is a "foreign power" or a "foreign agent" as defined in the act, and whether the targeted place is likely to be used by such a targeted person;[158] (2) whether the application complies with the statutory requirement that the procedures delineated in the application insure minimization of "acquisition, retention, and dissemination of information concerning citizens or resident aliens," if applicable;[159] and (3) whether the application possesses the required statements and averments.[160] In addition, if the target of the asked-for surveillance is a United States person, there is an inquiry whether the statements in the certification are clearly erroneous (these statements relate to the foreign intelligence character and the need of

155. 50 U.S.C.A. § 1804 (a) (7) (E) (Supp. 1979).

156. The emergency surveillance provision of 50 U.S.C.A. § 1802 (a) (Supp. 1979) provides little relief to this problem. *See* text accompanying notes 129-35, *supra*.

157. 50 U.S.C.A. § 1805 (a). The designation of the judges is provided for in 50 U.S.C.A. § 1803 (a) (Supp. 1979).

158. 50 U.S.C.A. § 1805 (a) (3) (Supp. 1979). There is also a review of the President's authorization of the Attorney General to approve the application for surveillance, 50 U.S.C.A. § 1805 (a) (1) (Supp. 1979), and a check to insure that a federal officer made the application. 50 U.S.C.A. § 1805 (a) (2) (Supp. 1979). The legislative history reflects that traditional inquiries into an informant's reliability and the basis of his knowledge is also to be scrutinized by the court in determining probable cause of 50 U.S.C.A. § 1805 (a) (3) (Supp. 1979). S. REP. No. 701, *supra* note 84, at 53.

159. S. REP. No. 701, *supra* note 83, at 53-54.

160. This is not a probe into the factual basis of each of these statements or averments, but merely a check of their existence. 50 U.S.C.A. § 1805 (a) (5) (Supp. 1979).

the surveillance).[161] The judge can request further information from the applicant to make this determination.[162] In essence, if the target of the proposed surveillance is a United States person, a comparable level of judicial scrutiny of an application for foreign intelligence electronic surveillance is required as would be required for an application for domestic criminal surveillance under Title III.[163] The degree of scrutiny for surveillance of a non-United States person is less than either of these.[164]

The judge, if satisfied that the application meets these criteria, then enters an *ex parte* order sanctioning the surveillance.[165] The order for a search where the target is not a foreign government, its entity, or a foreign faction is required to specify or describe: (1) the targeted individual; (2) the targeted location; (3)) the type of information and communications sought; (4) the means by which the surveillance is to be effectuated; (5) the permissible duration of the surveillance (the maximum period being ninety days, while the maximum permissible period for Title III is thirty days)[166]; and the limitations and minimization procedure for each surveillance device.[167] However, if the target of the eavesdropping is either a foreign government, an entity of a foreign government, or a foreign political faction or splinter group, the order need not be so detailed,[168] and the minimum duration of surveillance under

161. 50 U.S.C.A. § 1805 (a) (5) (Supp. 1979).

162. 50 U.S.C.A. § 1804 (d) (Supp. 1979).

163. 18 U.S.C. § 2518 (3) (1976) requires the judge to determine that four criteria exist from the facts alleged before issuance of a judicial warrant for electronic eavesdropping: (i) probable cause for belief that the target committed an enumerated offense; (ii) probable cause to believe that the communications concerning the offense would be intercepted; (iii) nonelectronic surveillance had proved or would prove to be fruitless; and (iv) probable cause to believe that the targeted premises was owned or leased by the targeted person or used or to be used in connection with the probable crime.

164. 50 U.S.C.A. § 1805 (a) (Supp. 1979).

165. 50 U.S.C.A. § 1805 (c) (Supp. 1979).

166. 50 U.S.C.A. § 1805 (d) (1) (Supp. 1979). The maximum term for any order for electronic surveillance or extension of an order under Title III is thirty days. 18 U.S.C. § 2518 (5) (1976).

167. 50 U.S.C.A. § 1805 (b) (1) (A)-(F) (Supp. 1979).

168. 50 U.S.C.A. § 1805 (c) (Supp. 1979) provides that such an order (if the target of the electronic eavesdropping fits within the definition of foreign powers set out in 50 U.S.C.A. § 1801 (a) (1), (2), or (3) may omit statements concerning the type of information sought and the communications to be seized, the means of effectuating the surveillance, and the number of bugs or taps to be used. Instead, a general statement as to these points suffices.

the order is raised to one year.[169] Generally, extensions of a surveillance order may be granted by the district judge on the same basis and for the same maximum term as applied to the original order.[170] Further, the court retains the power to review prior to or at the end of the terms of ordered eavesdropping the manner in which any acquired information concerning a citizen or a resident alien is being handled (i.e. minimization procedure).[171]

D. *Emergency Exceptions to the Warrant Procedure*

Besides the limited warrantless surveillance provided in § 1802 (a),[172] the Act allows the normal warrant procedure to be suspended in two situations. First, if the Attorney General reasonably ascertains that an emergency need exists for electronic foreign intelligence surveillance[173] and finds that the factual basis for the issuance of a judicial order exists,[174] he may order the surveillance, so long as he requires adherence to minimization procedures.[175] Concurrently, he must notify a designated district court judge[176] of his decision.[177] This emergency surveillance must discontinue at the end of twenty-four hours unless court approval is obtained in the interim.[178] The emergency provision of Title III[179] is much broader and contains fewer procedural requisites.[180] Any law enforcement officer designated by the Attorney General or by

---

169. 50 U.S.C.A. § 1805 (d) (1) (Supp. 1979).

170. 50 U.S.C.A. § 1805 (d) (2) (Supp. 1979). This section does provide that an extension up to one year may be granted for electronic surveillance targeted at international terrorism, a foreign entity controlled by a foreign government, or a foreign based political group if the judge determines no communications of a citizen or resident alien will be intercepted.

171. 50 U.S.C.A. § 1805(d)(3) (Supp. 1979). This judicial review of compliance with minimization procedures is not obligatory. S. REP. No. 701, *supra* note 83, at 57.

172. *See* p. 671 *supra.*

173. 50 U.S.C.A. § 1805(e)(1) (Supp. 1979).

174. 50 U.S.C.A. § 1805(e)(2) (Supp. 1979).

175. 50 U.S.C.A. § 1805(e) (Supp. 1979).

176. *See* p. 671 *supra.*

177. 50 U.S.C.A. § 1805(e) (Supp. 1979).

178. *Id.*

179. 18 U.S.C. § 2518(7) (1976). The grounds for the emergency exception to the warrant requirement in Title III are conspiratorial activities affecting national security or concerning organized crime which mandate immediate surveillance.

180. S. REP. No. 701, *supra* note 83, at 57.

any state attorney general may make the necessary determinations to institute emergency surveillance.[181] Emergency surveillance under Title III can be maintained for forty-eight hours without filing an application for a judicial order, and after the application is made the surveillance can continue indefinitely until the court refuses to sanction it and denies the application.[182] Second, FISA provides a very narrow exception to the warant procedure which allows fifteen days of Executive order electronic surveillance subsequent to a congressional declaration of war.[183]

E. *Use of the Surveillance Product*

Inter-law enforcement agency[184] use of any information acquired pursuant to FISA [hereinafter FISA information] and pertaining to a citizen or resident alien is regulated by the minimization procedures, which restrict the use to purely foreign intelligence or criminal law enforcement purposes.[185] Any information so obtained may only be used for lawful purposes.[186] Evidentiary use of FISA information is permitted in procedures before federal, state, and local courts, administrative bodies, or other political bodies or authorities, but only if notice of the intention to use it is given to the "aggrieved person"[187] within a reasonable time prior to the proceeding.[188] This party may then move to suppress the evidence in a pre-trial motion on the statutory grounds of unlawful acquisition of the information or governmental failure to conform to the order or authorization for electronic surveillance.[189] Title III provides comparable provisions

---

181. 18 U.S.C. § 2518(7) (1976).

182. *Id.*

183. 50 U.S.C.A. § 1811 (Supp. 1979).

184. The act also contemplates dissemination of information acquired pursuant to FISA surveillance to non-governmental officials in limited situations. S. REP. No. 604-pt.1, *supra* note 75, at 54.

185. 50 U.S.C.A. § 1806(a) (Supp. 1979); H.R. REP. No. 1283, 95th Cong., 2d Sess. 87 (1978).

186. This protection runs not only to "United States persons," but also to foreign visitors and non-resident aliens. 50 U.S.C.A. § 1806(a) (Supp. 1979). Lawful purposes restricts the use of FISA information to actual foreign intelligence purposes and the enforcement of the criminal law. S. REP. No. 701, *supra* note 83, at 59.

187. 50 U.S.C.A. § 1801(k) (Supp. 1979). Aggrieved person is synonymous with the subject of the electronic surveillance.

188. 50 U.S.C.A. § 1806(c),(d) (Supp. 1979).

189. 50 U.S.C.A. § 1806(d) (Supp. 1979). These two statutory grounds for

restricting law enforcement agency use of eavesdropping information,[190] requiring notice prior to evidentiary use,[191] and delineating non-exclusive statutory grounds for challenging the introduction of the information in official proceedings.[192] Title III further requires that the court give the parties notice of the judicial order sanctioning electronic eavesdropping, within ninety days of the order's entry.[193] FISA has no comparable provision because of the sensitivity of divulging such information in the foreign intelligence area.[194]

Both acts provide the opportunity for a pre-trial exclusionary hearing for statutory or other challenge to the admission into evidence or disclosure of the eavesdrop-attained information.[195] Title III gives the judge discretion to determine the portions of the intercepted communications the aggrieved person may review "in the interest of justice."[196] The implication is that only if the government can show exigent circumstances which warrant retention of the information will the targeted person be prohibited from seeing all or some of the transcript, prior to or at the hearing.[197] FISA on the other hand, states: "the court may disclose to the aggrieved person, under appropriate procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only when such disclosure is necessary to make an accurate determination of the legality of the surveil-

---

challenging admission of FISA information are not pre-emptive of other challenges, but it would appear any fourth amendment challenge would be subsumed within the unlawful acquisition statutory challenge. No matter what the basis of the motion is, this statutory procedure must be adhered to. *See* S. REP. No. 604-pt.1, *supra* note 75, at 56.

190. 18 U.S.C. § 2517 (1976).

191. 18 U.S.C. § 2518(8)(d) (1976).

192. 18 U.S.C. § 2518(10)(a) (1976). This subsection provides an additional ground for exclusion of the surveillance information based upon a finding that the authorization was deficient in some respect on its face. 18 U.S.C. § 2518(10)(a)(ii) (1976).

193. 18 U.S.C. § 2518(8)(d) (1976).

194. *See* S. REP. No. 604-pt.1, *supra* note 75, at 82-83.

195. 50 U.S.C.A. § 1806(e) (Supp. 1979) FISA; 18 U.S.C. § 2528(10)(a) (1976) Title III.

196. 18 U.S.C. § 2518(10)(a) (1976).

197. S. REP. No. 1097, 90th Cong., 2d Sess., *reprinted in* [1968] U.S. CODE CONG. & AD. NEWS 2195-96. In addition Title III requires law enforcement officers to record any intercepted conversations if at all feasible. Thus, a transcript or at least a recording is usually available. 18 U.S.C. § 2518(8)(a). FISA has no comparable provision.

lance."[198] The presumption is that the party may not review any of the government's materials unless he can meet the burden of demonstrating their indispensibility to his motion. Unless some privilege is the basis of the aggrieved party's motion, there would be no basis for requesting a transcript of the intercepted communications and normally only a copy of the application for surveillance and the court order would be available.[199]

In addition, under FISA the government, via the Attorney General, possesses the power to circumvent the normal hearing procedure for challenging the admission of electronically attained information.[200] The Attorney General need only swear by affidavit that either convening an adversary hearing or allowing any disclosure of the surveillance application or its order would jeopardize national security, to preempt such a proceeding.[201] Then he must file a copy of the surveillance application and the order with the court.[202] The court then makes an *ex parte* and *in camera* decision of whether the surveillance was lawful, and discloses its decision to the aggrieved party with any portion of the application, the order, or other materials it deems may be unveiled.[203] This government ability to force exclusion of the adversary party from a hearing on the admissibility of FISA information is predicated entirely upon the need for protection of national security interests.[204]

F. Enforcement and Congressional Oversight

Both acts provide the dual enforcement mechanism of criminal sanctions for intentional unauthorized electronic surveillance or disclosure of information from a known illegal bug or tap[205] and a concurrent statutory civil cause of action for damages.[206] Both

198. 50 U.S.C.A. § 1806(f) (Supp. 1979).
199. S. REP. No. 701, *supra* note 83, at 63-64.
200. 50 U.S.C.A. § 1806(f) (Supp. 1979).
201. *Id.*
202. *Id.*
203. *Id.*
204. S. REP. No. 701, *supra* note 83, at 64. Title III has no provision even remotely akin to this empowering of the Attorney General.
205. *Compare* 50 U.S.C.A. § 1809 (Supp. 1979) with 18 U.S.C. § 2511(a) (1976).
206. FISA provides that violations of the criminal proviso invokes the statutory civil damage cause of action. 50 U.S.C.A. § 1810 (Supp. 1979). Title III establishes a civil damage cause of action for any violation of the act whether it

acts also require that the Attorney General submit reports on all surveillance conducted pursuant to the application statute. Title III requires filing of a yearly detailed report by the United States Attorney General and state attorneys general or their appointed subordinates to a United States court.[207] The court in turn submits an annual report to Congress.[208] FISA requires the United States Attorney General to "fully inform" the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence on a semi-annual basis of all surveillance conducted pursuant to the Act.[209] It is unclear whether a written report, oral testimony, or both are envisioned by this duty, but it is clear that whatever mode is adopted, it must be detailed enough to allow the committees to understand the breadth, regularity, and purpose of such surveillance.[210] This means that the Attorney General must gather, analyze, and report on each agency which acted under FISA. The legislative justification for this close scrutiny is the lack of routine notice to the surveillance target, the expectation that few FISA surveillances will culminate in criminal trials, and the limited judicial review by just a few justices who may be closely aligned with the requesting parties.[211] The two Congressional committees report to their respective houses of Congress on the Act's implementation for each of five years after enactment of the statute and they are to append recommendations for amendments.[212]

V. Constitutional Issues

A threshold issue addressed in Congressional subcommittee hearings[213] and committee reports[214] is whether the legislature has the authority to circumscribe what has generally been thought of

---

be due to negligence or whether it is intentional. 18 U.S.C. § 2520 (1976).

207. 18 U.S.C. § 2519(2) (1976). Unlike FISA's vague standard for informing Congress of activities pursuant to it, this section of Title III specifies seven points which a report to the United States court must contain.

208. 18 U.S.C. § 2519(3) (1976).

209. 50 U.S.C.A. § 1808(a) (Supp. 1979).

210. S. Rep. No. 701, *supra* note 83, at 67.

211. *Id.*

212. 50 U.S.C.A. § 1808(b) (Supp. 1979).

213. *Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence,* 95th Cong., 2d Sess. 27-28, 133 (1978).

214. S. Rep. No. 604-pt.1, *supra* note 75, at 16.

as a purely Executive power to initiate warrantless foreign intelligence eavesdropping. Although there has been a wide discrepancy among constitutional authorities as to the existence and breadth of an inherent power of the President to act unchecked in this area,[215] at least one United States appellate court has recognized broad and seemingly immutable Executive authority. In *United States v. Brown,* the Fifth Circuit stated that:

> because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence. . . . Restrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere.[216]

Assuming arguendo that an inherent Presidential power to collect foreign intelligence exists, the constitutional basis for this power is found in the Presidential power to act as commander-in-chief of the armed forces,[217] the Presidential duty to preserve, protect, and defend the Constitution,[218] and inherent powers emanating from the Presidential status as the sole mouthpiece of the nation in dealing with other countries.[219] Congress as recently as 1973 acted to redefine and restrict the President's commander-in-chief power, via passage over Presidential veto of the War Powers Resolution.[220] Further, Congress has, at times, exercised its powers in an effort to curtail Presidential powers in the conducting of foreign affairs.[221] Since Congress clearly may limit the powers which form the foundation of the Presidential power to collect foreign intelligence, it appears logical that the emanating power is also subject to legislative curtailment.

Some authorities have maintained that congressional regulation of the basal powers is non-analogous to the case of an inherent

---

215. *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence,* 94th Cong., 2d Sess. 12-13 (1977) (Statement of Sen. Edward M. Kennedy).

216. 484 F.2d 426 (5th Cir. 1973).

217. U.S. CONST. art. II, § 2, cl. 1.

218. U.S. CONST. art. II, § 1, cl. 8.

219. U.S. CONST. art. II, § 3, *supra* note 30.

220. War Power Resolution, 50 U.S.C.A. §§ 1541-48 (Supp. 1979).

221. L. TRIBE, AMERICAN CONSTITUTIONAL LAW 163-67 (1978).

power.[222] This is premised upon the faulty assumption that all inherent powers of the President equate with plenary powers. The Supreme Court, in *Myers v. United States,* suggested that not all inherent powers are unlimited or limited only by specific constitutional proscriptions.[223] Further, in the absence of explicit constitutional delegation or congressional recognition and ratification of a claimed inherent executive power,[224] the legislature retains the authority to regulate or preclude executive authority.[225] This analysis by Justice Jackson in *Youngstown Co. v. Sawyer* was the authority which Congress cited when it rather summarily decided that it had the authority to enact FISA.[226]

A more perplexing issue raised by the statute is whether the procedures and provisions for limited warrantless and court sanctioned electronic surveillance are violative of the fourth amendment. Implicit within the basic premise and purpose of the statute is the recognition of the fourth amendment's applicability,[227] and rejection of the premise that there exists an absolute national security exception to the amendment.[228] Yet, the amendment's applicability does not automatically mandate usage of the prior judicial warrant procedure, as it must at least be shown that it is reasonable to procure a search warrant.[229] The relevant test is whether a warrant requirement would "frustrate the governmental purpose behind the search."[230] Even if a warrant procedure is appropriate, the Supreme Court said in *Keith,* "the warrant application may vary according to the governmental interest to be enforced and the nature of the citizen right deserving protection."[231] This fourth amendment analysis is the theoretical basis of FISA's two provisions authorizing and prescribing procedures for electronic foreign intelligence surveillance.

---

222. *Id.* at 159.

223. Myers v. United States, 272 U.S. 52 (1926); L. TRIBE, AMERICAN CONSTITUTIONAL LAW 159 (1978).

224. CONGRESSIONAL RESEARCH SERVICE LIBRARY OF CONGRESS, *supra* note 30, at 544-55.

225. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 637 (1952) (Jackson, J., concurring).

226. S. REP. No. 604-pt.1, *supra* note 75, at 16.

227. S. REP. No. 701, *supra* note 83, at 9.

228. S. REP. No. 604-pt.1, *supra* note 75, at 16.

229. 2 W. LAFAVE, SEARCH AND SEIZURE § 4.1 (a) (1978).

230. Camara v. Municipal Court, 387 U.S. 522, 533 (1967).

231. United States v. United States District Court, 407 U.S. 323 (1972).

One criticism of the judicial warrant procedure stems from the possibility that the surveillance authorization may issue against a United States person without a finding of probable cause that a crime has, is being, or is about to be committed and that there need not be a showing that evidence of criminal activity will be seized.[232] Proponents of the bill argue that the possibility of warrantless surveillance aimed at a United States person under FISA is extremely limited in lieu of the House amendment of the definition of an agent of a foreign power.[233] Furthermore, they maintain there is constitutional authority for searches without such probable cause, and the Supreme Court has insinuated that a broader focus of probable cause may be appropriate in cases involving national security.[234]

The statute's proponents rely on *Camara v. Municipal Court*[235] and *See v. Seattle*[236] as one line of authority supporting the notion that a judicial search warrant may issue upon a finding of something less than criminal probable cause. These cases held that although a warrant was required for housing code inspections or searches and business premises searches, such a warrant could issue without a showing of the inspector's belief that a particular dwelling or business was in violation of the relevant municipal code.[237] The Court went on to say in *Camara* that area code-enforcement inspections pursuant to a warrant are reasonable under the fourth amendment,[238] and that probable cause to issue such a warrant is met "if reasonable legislative or administrative standards for conducting an area inspection are satisfied with respect to a particular dwelling."[239] Thus, the quantum of evidence required for a code-enforcement inspection warrant is less than for a criminal warrant (*i.e.* criminal probable cause).

---

232. *Hearings on S. 1566, supra* note 213, at 112-13, (Prepared Statement of John H. F. Shattuck, Director, Washington Office, and Jerry J. Berman, Legislative Counsel, American Civil Liberties Union).

233. *Hearings on S. 1566, supra* note 213, at 14 (Prepared Statement of Hon. Griffin B. Bell, Attorney General of the United States).

234. *Id.* at 15.

235. 387 U.S. 523 (1967).

236. 387 U.S. 541 (1967).

237. Camara v. Municipal Court, 387 U.S. 523 (1967); See v. Seattle, 387 U.S. 541 (1967).

238. Camara v. Municipal Court, 387 U.S. 523, 537 (1967).

239. *Id.* at 538.

The Court justified this holding upon three factors.[240] First, area code-enforcement inspections had a history of judicial and public acceptance. Second, there was an overriding public interest coupled with the inadequacy of alternative enforcement methods. Third, the inspections were a limited invasion of an individual's privacy because they were not aimed at the discovery of criminal evidence nor were they personal in nature. This essentially is a balancing of governmental interest in the need to search with the individual's privacy interest. A similar analysis supported "stop and frisk"[241] and airport searches[242] upon a finding of less than criminal probable cause.

Likewise, warrantless foreign intelligence electronic surveillance has historically received judicial and public acceptance, and although there has not been strong precedent for non-criminal probable cause determinations to support the issuance of an order for such surveillance, there was wide support for such a measure as evidenced by the passage of FISA.[243] It is also maintained that there is an overriding governmental need for foreign intelligence and that other modes of acquisition of such information have proved fruitless or of attenuated value. Finally, although it can be argued that the purpose of the surveillance is not the collection of evidence for criminal prosecutions, it is not true that electronic surveillance is a less pervasive intrusion than a normal search for criminal evidence.[244] Thus, the balance of these factors is not clear as in the *Camara* and *See* cases and the "stop and frisk" cases.

The government also rests its assertion that foreign intelligence electronic surveillance can be sustained by a finding of less than criminal probable cause on the fact that custom searches have

240. *Id.* at 537-38.

241. Terry v. Ohio, 392 U.S. 1 (1968).

242. United States v. Davis, 482 F.2d 893 (9th Cir. 1973).

243. The judicial acceptance is evidenced by the Supreme Court's consistent denial of *certiorari* in cases where the appellate courts have upheld the executive authority to issue warrantless foreign intelligence electronic surveillance. Zweibon v. Mitchell, *cert. denied,* 425 U.S. 944 (1976); United States v. Butenko, *cert. denied,* 415 U.S. 960 (1974); United States v. Brown, *cert. denied,* 415 U.S. 960 (1974); United States v. Buck, *cert. denied,* 434 U.S. 890 (1979); United States v. Clay, *cert. denied,* 394 U.S. 310 (1969).

244. *See* 124 CONG. REC. S6019 (daily ed. April 20, 1978) and 124 CONG. REC. H9273 (daily ed. Sept. 7, 1978).

been similarly sustained and held constitutional.[245] Custom searches are compatible with the fourth amendment, because of the overriding governmental interest in the right of the sovereign to protect itself and the history of acceptance of such searches.[246] The court in *United States v. Ramsey* stated:

> Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended upon the existence of probable cause.[247]

A related fourth amendment issue precipitated by FISA is whether the dual standard of review created by the definition of "United States Person"[248] as used in the categories of "foreign power" and "agent of a foreign power" is permissible.[249] Congress recognized that the Act creates a lesser standard of review for the invocation of electronic surveillance targeted at illegal aliens and foreign visitors, and that eavesdropping upon such classes may be authorized without a showing of criminal probable cause.[250] Further, minimization procedures are only applicable to information concerning a United States person.[251]

It is clear that aliens, once within the United States, are afforded the full protection of the fourth amendment in the criminal justice system.[252] Critics argue that since the fourth amendment protects the "right of the people"[253] the standard mandated by the amendment for citizens and resident aliens should apply to illegal aliens, foreign visitors, foreign students, and alien foreign embassy personnel.[254] Proponents of FISA argue that a finding of

---

245. *Hearings on S. 1566, supra* note 213, at 114-15 (Prepared Statement of Hon. Griffin B. Bell, Attorney General of the United States).

246. United States v. Ramsey, 431 U.S. 606 (1977).

247. *Id.* at 619.

248. 50 U.S.C.A. § 1801 (i) (Supp. 1979).

249. *Hearings of S. 1566, supra* note 213, at 113-14 (Prepared Statement of John H. F. Shattuck and Jerry J. Berman) and at 102-04 (Prepared Statement of Prof. Christopher H. Pyle, Mount Holyoke College).

250. S. REP. No. 604-pt. 1, *supra* note 75, at 21-22.

251. 50 U.S.C.A. § 1801 (h) (Supp. 1979).

252. In re Weinstein, 271 F. 5, *aff'd*, 271 F. 673 (1920); Abel v. United States, 362 U.S. 217 (1960).

253. U.S. CONST. amend. XIV.

254. *Hearings on S. 1566, supra* note 213, at 113 (Prepared Statement of

less than criminal probable cause will support an arrest for deportation of an alien as it will support a border search involving illegal aliens.[255] Critics argue that at best these cases may support distinguishing illegal aliens from others properly in the country, but such authority cannot support a lesser standard for surveillance of legal foreign visitors.[256]

The congressional committee reports justified the distinction in summary fashion by stating that *Hampton v. Mow Sun Wong*[257] supports the proposition that alienage differentiation is permissible "where there are compelling considerations of national security."[258] The Supreme Court did find that the federal government may create classifications that distinguish aliens in an adverse manner consistent with the fifth amendment due process clause and its adjunct equal protection considerations if there is an overriding national interest justifying the discriminatory rule, even though an identical classification made by a state would be prohibited.[259] Yet, citation of this principle skirts the fourth amendment issue. Unlike *Hampton*,[260] the basis of the equal protection claim here is unequal statutory standards which are intended to implement and deliniate fourth amendment rights. Thus, a separate fourth amendment problem is created. The approach of Congress and the administration is to look only at the equal protection aspect of the issue and reason that since there is a rational basis for the classification and distinction between non-resident aliens and United States persons the statute is in accord with the entire Constitution.[261] The problem with this reasoning is that Congress has stated that FISA is a legislative interpretation of the fourth amendment which dictates in the area of foreign intelligence surveillance, and the Supreme Court has ratified the notion that aliens are entitled to the full protection of the fourth

---

John H. F. Shattuck and Jerry J. Berman).

255. *Id.* at 113-14.

256. *Id.* at 114.

257. 426 U.S. 88 (1976).

258. S. REP. No. 604-pt. 1, *supra* note 75, at 21; S. REP. No. 701, *supra* note 82, at 20.

259. Hampton v. Mow Sun Wong, 426 U.S. 88 (1976).

260. The claim in *Hampton* was that a Civil Service Commission regulation barring non-citizens from competing for Federal Civil jobs was violative of the fifth amendment due process clause. *Id.*

261. *Hearings of S. 1566, supra* note 213, at 15 (Prepared Statement of Hon. Griffin B. Bell).

amendment.[262] Yet the statute creates a lesser standard of fourth amendment protection for non-United States persons.

Authority for this divergent set of fourth amendment standards for United States persons and non-resident aliens might be found in the cases involving border searches for aliens and deportation interrogation and arrests of aliens. Under the Immigration and Nationality Act officers of the Immigration Service are empowered to interrogate or arrest a person believed to be an illegal alien on a finding of less than criminal probable cause.[263] Likewise, they may board and search any vehicle for illegal aliens within a reasonable distance from a United States border without having to acquire a warrant or without a showing of criminal probable cause.[264] These statutory provisions are in accord with the fourth amendment mandates even though they allow a lesser standard of protection for aliens.[265] The justification for such provisions lies in the overriding governmental interest of protecting the national boundaries and the national security.[266] This reasoning could easily be extended to justify the FISA system which provides a lesser standard of review prior to initiation of electronic surveillance directed at non-United States persons. A central legislative tenet of the Act is that the government has a legitimate and pressing need for foreign intelligence information to protect the national security.[267]

The equal protection criticism of the statutory dual standards is easily dealt with. The Supreme Court has consistently deferred to federal statutes creating classifications aimed against aliens or classes of aliens, so long as the statutory schemata has a rational basis in a permissible governmental goal.[268] The Court is unwilling to substitute its own judgment for that of either the federal legislature or the Executive on decisions involving aliens.[269] The Court stated in *Mathews v. Diaz:*

---

262. Abel v. United States, 362 U.S. 217 (1960).

263. Immigration and Nationality Act, 8 U.S.C. § 1357 (a) (1) and (2) (1976).

264. 8 U.S.C. § 1357 (a) (3) (1976).

265. Fernandez v. United States, 321 F.2d 283 (9th Cir. 1963); Tsimounis v. J. W. Holland, 132 F. Supp. 754 (E.D. Pa. 1955), *aff'd,* 228 F.2d 907; *see also* Almedia Sanchez v. United States, 413 U.S. 266 (1973).

266. Fernandez v. United States, 321 F.2d 283 (9th Cir. 1963).

267. S. REP. No. 604-pt. 1, *supra* note 75, at 9.

268. Mathews v. Diaz, 426 U.S. 67 (1976); Hampton v. Mow Sun Wong, 426 U.S. 88 (1976).

269. Mathews v. Diaz, 426 U.S. 67, 81 (1976).

> For reasons long recognized as valid, responsibility for regulating the relationship between the United States and our alien visitors has been committed to the political branches of the Federal Government. Since decisions in these matters may implicate our relations with foreign powers, and since a wide variety of classifications must be defined in the light of changing political and economic circumstances, such decisions are frequently of a character more appropriate to either the Legislature or the Executive than to the Judiciary.[270]

The collection of foreign intelligence is recognized as a permissible goal and legislative history provides support for the notion that the statutory differentiation has a rational basis.[271]

Another issue raised centers around the ability of the government, via the Attorney General, to usurp an aggrieved party's right to be present at the hearing on his motion to supress FISA information.[272] If the Attorney General files an affidavit stating "that an adversary hearing would harm the national security or the foreign affairs of the United States" he can force an *in camera* and *ex parte* hearing on the critical motion of the defendant's case.[273] The basis of the objection to this procedure is that it denies the defendant his sixth amendment right to counsel and his right to have an adversary hearing, an essential component of due process in a criminal proceeding.[274] An ancillary argument is that exclusion of the defendant from the pretrial suppression hearing may violate the defendant's sixth amendment right of confrontation.[275] Finally, it can be maintained that the proceeding violates the defendant's right to have a public trial.[276]

One government argument in support of such an *ex parte* and *in camera* hearing rests upon the premise that due process is a flexible standard that mandates "procedural protections as the

---

270. *Id.*

271. *Hearings on S. 1566, supra* note 213, at 136 (Prepared Statement of Steven B. Rosenfeld, Association of the Bar of the City of New York).

272. *Hearings on S. 1566, supra* note 213, at 15 (Prepared Statement of Hon. Griffin B. Bell).

273. 50 U.S.C.A. § 1806 (f) (Supp. 1979).

274. *See, Hearings on S. 1566, supra* note 213, at 136 (Prepared Statement of Steven B. Rosenfeld).

275. U.S. CONST. Amend. VI: "In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . and to have the Assistance of Counsel for his defense."

276. U.S. CONST. Amend. VI; In re Oliver, 333 U.S. 257 (1948).

particular situation demands."[277] In applying this premise, the court must balance the interest of the defendant with compelling governmental interests. Such governmental interests include protection of the national security and the need for secrecy in dealing with materials concerning foreign affairs which are either potentially harmful to the country or potentially embarrassing.[278] Without an *ex parte* and *in camera* proceeding the only way to effectively protect the government's interest is to not prosecute criminal cases based upon sensitive FISA acquired information. Likewise, the government would maintain that the nature of the hearing and the material involved warrants suspension of the defendant's sixth amendment claims.

Another point supporting the government's position is that a pretrial hearing to exclude evidence is not equivalent to a trial and as such the rights on which the critics of FISA base their objections to the *ex parte* and *in camera* proceeding are not applicable. The defendant's sixth amendment right to be confronted with antagonistic witnesses has been held to be "basically a trial right. . . . It includes both the opportunity to cross-examine and the occasion for the jury to weigh the demeanor of the witness."[279] Since a defendant would be availed of the opportunity to cross-examine the officers conducting the surveillance at trial, the confrontation right is not violated by the FISA *ex parte* and *in camera* pretrial hearing. Likewise the same argument can be made to refute the defendant's claim that the hearing violated his sixth amendment right to a public trial.[280]

The due process challenge relates to the fact that neither the defendant nor his attorney are allowed access to the hearing on their motion to suppress the FISA acquired information. In trials which involve possible admission of wiretap or bug attained information, the motion to suppress this information is often the critical issue.[281] The Supreme Court has held that a fourth amendment pretrial probable cause determination may be made without the defendant's presence, without offending due process man-

277. *Congressional Research Service, Library of Congress, supra* note 30, at 1406 (7th ed. 1972); Ex Parte Wall, 107 U.S. 265, 289 (1883).

278. *Id.* at 1145.

279. Barber v. Page, 390 U.S. 719, 725 (1968).

280. *See,* In re Oliver, 333 U.S. 257, 266-73 (1948).

281. *See,* Y. KAMISAR, W.R. LAFAVE, AND J.H. ISRAEL, MODERN CRIMINAL PROCEDURE, CASES, COMMENTS AND QUESTIONS 12 (4th ed. 1974).

dates.[282] The informal *ex parte* hearing was justified because a probable cause determination would only result in the defendant being bound over for trial and not a determination of guilt. The determination does not require "the fine resolution of conflicting evidence that a reasonable-doubt or even a preponderance of the evidence standard demands, and credibility determinations are seldom crucial in deciding whether the evidence supports a reasonable belief in guilt."[283] Further, the Court reasoned that the pretrial hearing was not a critical stage (i.e. a "pretrial procedure that would impair defense on the merits if the accused is required to proceed without counsel").[284] These authorities are arguably inapposite when applied to a pretrial motion to supress FISA acquired information. The determination of the evidence's admissibility is likely the crucial issue in the case, which may require a difficult resolution of convoluted and conflicting evidence and the application of intricate and rapidly evolving principles of law. Such a hearing is also arguably a "critical stage" of a criminal prosecution of the sixth amendment right to counsel purpose and as such it is subsumed within the defendant's right to an attorney at the trial itself.[285] The Supreme Court has similarly held that a defendant is entitled to both an adversary hearing and an attorney to determine probable cause for parole[286] and probation violations.[287]

The government may counter that irrespective of either sixth amendment challenges or the due process claim, the need for secrecy of the proceeding and the need to use FISA obtained information outweighs the defendant's interests. The government will argue that neither the right to an attorney nor the right to confront witnesses is particularly important at a FISA evidence suppression hearing. Defendant by his attorney may submit briefs detailing his objections to the admission of the eavesdropping product. The Act also provides that if the court decides disclosure of some of the information is necessary for a determination of the legality of the search, it may disclose selected portions of the re-

282. Gernstein v. Pugh, 420 U.S. 103 (1975).
283. *Id.* at 121.
284. *Id.* at 122-23.
285. Powell v. Alabama, 287 U.S. 45 (1932).
286. Morrissey v. Brewer, 408 U.S. 471 (1972).
287. Gagnon v. Scarpelli, 411 U.S. 778 (1973).

cord before the court.[288] Yet, even with such safeguards, the defense is unable to respond to factual inconsistencies of the presented evidence, unable to timely refute or attack any believed falsity of evidence the government introduces, unable to confront any witness the government puts on, and unable to oversee the level of scrutiny the court gives their motion, in this most critical stage of the defendant's case. Thus there are serious doubts as to the constitutionality of 50 U.S.C.A. § 1806 (f) (Supp. 1979).

A final constitutional challenge to FISA is based upon the Supreme Court's decision in *Berger v. New York*.[289] The Court overturned the eavesdropping pursuant to a New York statute, finding it "too broad in its sweep resulting in a trespassory intrusion into a constitutionally protected area and . . . therefore violative of the fourth and fourteenth amendments."[290] The Court found the statute reprehensible because it lacked a requirement for particularizing the specific crime suspected, the place to be searched, or the things (i.e. specific conversations) to be seized.[291] Secondly, the Act authorized eavesdropping for a period of two months upon a single application and an equally long extension upon a mere showing that such an extension is in the public interest (i.e. without showing new grounds for the surveillance).[292] Third, the statute failed to provide for termination of surveillance once the sought after information was attained.[293] Finally, the statute's procedure allowed eavesdropping without requiring a showing of exigent circumstances which would serve in place of the usual notice requirement of conventional search warrants.[294]

The schemata of surveillance envisioned by FISA could similarly be attacked. Eavesdropping of non-United States persons can occur without a showing of criminal probable cause, but the statute does require specification of the conversation to be seized,[295] the target of the surveillance,[296] and a showing that the target is a foreign power or an agent of a foreign power.[297] FISA

288. 50 U.S.C.A. § 1806 (f) (Supp. 1979).
289. 388 U.S. 41 (1967).
290. *Id.* at 44.
291. *Id.* at 55-56.
292. *Id.* at 59.
293. *Id.* at 59-60.
294. *Id.* at 60.
295. 50 U.S.C.A. § 1804 (a) (6) (Supp. 1979).
296. 50 U.S.C.A. § 1804 (a) (3) (Supp. 1979).
297. 50 U.S.C.A. § 1804 (a) (4) (A) (Supp. 1979).

authorized surveillance for periods up to 90 days or one year,[298] but requires that extensions be based upon new findings capable of supporting an original order.[299] Additionally, under FISA the surveillance normally terminates upon the acquisition of the desired information, but it is possible to circumvent this rule if the application for surveillance states that the intelligence gathering is to be ongoing and states facts which support the notion that more information will be acquired.[300] Finally, the statute assumes that the exigency and priority of the need for foreign intelligence surveillance compensates for any lack of notice.[301] Thus, an argument that FISA creates too great a trespassory infringement upon individuals can be made. Considering, however, the judicial history of yielding to executive and legislative discretion in this area, it is unlikely such an argument would prevail.

VI. Possible FISA Amendments

After one year of the statute's operation, not one executive request for court authorized electronic surveillance under FISA had been refused. This fact may either be attributable to the lack of thorough judicial screening and the close working relationship of the intelligence community and the seven district judges or it might be attributable to more thorough executive screening of possible FISA applications. This report does demonstrate, however, the need for further analysis and evaluation of the present Act. If the prior hypothesis is correct, it points to a need to either expand the number of judges who hear FISA petitions and/or to create a panel of judges to hear the government's request for surveillance. This expansion will minimize the chances of undue government influence over the decision making process and will enhance scrutiny of the decision makers. Another method of strengthening the screening of applications for surveillance might be to require the same standard for initiation of surveillance aimed at non-United States persons as is required for surveillance involving United States persons.

An amendment which would clear up the most troublesome constitutional issue would abandon the use of *ex parte* proceed-

298. 50 U.S.C.A. § 1805 (d) (1) (Supp. 1979); 50 U.S.C.A. § 1802 (a) (1) (Supp. 1979).

299. 50 U.S.C.A. § 1805 (d) (2) (Supp. 1979).

300. 50 U.S.C.A. § 1804 (a) (10) (Supp. 1979).

301. S. Rep. No. 95-604-pt.1, *supra* note 75, at 59.

ings for the review of the admissibility of FISA obtained evidence. The hearing still could be held *in camera* and by limiting accessability to the defendant and one of his attorneys and by ordering non-disclosure of any information brought out in the hearing (especially an agent's identity), the threat of security leaks may be attenuated. Furthermore, the government can always refuse to bring criminal charges if it feels that the risk of a security leak is too great and it may revert to the remedy of deportation if the putative defendant is an alien.

The emergency warrantless surveillance provisions of 50 U.S.C.A. § 1805 (e) should be expanded to at least coincide with the Title III provision.[302] Requiring the government to bring an application for electronic surveillance and to receive a judicial order pursuant to a hearing within twenty-four hours of initiation of the emergency surveillance presents an undue hardship on the government's ability to effectuate emergency surveillance.[303] Forty-eight hours is a more reasonable time parameter in which to file a petition for surveillance, especially in light of the fact that only seven judges are empowered to hear such petitions.

FISA, via statutory proscription of warrantless foreign intelligence surveillance, clarified a confusing area of federal law. The Act sets out specific procedures for the acquisition and regulation of electronic surveillance for foreign intelligence purposes by the Executive. In this respect the Act well serves a meritorious purpose. The Act was also designed to balance the government's need for procuring foreign intelligence information against the individual right to be free from invidous government intrusions upon his privacy. The proper positioning of this legal fulcrum will require careful evaluation of the current statutory schemata and of judicial and executive experience with the Act.

Kim L. Kelley

302. 18 U.S.C. § 2518 (7) (1976).
303. 50 U.S.C.A. § 1805 (e) (Supp. 1979).