San Diego Law Review

Volume 17 | Issue 4 Article 8

8-8-1980

Foreign Intelligence Surveillance Act: Unconstitutional Warrant Criteria Permit Wiretapping If a Possibility of International Terrorism Is Found

Chipp Purdy

FOREIGN INTELLIGENCE SURVEILLANCE ACT: UNCONSTITUTIONAL WARRANT CRITERIA PERMIT WIRETAPPING IF A *POSSIBILITY* OF INTERNATIONAL TERRORISM IS FOUND

This Comment examines the warrant criteria established in the Foreign Intelligence Surveillance Act of 1978 as applied to persons who may be international terrorists. The Act permits electronic surveillance if a possibility of international terrorism is found. The author concludes that the Act's warrant criteria are unconstitutional under the fourth amendment.

INTRODUCTION

In October of 1978 Congress passed the Foreign Intelligence Surveillance Act (FISA).[1] This legislation attempts to limit the executive's power to authorize warrantless electronic surveillance of foreign powers.[2] The Act requires government officials to obtain a warrant from a specially designated court[3] before wiretapping persons acting on behalf of foreign powers.[4] However, a finding of probable cause to believe criminal activity or activity harmful to the nation's security has been taking place is not re-

1. The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified at 50 U.S.C.A. §§ 1801-1811 (West Supp. 1979)).

2. *See* S. REP. No. 95-604, 95th Cong., 1st Sess. at 8 (1977) (The Foreign Intelligence Surveillance Act is "designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it."). *See also* S. REP. No. 95-701, 95th Cong., 2d Sess. (1978); H.R. REP. No. 1283, Pt. I, 95th Cong, 2d Sess. (1978).

3. 50 U.S.C.A. § 1803 (West Supp. 1979).

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

(a) "Foreign power" means—

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or

quired for issuance of a warrant.[5] Nor is a reasonable suspicion of objectionable activity required.[6] Rather, if the person to be tapped (hereinafter the target) is a United States citizen or resident alien, the special court need only find probable cause to believe that the target "may" be involved in clandestine intelligence gathering activities on behalf of a foreign power that are violative of federal criminal law.[7] If the target is a nonresident alien, the special court need only find probable cause to believe that the target "may" be engaged in clandestine intelligence activities on behalf of a foreign power that are "contrary to the interests of the United States."[8]

After briefly discussing the history giving rise to FISA, this Comment will explore the constitutionality of FISA's warrant criteria as applied to persons who may be international terrorists. It will be shown that the warrant criteria are unconstitutional. Before delving into the analysis, however, the modern threat of

---

governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefore;

(5) a foreign based political organization, not substantially composed of United States persons, or

(6) an entity that is directed and controlled by a foreign government or governments.

50 U.S.C.A. § 1801 (a)(1)-(6) (West Supp. 1979).

5. *See* 50 U.S.C.A. § 1805(a) (West Supp. 1979).

6. *Id.*

7. 50 U.S.C.A. §§ 1801(b), (a)(3)(A) (West Supp. 1979). The examining court must also find that:

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal Officer and approved by the Attorney General;

(3). . . .

(B) each of the facilities or places at which electronic surveillance is directed is being used, or about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under [50 U.S.C.A. § 1804]; and

(5) the application which has been filed contains all statements and certifications required by [50 U.S.C.A. § 1804] and, if the target is a United States person, the certification or certifications are not clearly erroneous

. . . .

50 U.S.C.A. § 1805(a) (West Supp. 1979). The certifications required by § 1804 involve statements that the information sought is foreign intelligence information and that such information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C.A. § 1804(a)(7) (West Supp. 1979). It seems unlikely that a warrant would be denied on the basis that a required certification is "clearly erroneous" when one considers the heavy burden that is ordinarily required for a showing that a finding is "clearly erroneous." *See* C. WRIGHT, LAW OF FEDERAL COURTS § 96 at 479 (3d ed. 1976).

8. 50 U.S.C.A. §§ 1801(b), 1805(a)(3)(A) (West Supp. 1979).

terrorism and the executive department's ability to uproot that threat will be discussed.

The scope of this Comment is limited to the FISA provisions that involve electronic surveillance of persons who may be international terrorists because these sections present the greatest danger to our privacy. Under the Act, a suspected group of international terrorists is a "foreign power" for purposes of invoking FISA's lax warrant provisions even though the group consists entirely of United States citizens.[9] This concern for United States citizens' privacy must not, however, belittle the importance of preserving the privacy rights of persons who are aliens. The fourth amendment[10] is applicable to persons who are not United States citizens.[11] Moreover, if the privacy interests of aliens are excessively infringed upon through the use of electronic surveillance, there will be direct and adverse consequences for the privacy rights of American citizens who are speaking with monitored aliens by means of instruments that are tapped.[12]

---

9. *See* 50 U.S.C.A. § 1801(a)(1)-(6) (West Supp. 1979). In order for persons not suspected of international terrorism to be a "foreign power," they must be either directed and controlled by a foreign government or "not substantially composed of" United States citizens or resident aliens. *Id.*

FISA applies to persons suspected of international, not domestic, terrorism. What differentiates international from domestic terrorism is that the former transcends national boundaries in some way. Surveillance of wholly domestic organizations that are believed to be engaged in, or preparing for, acts of domestic terrorism is apparently governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. On the bases of United States v. United States District Court, 407 U.S. 297 (1972), which held that the warrantless wiretapping of wholly domestic organizations for national security purposes was unconstitutional, and Congress' failure to enact a statute that prescribes a warrant procedure for the tapping of such organizations, it can safely be asserted that Title III is applicable to surveillance of wholly domestic organizations.

10. U.S. CONST. amend. IV.

11. Abel v. United States, 362 U.S. 217 (1960) (fourth amendment search and seizure principles are applicable to the search of a hotel room occupied by an alien suspected of espionage); United States v. Toscanino, 500 F.2d 267 (2d Cir., 1974) ("It is beyond dispute that an alien may invoke the Fourth Amendment's protection against an unreasonable search conducted in the United States.").

12. Information regarding contacts between members of Congress and foreign officials was picked up by FBI wiretaps and bugging devices and forwarded to Presidents Johnson and Nixon . . . .

> . . . None of the legislators was the direct target . . . but . . . instead they were overheard 'through the bureau's coverage of certain foreign establishments in Washington . . . .'
>
> Such eavesdropping is an example of a situation in which 'even properly authorized electronic surveillance directed against foreign targets . . . may result in possible abuses involving American Citizens.'

N.Y. Times, May 10, 1976, at 14, col. 4. *See also Foreign Intelligence Surveillance Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Pro-*

Modern terrorism is different from that of earlier ages in a very important respect. Today's rapidly developing technology has provided terrorists with a great deal of power.[13] Modern civilization has established a communications system that disseminates worldwide news of terrorists' acts,[14] has provided transport facilities that abet terrorists' ability to abscond,[15] and has centralized large numbers of persons in structures vulnerable to attack.[16] Most importantly, technology has produced sophisticated weapons to which terrorists have access[17] and has helped create a climate attuned to terrorism.[18] This increased power has contributed to the CIA's assessment that international terrorism will increase in the future[19] and commentators' beliefs that the world is entering an "Age of Terrorism."[20]

Anti-terrorism involves two strategies. The first requires that

cedures of the Judiciary, 95th Cong., 1st Sess. 91-92 (1977) [hereinafter cited as *1977 Judiciary Committee Hearings*].

13. *See* W. LINEBERRY, THE STRUGGLE AGAINST TERRORISM 37 (1977); Feary, *International Terrorism*, 74 DEP'T OF ST. BULL. 394, 395 (1976); Frank, *International Legal Action Concerning Terrorism*, 1 TERRORISM 187, 188 (1978).

14. W. LINEBERRY, THE STRUGGLE AGAINST TERRORISM 37 (1977); Feary, *International Terrorism*, 74 DEP'T OF ST. BULL. 394, 395 (1976).

15. *Id.*

16. Franck, *International Legal Action Concerning Terrorism*, 1 TERRORISM 187, 188 (1970).

17. It is generally conceded that individuals or groups with certain scientific and engineering skills could fashion a crude nuclear bomb with commercially available equipment plus the requisite amount of enriched uranium or plutonium. M. WILLRICH, and T. TAYLOR, NUCLEAR THEFT: RISKS AND SAFEGUARDS 13-21 (1974). *See* Smith, *The Plutonium Society: Deterrence and Inducement Factors*, 41 ALBANY L. REV. 251 (1977). This nuclear threat, however, must not overshadow the persistent danger of other types of advanced weaponry falling into the hands of terrorists. On September 5, 1973, police arrested five Arab terrorists preparing to shoot down a jetliner with two SA-7 heat-seeking missiles, each to be fired from a light shoulder launcher. W. LINEBERRY, THE STRUGGLE AGAINST TERRORISM 47 (1977). *See also* Javits, *International Terrorism: Apathy Exacerbates the Problem*, 1 TERRORISM 111, 112 (1978).

18. Because wars of aggression against the superpowers and other developed nations by smaller underdeveloped countries are usually expensive and long in duration, the possibility of small nations resorting to terrorism for purposes of coercing large powers must be given credence. The taking hostage of Americans in Iran by militant students with the support of the Iranian government is a startling example of the use of terrorism by a weaker nation against a superpower. *See* N.Y. Times, Nov. 25, 1979, § 4, at 1. *See generally* Milbank, *International and Transnational Terrorism: Diagnosis and Prognosis*, CIA RESEARCH STUDY 2 (1976) [hereinafter cited as CIA RESEARCH STUDY]. It has also been cogently suggested that the U.S.S.R. may use, or is using, surrogate terrorist techniques as an indirect means of warcraft against the West. *See generally* Sterling, *The Terrorist Network*, ATLANTIC, Nov., 1978 at 32.

19. *See* CIA RESEARCH STUDY, *supra* note 18, at 4-5.

20. CONTROL OF TERRORISM: INTERNATIONAL DOCUMENTS ix (Y. Alexander, M. Browne, and A. Nanes eds. 1979).

the public not be informed about the commission of the terrorists' overt act of destruction or victimization. Since terrorists' power is based on the fearful response to an act,[21] their leverage will not develop if the response is contained. That is, if the public does not experience fear, terrorism is negligible as a political force. There are two problems with this strategy. As a practical matter, today's alert and free media makes it difficult to prevent dissemination of news about the overt act of destruction.[22] In addition, this approach does nothing to prevent the terrorists' initial act of victimization. The second anti-terrorist strategy requires prevention of the act of violence. Because terrorists have the ability to commit devastating acts,[23] this latter strategy is obviously the sounder.

Active intelligence gathering is the most effective means by which initial acts of terrorism can be prevented.[24] Although intelligence work involves many techniques,[25] one of the most fruitful is that of wiretapping,[26] for it can acquire vast amounts of knowledge. Persons using the monitored line have no notice that a search is being conducted as they speak and all conversations,[27] inculpatory and exculpatory, are recorded.[28] Indeed, because of the difficulty of limiting the scope of a wiretap it has been suggested that electronic surveillance is inherently violative of the

21. *See* CIA RESEARCH STUDY, *supra* note 18, at 8.

22. *See* Alexander, *Terrorism and the Media*, 2 TERRORISM 55 (1979).

23. "U.S. Army Special Forces exercises have shown that nuclear weapons storage areas can be penetrated successfully without detection despite guards, fences, and sensors. Their example could obviously be followed by a daring and well-organized terrorist organization." Beres, *Terrorism and the Nuclear Threat in the Middle East*, 70 CURRENT HIST. 27 (1976).

24. Alexander, *Terrorism and the Media*, 2 TERRORISM 55 (1979); Feary, *International Terrorism*, 74 DEP'T OF ST. BULL. 395, 396 (1976); Kerstetter, *Terrorism and Intelligence*, 3 TERRORISM 109 (1979).

25. Examples include infiltration and mail opening. SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, Bk. II 94th Cong., 2d Sess., 31, 40 (1976).

26. *See generally* M. BRENTON, THE PRIVACY INVADERS (1964); M. PAULSEN, THE PROBLEMS OF ELECTRONIC EAVESDROPPING (1977).

27. Statistics released by the Administrative Office of the U.S. Courts show that the average court-ordered federal wiretap in 1976 involved the interception of 1,038 separate conversations between 58 persons over a period of an average of three weeks. *1977 Judiciary Committee Hearings, supra* note 12, at 74.

28. Minimization procedures that attempt to limit as far as possible the privacy invasion from electronic surveillance have been largely unsuccessful. *See* Shapiro, *The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment*, 15 HARV. J. LEGIS. 118, 195 (1978).

fourth amendment as a "general" search.[29]

The threat to civil liberties posed by wiretapping was recognized by Justice Brandeis in his dissent in *Olmstead v. United States*,[30] when he declared that "writs of assistance and general warrants are but puny instruments of tyranny compared to wiretapping."[31] The danger wiretapping presents to civil liberties[32] in the context of preventing international terrorism brings us to the gravamen of this Comment: the Foreign Intelligence Surveillance Act of 1978.[33]

FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

In 1940 President Roosevelt issued a memorandum to the Attorney General stating that warrantless electronic surveillance would be proper under the Constitution when "grave matters involving defense of the nation" were at stake.[34] The Attorney General, pursuant to Roosevelt's direction, began "to secure information by listening devices [directed at] the . . . communications of persons suspected of subversive activities. . . ."[35] The practice embodied in Roosevelt's memo was continued in successive administrations.[36]

The United States Supreme Court has not ruled on the constitutionality of executive authorization of warrantless wiretapping of foreign powers. *Katz v. United States*[37] held that electronic surveillance conducted on behalf of law enforcement is subject to fourth amendment restraints.[38] The question of whether the fourth amendment is applicable to wiretaps conducted for na-

29. *1977 Judiciary Committee Hearings, supra* note 12, at 77 (statement of John Shattuck, A.C.L.U.).

30. 277 U.S. 438 (1927).

31. 277 U.S. 471, 476 (Brandeis, J., dissenting).

32. *See generally 1977 Judiciary Committee Hearings, supra* note 12, at 2 (discussion of wiretapping abuses aimed at National Security Advisor Morton Halperin and civil rights leader Martin Luther King, Jr.).

33. 50 U.S.C.A. §§ 1801-1811 (West Supp. 1979).

34. *See* H.R. REP. NO. 95-1283, Pt. I, 95th Cong., 2d Sess. 15 (1978); S. REP. NO. 95-604, 95th Cong., 1st Sess. 7-8 (1977).

35. H.R. REP. NO. 95-1283, Pt. I, 95th Cong., 2d Sess. 15 (1978); S. REP. NO. 95-604, 95th Cong., 1st Sess. 7-8 (1977).

36. "Since the early 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of a judicial warrant." SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, Bk. II, 94th Cong., 2d Sess., 12 (1976).

37. 389 U.S. 347 (1967) (police had bugged a public phone booth and overheard defendant's conversations).

38. "[A]ntecedent justification [is] a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case." *Id.* at 359.

tional security purposes was explicitly reserved.[39] In *United States v. United States District Court*[40] the Supreme Court stated that electronic surveillance of wholly domestic organizations[41] in the name of national security is subject to judicial authorization. The Court refused, however, to extend its ruling to wiretaps involving foreign powers.[42] Neither the disposition of *Katz* nor that of *District Court* required resolving the question of whether an executive power to unilaterally wiretap foreign powers, and their suspected agents, is constitutional. The Supreme Court has, however, been petitioned for purposes of addressing the specific issue. In all cases certiorari was denied.[43]

The Supreme Court's reluctance to tackle the issue resembles a similar hesitancy on behalf of Congress prior to enactment of FISA. Title III of the Omnibus Crime Control and Safe Streets Act of 1968[44] was the first major statutory scheme dealing with wiretaps.[45] It permits issuance of a warrant allowing electronic surveillance if probable cause requirements are fulfilled.[46] The warrant procedures, however, are expressly inapplicable to wiretaps involving national security.[47] Indeed, FISA represents the first attempt by a coordinate branch of the national government to

39. "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Id.* at 358 n.23.

40. 407 U.S. 297 (1972) (United States charged anti-war demonstrators with destroying and conspiring to destroy government property).

41. "We use the term 'domestic organization' in this opinion to mean a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies." *Id.* at 309 n.8.

42. "The instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* at 308.

43. Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976); United States v. Butenko, 494 F.2d 593 (3rd Cir.), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418 (1973), *cert. denied*, 415 U.S. 960 (1974).

44. 18 U.S.C. § 2510 (1976), *as amended by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, tit. I, § 101, 92 Stat. 1783.

45. Section 605 of the Federal Communications Act of 1934, tit. VI, § 605, 48 Stat. 1103 (codified at 47 U.S.C. § 605 (1976)), was the first federal wiretap statute. It proscribed the interception and divulgence of wire communications without the consent of the sender, but it did not prohibit the mere interception of communications.

46. *See* 18 U.S.C. § 2518(3)(a)-(d) (1976).

47. 18 U.S.C. § 2511(3) (1976) (repealed by Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, tit. II, § 201(c), 92 Stat. 1797).

limit the ability of the executive to authorize warrantless electronic surveillance of suspected foreign powers and their agents.

FISA establishes a classification between United States persons and non-United States persons.[48] The warrant procedure for the former is more rigorous than that for the latter. "United States person" refers to United States citizens and resident aliens.[49] Non-United States person includes visiting foreign nationals.[50]

The special court shall enter an ex parte order approving the electronic surveillance of a non-United States person if there is probable cause to believe that the target "may" engage in "clandestine intelligence activities . . . contrary to the interests of the United States" on behalf of a foreign power.[51] Certain other findings must also be made.[52] This standard has the potential to bring various types of innocuous conduct within its purview. The judge need not find reasonable grounds to believe the target presents a danger to the security of the United States or is engaged in criminal activity. Moreover, the Act fails to give definitions for, or examples of, "clandestine intelligence activities" that are "contrary to the interests of the United States."[53]

A warrant approving surveillance of a United States citizen or resident alien shall be issued if there is probable cause to believe the target may engage in "clandestine intelligence gathering activities" on behalf of a foreign power that are violative of the criminal statutes of the United States.[54] The court must also find that certain other requirements have been fulfilled.[55] Again, "clandestine intelligence gathering activities" is undefined,[56] although the Act does provide the amorphous admonition that conduct protected by the first amendment[57] does not fall within the purview of such activities.[58] This standard is more demanding than that applied to non-United States persons in one significant respect. In the case of non-United States persons, the judge's findings need not include the possibility of criminal activity. With respect to United States persons, however, it must be shown that the target's activity "may" involve criminal activity.

48. 50 U.S.C.A. § 1801(b)(1) and (2) (West Supp. 1979). *See generally*, Peirce, *Does the Foreign Intelligence Surveillance Act of 1978 Infringe the Fourth Amendment Rights of Nonresident Aliens?*, 3 ASILS INT'L. L. J. 91 (1979).
49. 50 U.S.C.A. § 1801(i) (West Supp. 1979).
50. 50 U.S.C.A. § 1801(b)(1) (West Supp. 1979).
51. 50 U.S.C.A. §§ 1801(b)(1)(B), 1805(a)(3)(A) (West Supp. 1979).
52. *See* note 7 *supra*.
53. *See* 50 U.S.C.A. § 1801 (West Supp. 1979).
54. 50 U.S.C.A. §§ 1801(b)(2)(A), 1805(a)(3)(A) (West Supp. 1979).
55. *See* note 7 *supra*.
56. *See* 50 U.S.C.A. § 1801(a)(3) (West Supp. 1979).
57. U.S. CONST. amend. I.
58. 50 U.S.C.A. § 1805(a)(3)(A) (West Supp. 1979).

Issuance of a warrant[59] based on activity that "may" be criminal or "may" be contrary to the interests of the United States, depending on the target's status, permits electronic surveillance on the basis of a *possibility*.[60] To allow governmental intrusion on such a basis is unreasonable and, thus, violative of the fourth amendment because there is almost always a *possibility* that a given form of conduct will involve objectionable activity.[61] When *X* drives his automobile on the highway, there is a possibility that he is in the process of delivering a bomb. When *X* is speaking with his friends there is a possibility that he is discussing the commission of a planned hyjacking. Indeed, warrant criteria demanding the demonstration of only a *possibility* require that the judge be nothing more than a rubber stamp.

CONSTITUTIONALITY OF THE FISA STANDARD

The fourth amendment protects people from unreasonable searches and seizures by the state—a right "basic to a free society."[62] The policy behind this limitation on government is "to keep the state out of [areas where a reasonable expectation of

59. Electronic surveillance may be placed on anyone, regardless of their status, if the Attorney General determines that an "emergency situation" exists. In such a case, a warrant must be procured within 24 hours after the surveillance is instituted. 50 U.S.C.A. § 1805(e) (West Supp. 1979).

60. In the context of FISA, "may" means "expressing . . . a possibility." *See* THE OXFORD UNIVERSAL DICTIONARY 1221 (3d ed. 1955).

61. One commentator who found the FISA issuance criteria constitutional as a proper balancing of national security and the fourth amendment focused on whether it was constitutionally permissible to issue warrants when there is probable cause to believe the target is engaged in activity that does not necessarily involve *crime*. *See* Shapiro, *The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment*, 15 HARV. J. LEGIS. 119, 146-67 (1977). This is not the crucial issue in determining the constitutionality of FISA. Rather, the determinitive question is whether a *possibility* of undesirable activity that may or may not be criminal is sufficient for issuance of a warrant. *See* text accompanying notes 72-82 *infra*.

FISA states that the judge shall issue a warrant if he finds "probable cause to believe that the target . . . may" be engaged in certain activity. 50 U.S.C.A. §§ 1805(a), 1801(b) (West Supp. 1979). Use of the term "probable cause" does not cure the problem caused by the term "may." Resort to mathematics is illustrative. Assume a scale of 0 to 1 where certainty=1, probable cause=.75, justifiable suspicion (as defined in Terry v. Ohio, 392 U.S. 1 (1968)) =.50, and possibility=.25. When the "probable cause . . . may" language of FISA is presented in terms of this scale we get .75 × .25 or .18. The product of .18, which is less than possibility (.25), indicates that the use of the term "probable cause" (.75) actually makes the FISA warrant criteria require less than a possibility.

62. Wolf v. Colorado, 338 U.S. 25, 27 (1938).

privacy is enjoyed] until it has reason to believe that a specific crime has been or is being committed. . . ."[63] By authorizing executive officials to institute electronic surveillance whenever the special court agrees that there is a possibility of criminal activity or activity contrary to the interests of the United States, FISA fails to heed adequately the fourth amendment policy of preserving privacy and is, therefore, unconstitutional.

The Supreme Court has permitted governmental invasions of privacy in only a few instances in the absence of a finding of probable cause.[64] A two-pronged test has been developed by the Supreme Court for determining when a finding of probable cause is not necessary for a search to be constitutional.[65] The test requires that there be a strong public interest in conducting the search and that the search be limited.[66] It has been argued by the Justice Department that the FISA standard satisfies this test.[67] Such an argument is flawed. Although the first requirement is fulfilled because there is certainly a strong public interest in preventing acts of international terrorism, the second requirement is not satisfied. The scope of the search is not limited. In fact, electronic surveillance is one of the broadest forms of privacy invasion known.[68]

It has been suggested that Supreme Court dictum in *United*

63. Berger v. New York, 388 U.S. 41, 59 (1967).

64. The probable cause exception permitted in FISA must be distinguished from the exception to the fourth amendment that allows a search in the absence of a warrant. Dispensing with the procedural requirement of procuring a warrant, although significant, Coolidge v. New Hampshire, 403 U.S. 443 (1971), is not as threatening to privacy as the disregarding of the substantive requirement of probable cause. With the former the danger lies in eliminating the judgment of the neutral magistrate as to whether probable cause exists; with the latter a greater danger lies in removing the traditional basis for state intrusion altogether.

65. In Camara v. Municipal Court, 387 U.S. 532 (1967), it was held that administrative inspection of housing facilities was subject to the warrant requirements of the fourth amendment. The Supreme Court declined, however, to make a finding of probable cause necessary for issuance of a warrant. This latter part of the holding had a twofold basis: the strong public interest in eliminating unsafe and dangerous housing conditions and the limited invasion that such inspections pose to citizens' privacy. A similar analysis was employed in Terry v. Ohio, 392 U.S. 1 (1968). Therein, the Supreme Court stated that a governmental "stop and frisk" of a person when there is a reasonable suspicion of criminal activity, but no probable cause, is constitutional. The decision was based on the public interest in protecting police officers and the limited scope of the search. Other Supreme Court decisions permitting governmental intrusions in the absence of probable cause have used the reasoning of *Camara* and *Terry*. *See, e.g.*, United States v. Brigoni-Ponce, 422 U.S. 873, 881 (1975).

66. Terry v. Ohio, 392 U.S. 1 (1968); Camara v. Municipal Court, 387 U.S. 532 (1967).

67. *1977 Judiciary Committee Hearings, supra* note 12, at 15.

68. *See* notes 25-28 and accompanying text *supra*.

States v. United States District Court[69] may provide a constitutional justification for the FISA warrant criteria.[70] In *District Court* the Supreme Court recognized that the policy of preserving privacy may have to be compromised when in conflict with the policy of maintaining the nation's security. The case involved a criminal action charging certain persons with destroying or conspiring to destroy government property. The defendants contended that evidence obtained by the government through warrantless electronic surveillance must be disclosed in order for suppression motions to be brought. The Supreme Court agreed and held that wiretaps placed on wholly domestic organizations for purposes of domestic security are subject to prior judicial approval. Although the Court did not address the question of whether electronic surveillance relating to foreign affairs was subject to the fourth amendment, an aspect of the *District Court* analysis is pertinent to determining the constitutionality of the FISA standard. The Court noted that because there are "potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for crimes in Title III."[71] This statement permits the inference that a warrant procedure less rigorous than that in Title III is permissible when surveillance relating to foreign powers is contemplated. This language cannot, however, be used as a justification for FISA's warrant criteria. *District Court* stands for the proposition that the warrant criteria of Title III can be watered down when electronic surveillance relating to the nation's security is at issue, but it does not support the proposition that the fourth amendment's requirement of reasonableness can be abandoned when such surveillance is instituted. And, as shown above, warrant criteria based on a possibility are unreasonable.

Two Circuits have held that a probability of criminal activity need not be shown when the objective of the electronic surveillance is to gather intelligence relating to foreign powers.[72] In

69. 407 U.S. 297 (1972).

70. Shapiro, *The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment* 15 HARV. J. LEGIS. 119, 146-47 (1977).

71. 407 U.S. at 322.

72. Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976); United States v. Butenko, 494 F.2d 593 (3d Cir.), *cert. denied*, 419 U.S. 881 (1974).

United States v. Butenko[73] the Third Circuit upheld a conviction for conspiring to transmit to a foreign government information relating to the national defense of the United States. Some of the government's evidence had been procured through the use of warrantless electronic surveillance. Although the court held that the fourth amendment is applicable to wiretaps instituted to obtain information relating to foreign powers, the fourth amendment was held not to require prior judicial approval of the wiretap. Rather, the court decided that there need only be a post hoc determination of reasonableness if the defendant moves for divulgence. In determining "reasonableness" the court held that a finding of probable criminal activity was not necessary because the "primary purpose of these searches is to secure foreign intelligence information" and not to uproot crime.[74]

In *Zweibon v. Mitchell*[75] members of the Jewish Defense League, which was demonstrating against Soviet emigration policy, brought an action against the Attorney General and the FBI to recover damages sustained as a result of alleged unlawful electronic surveillance of the League's New York headquarters. The District of Columbia Circuit's analysis indicates that all foreign security wiretaps must be subject to prior judicial approval.[76] The court's holding, however, was not so broad. It found that a warrant must be secured before electronic surveillance for foreign intelligence purposes can be authorized unless the target is an agent of, or acting in collaboration with, a foreign power.[77] By requiring prior judicial approval, instead of permitting a post hoc determination of reasonableness, *Mitchell* differs significantly from *Butenko*.[78] There is, however, an important similarity be-

73. 494 F.2d 593 (3d Cir. 1975), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974).

74. 494 F.2d at 605.

75. 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

76. The court cogently dispensed with each of the following reasons the government submitted in support of immunizing such electronic surveillance from the fourth amendment: (1) lack of judicial competence to deal with foreign affairs data; (2) danger of security leaks; (3) the fact that such surveillance is not being used for criminal prosecutions, but only for "strategic" intelligence gathering; (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 might be enormous. 516 F.2d at 602, 633-52. *But see* United States v. Hung, No. 78-5177 (4th Cir. July 17, 1980). *See generally* Note, *Foreign Security Surveillance—Balancing Executive Power and the Fourth Amendment*, 45 FORDHAM L. REV. 1179, 1199 (1977); Note, *The Fourth Amendment and Judicial Review of Foreign Intelligence Wiretapping*: Zweibon v. Mitchell, 45 GEO. WASH. L. REV. 55 (1976).

77. 516 F.2d at 602.

78. Another difference between the two cases involves the determination of reasonableness. Under *Butenko* the surveillance is to be deemed reasonable if its primary purpose is to secure foreign intelligence information. 494 F.2d at 606. Un-

tween the two cases. Neither decision requires the examining court to consider the probability of criminal activity in determining the legality of the contemplated, or already instituted, electronic surveillance.[79] *Butenko* and *Mitchell* cannot, however, be used as a constitutional justification for the FISA warrant criteria. The *Butenko-Mitchell* doctrine is not germane to the crucial issue that must be resolved to determine the constitutionality of FISA's warrant criteria. The crucial issue is whether a warrant can issue on the basis of a *possibility*, not whether evidence of *criminality* is required for issuance.

In sum, it must be said that each of the available avenues for a constitutional justification of FISA's warrant criteria is plagued with roadblocks. The two-pronged test developed by the Supreme Court that requires a strong public interest and a limited search before the probable cause requirement can be abandoned is not satisfied by FISA. Electronic surveillance is not a limited form of search. In *United States v. United States District Court*[80] Supreme Court dictum indicates that the rigorous probable cause requirements of Title III can be mitigated, although the fourth amendment's requirement of reasonableness cannot be abandoned, when the wiretap involves national security. FISA cannot be justified by *District Court* because warrant criteria requiring only a possibility of undesirable conduct are unreasonable. Finally, FISA cannot be justified by the doctrine of *United States v. Butenko*[81] and *Zweibon v. Mitchell*.[82] *Butenko* and *Mitchell* stand for the proposition that a probability of criminal activity is not required when the object of the wiretap is not to prevent crime or apprehend criminals. *Butenko* and *Mitchell* do not support the idea that a warrant to wiretap can be issued on the basis of a *possibility* when the purpose of the surveillance is to acquire intelligence relating to foreign powers.

One more point should be made. The President does not have

---

der *Mitchell*, however, reasonableness cannot be found unless the ratio of expected relevant information to irrelevant information is high. 516 F.2d at 657. The latter test would appear to be more stringent than the former.

79. The *Mitchell* court stated that "it would appear to be proper to issue warrants . . . even though evidence of crime is neither sought nor likely to be uncovered." 516 F.2d at 656.

80. 407 U.S. 297 (1972).

81. 494 F.2d 594 (3d Cir. 1975), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1976).

82. 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

the inherent power to conduct warrantless electronic surveillance when gathering foreign intelligence. Because the FISA warrant criteria are unconstitutional, a new statute with acceptable warrant criteria is needed. In *United States v. Brown*[83] the Fifth Circuit held that the President had authority "over and above the Warrant Clause of the Fourth Amendment" to authorize warrantless electronic surveillance of foreign powers.[84] The decision is based on the President's inherent power to act in foreign affairs. *Brown* is erroneous. The doctrine of inherent executive power stems from *United States v. Curtiss-Wright*.[85] *Curtiss-Wright* involved the constitutionality of a congressional delegation of power to the President to declare illegal the sale of arms to certain foreign nations. The exercise of such a power by the President was held to be constitutional on a twofold basis: the congressional delegation of power coupled with the President's inherent power to act in foreign affairs.[86] The Supreme Court recognized the doctrine of inherent power in *Curtiss-Wright* as a matter of policy. To ensure the achievement of national goals in the international arena it was held that the President must have an independent freedom to act in the international field.[87] However, in *Youngstown Sheet & Tube Co. v. Sawyer*,[88] the Supreme Court established definite limits on the exercise of inherent executive power. *Youngstown* dealt with the constitutionality of President Truman's ordering of the steelworkers back to work in order to avoid a steel shortage during the Korean War. It was held that the President lacked the power to take such domestic action in the absence of a delegation of power from Congress. *Youngstown* stands for the doctrine that the executive cannot exercise inherent power when such causes a domestic infringement of rights. President Truman, in the absence of statutory approval, had deprived the steelworkers of their right to strike. Thus, under *Curtiss-Wright* as limited by *Youngstown* the President does not have the inherent power to institute warrantless wiretaps because there is a domestic infringement of privacy when one's communications are tapped without a warrant.

But, even if the President does have the inherent power to wiretap within the United States, there is no reason why this inherent executive power, like any other power of the national government, should not be subject to the fourth amendment. In

83. 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974).
84. *Id.* at 426.
85. 299 U.S. 304 (1936).
86. *Id.* at 319-20.
87. *Id.*
88. 343 U.S. 579 (1952).

Youngstown the Supreme Court stated that inherent executive power must be "exercised in subordination to [other] provisions of the Constitution."[89] In *Reid v. Covert*[90] any doubt about whether inherent executive power was exempt from the Bill of Rights was settled. The Supreme Court declared that executive agreements made pursuant to inherent executive power must observe constitutional prohibitions.[91]

CONCLUSION

The threat of international terrorism is real. Effective intelligence gathering through electronic surveillance is one of the most efficacious means available for preventing international terrorism and dismantling the threat it poses. Unfortunately, overzealous use of interception devices places privacy rights in jeopardy. In an effort to protect citizens' and aliens' privacy from this type of invasion, Congress passed the Foreign Intelligence Surveillance Act. This legislation requires, among other things, a warrant to be obtained before the communications of persons who may be international terrorists can be monitored. To procure a warrant to wiretap a United States citizen or resident alien, it must be shown that the target "may" be engaged in criminal activity on behalf of a foreign power. To wiretap a nonresident alien it must be shown that the target "may" be involved in activity contrary to the interests of the United States on behalf of a foreign power. Because these criteria permit wiretapping on the basis of a mere possibility of criminal activity or activity contrary to the interests of the United States, depending on the target's status, the Foreign Intelligence Surveillance Act is unconstitutional. The peril of international terrorism is not so omnipresent as to require such a surrender of our privacy.

CHIP PURDY

89. 299 U.S. at 320.
90. 354 U.S. 1 (1957).
91. *Id.* at 17.