UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 58 | Number 1 Article 9

10-1-1979

Criminal Procedure -- Foreign Intelligence Surveillance Act of 1978: A New Charter for Electronic Intelligence Gathering

Johnson A. Salisbury

ness, in turn, will enhance the overall fairness of the jury system.[124] With the prosecutor forbidden to use the peremptory to remove jurors solely because of their group association, fewer defendants will be tried by juries from which members of their racial, sexual or other cognizable group have been excluded. Also, fewer defendants will be able to exploit the peremptory challenge to produce a jury that gives them an advantage over both the state and other defendants not so situated. Instead of reflecting the judgment of a group shaped by the number of peremptory challenges available and the racial, sexual or similar characteristics of the defendant and the victim, the jury verdict following *Wheeler* is more likely to represent the true judgment of the community.[125]

CHRISTOPHER WHITMAN MOORE

Criminal Procedure—Foreign Intelligence Surveillance Act of 1978: A New Charter for Electronic Intelligence Gathering

Title III of the Omnibus Crime Control and Safe Streets Act of 1968[1] stands as the most comprehensive grant of judicial control over electronic surveillance to date. Section 802 of that Act, however, expressly disclaimed any intention of imposing restrictions upon the Executive when the national security is at stake.[2] The consequence was

124. *See* J. VAN DYKE, *supra* note 2, at xiii-xiv, 11-12.
125. *See id.*

1. Pub. L. No. 90-351, §§ 801-804, 82 Stat. 197 (1968). Section 802 of title III amended part I of title 18, United States Code, by adding a new chapter entitled "Chapter 119—Wire Interception and Interception of Oral Communication" (codified as amended at 18 U.S.C.A. §§ 2510-2520 (West 1969 & Cum. Supp. 1979)). Section 803 of title III amended § 605 of the Communications Act of 1934 (formerly codified at 47 U.S.C. § 605 (1964)), to conform with the new chapter, which was intended to be a comprehensive electronic surveillance statute. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-357, § 803, 82 Stat. 211 (codified at 47 U.S.C. § 605 (1976)). *See generally* S. REP. No. 1097, 90th Cong., 2d Sess. 89-109, *reprinted in* [1968] U.S. CODE CONG. & AD. NEWS 2112, 2177-97.

2. Pub. L. No. 90-351, § 802, 82 Stat. 197 (1968) (formerly codified at 18 U.S.C. § 2511(3) (1970)) (repealed 1978) provided that:

> 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 infor-

ten years of continued debate over whether this provision represented an affirmative grant of surveillance power to the President.[3] Although the United States Supreme Court has held that no exception to the warrant requirement is permitted when government surveillance is directed at wholly domestic threats to the national security,[4] the question of the existence of such an exception when foreign powers are involved has remained open. Congress has now intervened, however, by enacting the Foreign Intelligence Surveillance Act of 1978 (the Act).[5] By repealing the controversial section 802 of title III[6] and providing an exclusive charter[7] for the conduct of electronic surveillance[8] aimed at gathering

---

mation 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 authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

3. *See, e.g.*, United States v. United States Dist. Court (Keith), 407 U.S. 297 (1972); 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.) (en banc), *cert. denied*, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); United States v. Clay, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); United States v. Smith, 321 F. Supp. 424 (C.D. Cal. 1971) (mem.); United States v. Stone, 305 F. Supp. 75 (D.D.C. 1969) (mem.).

4. United States v. United States Dist. Court (Keith), 407 U.S. 297 (1972); *see* text accompanying notes 35-37 *infra*.

5. Pub. L. No. 95-511, §§ 101-301, 92 Stat. 1783 (codified at 50 U.S.C.A. § 1801 (West Cum. Supp. 1979)). The Foreign Intelligence Surveillance Act of 1978 was enacted following four prior, unsuccessful attempts to pass legislation regulating the use of electronic surveillance within the United States for foreign intelligence purposes. *See* S. 3197, 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. 2820, Surveillance Practices and Procedures Act of 1973, 93d Cong., 1st Sess. (1973); S. 4062, Freedom From Surveillance Act of 1974, 93d Cong., 2d Sess. (1974).

6. Pub. L. No. 95-511, § 201(c), 92 Stat. 1783 (1978).

7. Pub. L. No. 95-511, § 201(b), 92 Stat. 1783 (1978) (amending 18 U.S.C. § 2511(2) (1970)); *see* S. REP. No. 95-604, 95th Cong., 2d Sess. pt. 1, at 63-65, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS 5654, 5714-16. The legislators agreed, however, that

> the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional powers minus any Constitutional power of Congress over the matter."

H. CONF. REP. No. 95-1720, 95th Cong., 2d Sess. 35, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS 5798, 5814 (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)).

8. The term "electronic surveillance" is broadly defined by the Act to include the nonconsensual acquisition of all domestic radio and wire communications, Pub. L. No. 95-511, § 101(f)(1)-(3), 92 Stat. 1783 (1978) (codified at 50 U.S.C.A. § 1801(f)(1)-(3) (West Cum. Supp. 1979)), and the use of any surveillance device in the United States for acquiring information

foreign intelligence information,[9] Congress has attempted to balance the President's power to conduct foreign affairs and the need to protect individual liberties.

Under the Act, the Attorney General, upon general authorization of the President,[10] may approve applications[11] for review by a specially designated court for orders to conduct such electronic surveillance. Jurisdiction to review applications and grant orders lies with any one of seven district court judges appointed by the Chief Justice of the United States for staggered seven year terms.[12] Denials of such applications are to be appealed to a special three judge court of review and ultimately to the Supreme Court.[13]

Approval of applications requires a finding by the judge, based on the facts submitted by the applicant, that there is probable cause to believe that the target of the electronic surveillance is a "foreign power"[14] or an "agent of a foreign power"[15] and that the facilities or places at which the electronic surveillance is directed are being used or are about to be used by a foreign power or an agent of a foreign

---

"under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." *Id.* § 101(f)(4) (codified at 50 U.S.C.A. § 1801(f)(4) (West Cum. Supp. 1979)).

9. *Id.* § 101(e) (codified at 50 U.S.C.A. § 1801(e) (West Cum. Supp. 1979)) defines "foreign intelligence information" as

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

Thus information pertaining to a United States person must not only "relate to" these national defense, national security, or foreign affairs interests, but must also be "necessary to" that end in order to come within the concept of "foreign intelligence surveillance." Unfortunately, the legislative history does not satisfactorily distinguish these phrases. *See* S. REP. NO. 95-701, 95th Cong., 2d Sess. 31-33, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS 5723, 5750-52.

10. Presidential authorization need not accompany Attorney General approval of each application. 50 U.S.C.A. § 1802(b) (West Cum. Supp. 1979); *see* S. REP. NO. 95-604, *supra* note 7, at 42, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS 5693.

11. The required contents of an application are set forth at 50 U.S.C.A. § 1804 (West Cum. Supp. 1979).

12. *Id.* § 1803(a), (d).

13. *Id.* § 1803(b). The court of review is to be selected from among the federal district and court of appeals judges. *Id.*

14. "Foreign power" is defined by § 1801(a) of the Act as

power.[16] Furthermore, the judge must be satisfied that the surveillance procedures proposed by the applicant reasonably minimize the acquisition and retention, and prohibit the dissemination, of information concerning United States citizens to the extent that such minimization is consistent with the need for foreign intelligence information.[17] Finally, the executive branch must certify to the judge that the information sought is foreign intelligence information that cannot reasonably be obtained by normal investigative techniques.[18] The judge may not look beyond this certification unless the target is a United States person,[19] in

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

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

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

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

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

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

Id. § 1801(a).

15. The Act defines "agent of a foreign power" with respect to persons other than United States persons, *see* note 19 *infra*, to include officers or employees of foreign powers, members of international terrorist groups, and persons acting on behalf of foreign powers engaged in clandestine intelligence activities within the United States. 50 U.S.C.A. § 1801(b)(1) (West Cum. Supp. 1979). With respect to all persons, including United States persons, an "agent" is anyone who knowingly engages in clandestine intelligence gathering activities, sabotage, or international terrorism for a foreign power, or who knowingly aids or abets any person engaged in those activites. *Id.* § 1801(b)(2).

16. 50 U.S.C.A. § 1805(a)(3) (West Cum. Supp. 1979).

17. *Id.* § 1805(a)(4); *see id.* § 1801(h).

18. *Id.* § 1804(a)(7). Each application for an electronic surveillance order must include a certification

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that the purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought . . . ; and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques . . . .

The legislative history explains that the purpose of the certification requirement is to ensure careful consideration of the case by the responsible official and to avoid use of boilerplate language in the certification itself. S. REP. NO. 95-604, *supra* note 7, at 45, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5696-97.

19. The phrase "United States person" includes United States citizens, permanent resident aliens, unincorporated associations substantially composed of United States citizens or permanent resident aliens, and United States-based corporations. Specifically excluded are associations and corporations that are "foreign powers" under 50 U.S.C.A. § 1801(a) (West Cum. Supp. 1979). *Id.* § 1801(i).

which case he must find that the certification is not clearly erroneous.[20] Upon making the above findings, the judge must issue an order approving the use of electronic surveillance for foreign intelligence purposes.[21]

The Act expressly provides two exceptions to the general warrant requirements previously enumerated. A court order is not required for any electronic surveillance that is authorized by the President and certified by the Attorney General as being directed at communications exclusively between or among "official" foreign powers[22] or at acquiring technical intelligence from premises controlled exclusively by such foreign powers.[23] The Attorney General must further certify that there is no "substantial likelihood" that a United States person will be a party to the intercepted communcations[24] and that the surveillance will conform to the minimization procedures required under the Act.[25]

An emergency electronic surveillance authorized by the Attorney General is also excepted from the requirement of prior judicial authorization under certain limited circumstances.[26] To come within this exception, the Attorney General must determine that a factual basis supporting surveillance under the standards of the Act exists and that even "with due diligence" a prior court order cannot be obtained in

20. *Id.* § 1805(a)(5). Thus, in all cases in which a United States person is not a target of the surveillance, judicial review is limited to examination of the form, but not the substance, of the certification that only foreign intelligence information is sought; the judge may not "substitute [his] judgment for that of the executive branch officials." S. REP. NO. 95-604, *supra* note 7, at 48, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5700.

21. 50 U.S.C.A. § 1805(a). That the issuance of the order is mandatory when the judge makes the necessary findings under § 1805 is clear from a reading of the legislative history of the Act. *See* S. REP. NO. 95-604, *supra* note 7, at 47, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5698. The judge does have discretion, however, to modify the order in terms of the period of authorization and the minimization procedures. *Id.* The order itself must specify the target of the surveillance, the place or facilities against which the surveillance will be directed, the type of information sought, the means by which the surveillance will be effected, and the period of authorization. 50 U.S.C.A. § 1805(b)(1) (West Cum. Supp. 1979). The judge may authorize electronic surveillance for a period of up to ninety days. In the case of surveillance of a foreign government, faction of a foreign government, or entity openly controlled by a foreign government, the order may authorize surveillance for up to one year. *Id.* § 1805(d)(1). Extensions of any order require reapplication and new findings as required for the original order. *Id.* § 1805(d)(2).

22. 50 U.S.C.A. § 1802(a)(1)(A)(i) (West Cum. Supp. 1979). "Official" foreign powers include definitions (1), (2), and (3) within § 1801(a), *quoted in* note 14 *supra*.

23. *Id.* § 1802(a)(1)(A)(ii).

24. *Id.* § 1802(a)(1)(B). Further protection is provided by *id.* § 1801(h)(4), which requires that any communication of a United States person that is intercepted pursuant to warrantless surveillance under *id.* § 1802(a) must be destroyed within 24 hours unless a court order is obtained. *See* H. CONF. REP. NO. 95-1720, *supra* note 7, at 25, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5804.

25. 50 U.S.C.A. § 1801(a)(1)(C) (West Cum. Supp. 1979).

26. *Id.* § 1805(e).

time.[27] One of the judges designated under the Act must be notified at the time of the authorization, and an application for a court order approving the surveillance must be made to that judge within twenty-four hours.[28] If the application is denied or the surveillance is terminated without an order having been issued, any information obtained is inadmissible as evidence in any proceeding, and the judge may inform any United States person subject to the surveillance of its occurrence.[29]

Prior to the enactment of the Foreign Intelligence Surveillance Act of 1978, the only electronic surveillance legislation that specifically addressed the issue of Presidential authority in the national security area was Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[30] Section 802 of title III provided that nothing in title III or section 605 of the Communications Act of 1934[31] was to limit the President's constitutional 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."[32]

27. *Id.*

28. The Attorney General must make this application whether or not the surveillance is terminated within the 24 hour period or the information sought is obtained. S. REP. No. 95-604, *supra* note 7, at 52, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5703. The Attorney General must also ensure that the minimization procedures of the Act are followed. 50 U.S.C.A. § 1805(e) (West Cum. Supp. 1979).

29. 50 U.S.C.A. §§ 1805(e), 1806(j) (West Cum. Supp. 1979).

30. Title III was the congressional response to the Supreme Court decisions in Berger v. New York, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967). S. REP. No. 1097, *supra* note 1, at 27-28, *reprinted in* [1968] U.S. CODE CONG. & AD. NEWS at 2113. In *Berger*, the Court declared a New York eavesdropping statute unconstitutional and set forth the standards of reasonable search and seizure under the fourth amendment that such statutes would be required to meet. 388 U.S. at 58-60. The Court placed particular emphasis upon the requirement that police officers describe conversations sought with specificity, a factor bearing on the finding of probable cause. *Id.* at 57-58. In *Katz*, the Court overruled the "trespass" doctrine of Olmstead v. United States, 277 U.S. 438 (1928), and held that warrantless electronic interception of an individual's conversations is an unreasonable search and seizure within the meaning of the fourth amendment, even if no physical trespass is involved. 389 U.S. at 353. *Katz*, however, carefully excluded national security surveillances from its holding. *Id.* at 358 n.23. *See generally* Dash, *Katz—Variations on a Theme by Berger*, 17 CATH. U.L. REV. 296 (1968). Congress employed the constitutional standards delineated in *Berger* and *Katz* in drafting title III, which limits the use of all electronic surveillance to investigation of specified crimes by law enforcement officials authorized by a court order issued upon a showing of probable cause. *See generally* S. REP. No. 1097, *supra* note 1, at 96-107, *reprinted in* [1968] U.S. CODE CONG. & AD. NEWS at 2153-63; Note, *Wiretapping and Electronic Surveillance—Title III of the Crime Control Act of 1968*, 23 RUTGERS L. REV. 319 (1969).

31. Act of June 19, 1934, ch. 652, § 605, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 605 (1976)). The Act reads in pertinent part:

> [N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person . . . .

32. Pub. L. No. 90-351, § 802, 82 Stat. 197 (1968) (formerly codified at 18 U.S.C. § 2511(3) (1970)) (repealed 1978), *quoted in* note 2 *supra*.

Nor was there to be any limitation on the President's power to protect the nation against hostile acts of a foreign power, overthrow by force or other unlawful means, or any other clear and present danger to the structure or existence of the government.[33] The last line of section 802 provided for the introduction of evidence obtained by national security surveillance "where such interception was reasonable."[34] The scope of "reasonable" national security surveillances was thus an issue for judicial interpretation.

The Supreme Court addressed this issue only once. In *United States v. United States District Court (Keith)*,[35] the Court held that prior judicial approval is required for purely domestic security surveillance, even when there is fear of a direct threat to national security.[36] In reaching its decision, the Court held that title III was essentially neutral toward the President's constitutional powers and that the latter must be examined independently of the statute.[37] Accordingly, the Court adopted a balancing approach with the goal of accommodating both the President's duty to protect national security and the individual's right to privacy and free expression.[38]

Recognizing that national security surveillance served a legitimate governmental need, the Court first inquired whether prior judicial review was necessary to protect the first and fourth amendment rights involved.[39] The Court reasoned that unrestrained surveillance pursuant to the vague concept of "domestic security" posed a grave threat to the rights of privacy and political expression, and thus concluded that a total departure from the fourth amendment warrant requirement was not appropriate.[40] The Court next examined the compatibility of the warrant requirement with executive needs. After dismissing the government's arguments of judicial incompetence regarding internal security matters and the threat of security leaks, the Court reasoned that the additional burden imposed upon the government by pre-surveillance review was minimal and fully justified in light of the expected benefits of safeguarding constitutional rights.[41] The Court thus held that na-

33. *Id.*
34. *Id.*
35. 407 U.S. 297 (1972).
36. *Id.* at 323-24.
37. *Id.* at 308.
38. *Id.* at 314-15.
39. *Id.* at 315.
40. *Id.* at 320.
41. *Id.* at 321.

tional security surveillance in the domestic context does not constitute the type of special circumstance that justifies an exception to the warrant requirement.[42]

The Court in *Keith* specifically declined to address the issue of warrantless security surveillance involving foreign powers or their agents.[43] Since that decision, however, two lower federal courts have considered this question. Acknowledging the President's "inherent power" in the conduct of foreign affairs and the strong public interest in a continuous flow of foreign intelligence information, the United States Court of Appeals for the Fifth Circuit, in *United States v. Brown*,[44] and for the Third Circuit, in *United States v. Butenko*,[45] held that the prior review requirements of the fourth amendment are inapplicable to foreign intelligence surveillance. In neither case, however, did the court attempt to delineate the scope of this exception to the warrant requirement.[46] The consequence of these inconclusive decisions and of the silence of the Supreme Court was an uncertain and ambiguous exemption from prior judicial review for electronic surveillance of foreign powers and their agents within the United States.[47]

Enactment of the Foreign Intelligence Surveillance Act of 1978 has filled the gap left by title III and answered the question avoided by the Supreme Court. By providing a specific charter for the conduct of

42. *Id.*

43. *Id.* at 321-22.

44. 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974).

45. 494 F.2d 593 (3d Cir. 1974) (en banc), *cert. denied*, 419 U.S. 881 (1975).

46. The *Butenko* court even suggested that a case-by-case application of this exception should be left to the "good faith" of the Executive, subject to the sanctions available during post hoc review. 494 F.2d at 605.

Furthermore, the facts of the two cases provide little assistance in distinguishing domestic security surveillance from surveillance in the foreign context for the purposes of this warrant clause exception. In *Brown*, defendant was convicted under the Federal Firearms Act for transporting firearms interstate while under indictment. The warrantless foreign intelligence wiretaps challenged by defendant were found to be both lawful and unrelated to the prosecutor's case. Consequently, the purpose and contents of the surveillance remained undisclosed. 484 F.2d at 426. In *Butenko*, defendants were convicted of conspiring to transmit national defense information to a foreign government. This activity was so clearly within the ambit of "foreign intelligence" that the court's decision to find the warrantless surveillance lawful did little to clarify the domestic intelligence-foreign intelligence distinction.

47. The ambiguous situations would be those in which a domestic organization's actions have a significant impact on foreign affairs, or a substantial portion of the group's members are foreign or foreign nationals. Would these organizations properly fall within the *Brown-Butenko* exception to the warrant clause requirement, and if so, what is the dividing line between significant and insignificant impact or substantial and insubstantial portions? The United States Court of Appeals for the District of Columbia Circuit has rendered its opinion on the first situation. In Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1973), *cert. denied*, 425 U.S. 944 (1976), the court held that warrantless surveillance of a domestic organization may not be justified on the ground that the organization's activity "affected foreign relations." *Id.* at 653.

foreign intelligence surveillance by the government, Congress has come down clearly on the side of careful judicial supervision. Furthermore, the Act significantly limits the warrant clause exception suggested by the lower federal courts.[48]

Evaluation of the warrant requirements of the Act might best be made along the lines of the balancing approach adopted by the Supreme Court in *Keith*. Thus the utility of the Act's warrant requirement in protecting the constitutional rights of individuals subjected to surveillance[49] can be balanced against the extent to which those warrant requirements impede the legitimate functions of the government in gathering necessary foreign intelligence information.[50]

An important goal of the fourth amendment warrant requirement is to ensure careful consideration and justification by the government of the need for the particular surveillance.[51] Only in this manner will all questionable or illegal surveillances come to light.[52] The Act addresses this goal by requiring that each application for an order authorizing electronic surveillance set forth the identity of the surveillance target and the justification for believing that the target is a foreign power or agent of a foreign power[53] and be accompanied by a supported certification that the information sought is foreign intelligence

48. *See* notes 44-47 and accompanying text *supra*.

49. The suggestion of the Supreme Court in *United States Dist. Court (Keith)* that both first and fourth amendment rights are threatened by electronic surveillance for the purpose of domestic security, *see* notes 39-40 and accompanying text *supra*, is no less applicable in the foreign intelligence field. To the extent that the surveillance intercepts communications of political dissenters, for example, first amendment rights are implicated. The chilling effect upon the exercise of these rights as a result of such surveillances is no less likely in light of the objection that foreign security surveillances are targeted exclusively toward foreign agents or organizations. An innocuous domestic group may become a target based upon the existence of a single foreign agent among its membership or a suspicion of foreign ties.

50. Indeed, the legislative history invites this method of analysis: "[The Act] is designed to permit the Government to gather necessary foreign intelligence information by means of electronic surveillance but under limitations and according to procedural guidelines which will better safeguard the rights of individuals." S. REP. No. 95-604, *supra* note 7, at 9, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5660.

51. *See, e.g.*, Camara v. Municipal Court, 387 U.S. 523, 528 (1967) ("The basic purpose of [the fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."). *See generally* Note, *Foreign Security Surveillance and the Fourth Amendment*, 87 HARV. L. REV. 976, 985-92 (1974).

52. In the absence of a warrant requirement a large number of surveillances go unreviewed, unless the target of the surveillance becomes the defendant in a criminal prosecution and the government attempts to introduce the fruits of the surveillance into evidence. This is particularly true in the case of national security surveillance, which tends to be "strategic" in nature and directed toward general information gathering. United States v. United States Dist. Court (Keith), 407 U.S. 297, 322 (1972).

53. *See* notes 14-16 and accompanying text *supra*.

information unobtainable by normal investigative techniques.[54] In reviewing the application for an order, however, the judge need only find "probable cause" to believe that the target is a foreign power or an agent of a foreign power. Unless that target is a United States person, the judge may not "go behind" the certification to determine whether the desired information is actually foreign intelligence information.[55]

The traditional view of the fourth amendment's probable cause requirement is that authorization of a warrant must be based on probable cause to believe that "the evidence sought will aid in a particular apprehension or conviction."[56] Clearly, the probable cause requirements of the Act diverge from this traditional interpretation. The Act focuses the judicial finding upon the target of the surveillance, not the evidence sought. Consequently, the fourth amendment's prohibition against general warrants may be threatened. The certification that the surveillance seeks only foreign intelligence information places minimal limitations on the scope of the intrusion into communications of the targeted person or group.[57] Essentially, the government has the right under a judicially approved order, subject to the minimization requirements, to intercept conversations continuously or at random for at least ninety days in order to gather all relevant "foreign intelligence information."[58]

Two arguments can be made, however, to justify this deviation from the strict probable cause standard. First, although the probable cause finding of the Act is based on the mere identification of the target as a foreign power or an agent of a foreign power, the terms are defined to limit foreign intelligence surveillance of United States persons to situations involving the commission of a crime. The term "agent of a foreign power" includes only those United States persons knowingly engaged in criminal activity against the United States; therefore, a

54. *See* notes 18-20 and accompanying text *supra.*

55. *See* note 20 *supra.*

56. Warden v. Hayden, 387 U.S. 294, 307 (1967); *see* Berger v. New York, 388 U.S. 41, 56-59 (1967).

57. Verification that the information sought is "foreign intelligence information," the focus under a traditional probable cause inquiry, is permitted only if the target of the surveillance is a United States person. *See* notes 18-20 and accompanying text *supra.* Even in that event, the judge is limited to a "clearly erroneous" standard in reviewing the certification. *See id.*

58. The right to conduct continuous surveillance is a tremendous power, permitting law enforcement officers to intrude upon the rightfully private aspects of a person's life in the search for criminal activity. *See* A. WESTIN, PRIVACY AND FREEDOM 62 (1967). Such a broad grant was found unconstitutional by the Supreme Court in *Berger v. New York*, 388 U.S. 41 (1968), and led the Court to require that the conversations sought by the surveillance be described with specificity in the finding of probable cause. *Id.* at 58-59.

judge must find probable cause to believe that a United States person is committing a crime against the federal government before he can find that that person is an "agent." The probable cause requirement thus appears to be met in situations involving United States persons, although the information sought from the surveillance will not necessarily be used in a particular criminal prosecution.

This argument, however, cannot be made with respect to aliens. An alien need not be engaged in criminal activity to fall within the statutory definition of "agent;" he need only be acting within the United States as an officer or employee of a foreign power or engaged in "clandestine intelligence activities . . . contrary to the interests of the United States."[59] The probable cause requirements with regard to aliens under the Act thus deviate from the traditional formulation of probable cause as a belief that the evidence sought is directly related to a specific criminal activity. In light of the recent trend by the Supreme Court toward full fourth amendment protection for aliens,[60] the Act's probable cause requirements for aliens are of questionable constitutional validity.[61] Furthermore, the nonspecific nature of this provision increases the likelihood that the conversations of United States persons lawfully associating with the alien "agents" will be indiscriminantly intercepted.

The definition of "foreign power" suffers from similar defects. Primarily included are foreign governments themselves or factions that are essentially extensions of foreign governments and organizations en-

59. 50 U.S.C.A. § 1801(b)(1)(B) (West Cum. Supp. 1979).

60. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973) (warrantless search of alien's automobile by roving patrol 25 miles north of Mexican border declared unconstitutional because "[i]n the absence of probable cause or consent, that search violated the petitioner's Fourth Amendment right to be free of 'unreasonable searches and seizures' "); Graham v. Richardson, 403 U.S. 365, 371-72 (1971) ("classifications based on alienage, like those based on nationality or race, are inherently suspect and subject to close judicial scrutiny"); Au Yi Lau v. United States Immigration & Naturalization Serv., 445 F.2d 217, 223 (D.C. Cir. 1971) ("aliens in this country are sheltered by the Fourth Amendment in common with citizens"). *But see* Abel v. United States, 362 U.S. 217, 232-34 (1960) (dictum) (arrest of alien prior to deportation proceeding on "administrative warrant" that would not have satisfied the fourth amendment was constitutionally valid). *See generally* Gordon, *The Alien and the Constitution*, 9 CALIF. W.L. REV. 1 (1972).

61. The framers of the Act were cognizant of this discrepancy in treatment of United States persons and aliens. S. REP. NO. 95-604, *supra* note 7, at 20-21, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5671-73. Their justification was that, given the specificity of the two categories within the definition of "agent" and the compelling national security interests, the bifurcated standard is lawful. *Id.* Aliens who are officers or employees of a foreign power are considered "likely sources of foreign intelligence information" and thus reasonable targets, even in the absence of participation in criminal activity. *Id.* at 20, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5671. Furthermore, those aliens engaged in "clandestine intelligence activities" for a foreign power must do so in a manner harmful to national security to be considered agents under the Act. *Id.* at 21-22, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5673.

gaged in terrorist or espionage activities for a foreign government.[62] Surveillance of communications between members of the first group is exempt from the requirement of prior judicial review, provided no United States person is involved.[63] To the extent that this group includes foreign embassies and consulates within the United States, an exemption based on this definition is reasonable.[64] This first group of "foreign powers," however, also includes any "faction of a foreign nation . . . , not substantially composed of United States persons"[65] and any "entity" that is openly controlled by a foreign government.[66] The definition is thus sufficiently ambiguous to include virtually any foreign affiliated organization regarded by the United States government as a potential threat to national security.[67] This broad discretion in the use of warrantless surveillance therefore threatens the constitutional rights of all aliens and United States persons lawfully associated with such organizations.

Ironically, the second group of organizations included within the definition of foreign power—those engaged in terrorism or espionage for a foreign government[68]—are never exempted from the judicial review requirements of the Act, even though such organizations are more clearly involved in criminal activity within the United States than are

62. *See* note 14 *supra.*

63. *See* notes 22-25 and accompanying text *supra.*

64. In balancing the competing interests, it seems clear that the government's claim of reasonableness would be easily supported in such surveillances. Surveillances of these targets will likely be very productive and easily justifiable on national security grounds. Furthermore, the potential danger to privacy interests from warrantless surveillance of embassies and consulates is minimal or nonexistent. First, the interests of United States persons are not involved. *See* note 24 and accompanying text *supra.* Second, the interests of embassy or consulate personnel are less deserving of full constitutional protection. An embassy compound is regarded as sovereign territory of the represented foreign nation and constitutional protection does not extend to the interest of aliens on foreign soil. Furthermore, embassy personnel, given the nature of their work, which usually includes surveillance of United States targets, have less "expectation of privacy," *see* Katz v. United States, 389 U.S. 347, 353 (1967), than other aliens residing or working within the United States.

65. 50 U.S.C.A. § 1801(a)(2) (West Cum. Supp. 1979).

66. *Id.* § 1801(a)(3).

67. With respect to the "entity" definition, the legislative history suggests that the "question whether a group, commercial enterprise, or organization comes within the scope of this definition is one for the court to answer on the basis of a probable cause standard." S. REP. No. 95-701, *supra* note 9, at 17, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5736. If, however, the surveillance satisfies the requirements of 50 U.S.C.A. § 1802(a) (West Cum. Supp. 1979), *see* text accompanying notes 22-25 *supra*, and is targeted toward such an "entity," the surveillance order is not subject to review by the court. *See* 50 U.S.C.A. § 1802(b) (West Cum. Supp. 1979).

68. 50 U.S.C.A. § 1801(a)(4), (6) (West Cum. Supp. 1979). The legislative history explains that the *id.* § 1801(6) definition of "entity that is directed and controlled by a foreign government" covers those situations in which the "entity" is actually a "cover for espionage activities." S. REP. No. 95-604, *supra* note 7, at 20, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5671.

other organizations that may be exempted. The one problem that arises with respect to the Act's coverage of this second group is that the "foreign based political organizations"[69] provision, which provides for surveillance based upon the organization's status per se, is clearly in contravention of the traditional probable cause formulation.[70]

The second, and perhaps better, argument justifying the Act's deviance from traditional probable cause standards is derived from the suggestion by the Supreme Court in *Keith* that standards of review applicable to domestic security surveillance may be less stringent than those prescribed by title III for surveillance of "ordinary" crime.[71] The Court recognized that the targets of security surveillances are often less readily identifiable than the targets of other title III surveillances, and consequently, the surveillance itself must be broader in scope. The traditional formulation of probable cause would thus be too restrictive for effective security surveillance.

Although the Court in *Keith* did not address the issue, this argument appears to be equally applicable to the foreign intelligence surveillance context.[72] The foreign nature of a threat indicates that it can never be fully eliminated, as can a domestic threat, by way of criminal prosecution. Therefore, the government must necessarily be interested in ongoing, "strategic" intelligence gathering. Subjecting such surveil-

69. 50 U.S.C.A. § 1801(a)(5) (West Cum. Supp. 1979).

70. This provision harks back to the Internal Security Act of 1950, ch. 1024, § 22, 64 Stat. 987 (codified as amended in scattered sections of 8, 18 U.S.C.), which designated the Communist Party as a forbidden organization and permitted deportation of past and present alien members. Although the Supreme Court upheld the constitutionality of the Internal Security Act as not violative of due process, Galvan v. Press, 347 U.S. 522 (1954), a requirement of "meaningful membership" was developed in order to protect casual or unwitting Communist Party members from deportation. Gastelum-Quinones v. Kennedy, 374 U.S. 469, 473-74 (1963); Rowoldt v. Perfetto, 355 U.S. 115, 120 (1957). Moreover, the Court has recently adopted an attitude of strict construction toward deportation statutes. *See* note 60 *supra*.

To the extent that the Court continues or extends this cautious attitude toward the denial of certain constitutional protections to aliens, *see* Gordon, *supra* note 60, at 32, use of the "foreign-based political organization" definition within the Foreign Intelligence Surveillance Act as a basis for finding probable cause may be of questionable constitutional validity. Of the six alternative definitions of "foreign power," *see* note 14 *supra*, "political organization" is the least consistent with the particularized probable cause requirement since there is no proof of illegal activity required. In contrast, the Internal Security Act of 1950 provision forbidding membership in the Communist Party was based on an express declaration of the illegality of that organization. Subversive Activities Control Act of 1950, ch. 1024, § 2, 64 Stat. 987.

71. United States v. United States Dist. Court (Keith), 407 U.S. 297, 322 (1972). The Court, however, did not suggest an alternative probable cause standard.

72. This argument assumes that foreign intelligence surveillance is no more offensive to personal rights than domestic surveillance. To the extent that the former involves only nonresident aliens and foreign agents not deserving of first and fourth amendment protection, foreign intelligence surveillance may even be less offensive. *But see* Note, *supra* note 51, at 985-88; note 60 and accompanying text *supra*.

lances to a probable cause standard of review based upon the goal of an identifiable prosecution would again be too restrictive for effective information gathering.

The Supreme Court has allowed lower standards of probable cause in other, noncriminal contexts. Maintenance of effective regulatory schemes, for example, often requires periodic inspections to assure compliance by the regulated class. The Court has recognized that, while the fourth amendment is applicable to administrative searches,[73] the goals of these regulations may well be frustrated if the inspections are permitted only in response to actual or suspected violations. This is certainly true in the contexts of housing codes[74] and the Occupational Safety and Health Act,[75] which are designed to prevent dangerous living and working conditions from developing. Effective enforcement of these regulations consequently requires periodic inspections of broad segments of the regulated class. The Court has responded to these governmental needs by holding that a relaxed standard of probable cause, based upon a showing that "reasonable legislative or administrative standards for conducting an area inspection are satisfied with respect to a particular dwelling,"[76] is sufficient for the conduct of certain administrative searches.[77] The Court has reasoned that this formulation of probable cause is not only necessary to protect the governmental interests represented by the regulatory statutes, but is also sufficient to protect the privacy interests affected by the administrative inspections, which have been discounted to an extent by the Court because of the noncriminal nature of the inspections.[78]

The relative interests at stake under a program of national security

73. Marshall v. Barlow's, Inc., 436 U.S. 307, 324 (1978). *Barlow's* is the most recent pronunciation by the Supreme Court on the application of fourth amendment protections to administrative searches conducted pursuant to federal regulatory statutes. The standard was established in See v. City of Seattle, 387 U.S. 541 (1967), and Camara v. Municipal Court, 387 U.S. 523 (1967), in which the Court held that warrants were required for the conduct of municipal housing code inspections. 387 U.S. at 542; 387 U.S. at 534. Since the holdings in these two cases were limited to their facts, however, the Court was free to fashion a different conclusion when reviewing warrantless inspections of federally licensed businesses. *See, e.g.*, United States v. Biswell, 406 U.S. 311, 316 (1972), in which the Court reasoned that the pervasiveness of the regulatory schemes diminished the petitioner's claim of privacy. *Barlow's* also involved a regulated business, subjected to Occupational Safety and Health Act inspections. In that case, however, the Court refused to expand the exception to the *Camara/See* rule, and held that warrantless inspections pursuant to federal regulatory schemes are permissible only in certain narrow circumstances. 436 U.S. at 313-14; *see* Note, 57 N.C.L. REV. 320 (1979).

74. *See* Camara v. Municipal Court, 387 U.S. 523, 535-36 (1967).

75. *See* Note, *supra* note 73, at 331.

76. Camara v. Municipal Court, 387 U.S. 523, 538 (1967).

77. *Id.*; Marshall v. Barlow's, Inc., 436 U.S. 307, 320-21 (1978).

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

surveillances differ substantially, however, from those involved in administrative inspections. On the individual's side of the balance, first as well as fourth amendment rights are threatened if citizens are deterred from associating with activities or organizations that the government may suspect of being potential security threats and thus likely surveillance subjects.[79] Also, security surveillances, unlike administrative searches, often lead to criminal prosecutions, further threatening the interests of individuals subjected to surveillance. Although these considerations seem to support the need for the traditional, particularized standard for probable cause in order to protect the public from unreasonable surveillances, the competing governmental interests militate in favor of quite the opposite conclusion. As suggested above, limiting security surveillances to instances in which there was probable cause to believe that the surveillance would uncover criminal evidence might frustrate the goals of foreign intelligence gathering. Especially in matters of military preparedness, strategic intelligence gathering is necessary to understand the development of a foreign power's posture in relation to the United States. In this light, a relaxed standard of probable cause is necessary to permit periodic or continuous intelligence gathering.

The probable cause formulation contained in the Act arguably reconciles these competing interests. This formulation protects the rights and interests of individuals by permitting surveillance of only those targets that fall within a specified class of "foreign powers" or "foreign agents." If these classes are sufficiently narrow in scope, then innocent persons are protected against privacy invasions. Once the court finds probable cause to believe that the target is within one of the designated classes, the surveillance is unrestricted, except with respect to minimization of intrusion and duration. Thus the government is not hindered by requirements of proof that criminal evidence is sought. Finally, this formulation of probable cause is arguably consistent with the administrative probable cause standard that the Supreme Court has found to be valid. Both are based on the definition of a class of targets rather than upon a showing that criminal evidence is sought, both can be justified by overriding government needs, and both govern "searches" regulated by legislative guidelines and standards.[80]

79. *See generally* A. WESTIN, *supra* note 58, at 57-63.

80. These legislative standards provide a check against governmental abuse of the authority available under the relaxed probable cause formulations and distinguish intelligence surveillance from ordinary search and seizure, in which the officer exercises a greater degree of discretion in executing the warrant.

The extent to which interposition of prior judicial review by the Act impedes the President in the performance of his constitutional obligations to provide for national security may be assessed in terms of the practical objections asserted by several courts: problems of delay,[81] concerns about secrecy,[82] and the complexity of foreign intelligence issues and the ability of judges to deal with them.[83]

The first objection arises when fulfillment of the warrant requirement prevents initiation of a surveillance immediately. The conceivable result is the failure to intercept crucial communications during the period of delay. The delay may result from the necessity of presenting technical information for review by a judge who is unfamiliar with it and from the need for additional precautions against security leaks. The Act responds to this objection in two ways. First, the designation of seven federal judges, with instructions to handle all warrant applications as expeditiously as possible, creates a reviewing court whose expertise in the area of foreign intelligence surveillance can only increase over time.[84] Second, the Act provides a narrowly drawn exception to the warrant requirement for cases of emergency.[85] This exception is comparable to the one permitted in ordinary criminal cases in which destruction or removal of evidence is imminent.[86]

The second argument asserted against the warrant requirement is that secret information presented for judicial review may easily be "leaked." Although the Court rejected this argument in *Keith*,[87] the potential danger may be greater in the foreign security context than in the domestic context. Certainly the contents of the certification and the judicial finding of probable cause probe deeply into information that, if revealed, would threaten the safety and continued effectiveness of government agents, particularly those operating abroad.[88] The Act goes far in minimizing the number of persons with access to security information, however, because only one of the seven designated judges re-

81. United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (en banc), *cert. denied*, 419 U.S. 881 (1974).

82. United States v. United States Dist. Court (Keith), 407 U.S. 297, 319 (1972).

83. United States v. Butenko, 318 F. Supp. 66, 72 (D.N.J. 1970), *aff'd*, 494 F.2d 593 (3d Cir.), *cert. denied*, 419 U.S. 881 (1974).

84. The countervailing consideration is that a delay may occur in reaching one of those seven judges.

85. *See* notes 26-29 and accompanying text *supra*.

86. *See* Carroll v. United States, 267 U.S. 132, 153 (1925).

87. 407 U.S. at 320-21.

88. *See* S. REP. NO. 95-604, *supra* note 7, at 47, *reprinted in* [1978] U.S. CODE CONG. & AD. NEWS at 5698-99.

views a particular application and because the proceedings must be conducted ex parte. Further precautions not specified by the Act may also be taken to protect against security leaks; for example, the names of informants or secret agents need not be revealed[89] and the Justice Department might supply all of the necessary clerical assistance.[90]

The third concern with the burden of the warrant requirement is the possibility of judicial error in the review of complex foreign intelligence issues. The judiciary's expertise in determining what constitutes "foreign intelligence" is limited; judges are more comfortable deciding whether the traditional elements of probable cause—evidence of a crime—are present. Here again, the designation of seven judges with the duty of reviewing all government applications provides a safeguard against errors inasmuch as judicial expertise will probably increase with experience. Furthermore, the finding of probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power is governed by fairly clear and manageable, albeit broad, standards. Only when the target is a United States person must the judge "look behind" the government's certification that the information sought is "foreign intelligence information." Even then, the judge need only find that the certification is not "clearly erroneous"; he will most likely defer to the greater expertise of the government officials and grant any application that is colorable. Indeed, the Act specifically exempts those surveillances that are clearly directed toward communications between specifically enumerated foreign powers alone. These surveillances—embassy taps and bugs for example—are logically left outside the scope of the warrant requirement because of the overriding governmental interests.[91]

The Act represents a minimal burden upon the governmental conduct of foreign intelligence gathering—indeed, one may wonder whether the process may eventually become a mere "rubber-stamp," with the constitutional rights of individuals no more protected than in the absence of a warrant requirement. This result, however, is unlikely. The possibility of even an occasional rejection of a government application should be sufficient to force officials to carefully justify their activities, especially with respect to the more closely scrutinized surveillances of United States persons. Nevertheless, the flexibility in-

89. *See* United States v. Ventresca, 380 U.S. 102 (1965) (affidavit submitted for purpose of establishing probable cause need only demonstrate affiant's belief that informant was credible and his information reliable; informant's identity need not be disclosed).

90. *See* 407 U.S. at 321.

91. *See* note 64 *supra*.

corporated into the Act to accommodate governmental interests places great responsibility upon the court to construe the specified classes of "foreign powers" and "foreign agents" quite narrowly. Only by limiting the definitions to individuals and groups clearly engaged in criminal activity or to those otherwise undeserving of full constitutional protection will the statutory standard arguably comport with the traditional notion of probable cause.[92] The conduct of the district court judges appointed to review applications under the Act will thus determine whether the Act provides a viable means of arresting the erosion of constitutional rights that accompanies the use of electronic surveillance as a means of gathering foreign intelligence information.

JOHNSON A. SALISBURY

92. *See* notes 56-70 and accompanying text *supra.*