Order Code RL30465

CRS Report for Congress

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance

Updated September 18, 2001

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Distributed by Penny Hill Press

http://pennyhill.com

Prepared for Members and Committees of Congress

Congressional Research

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance

Summary

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, provides a statutory framework for electronic surveillance in the context of foreign intelligence gathering. In so doing, the Congress sought to strike a delicate balance between national security interests and personal privacy rights. This report will examine the detailed statutory structure provided by this act and related provisions of E.O. 12333. This report is current through the changes to FISA in P.L. 106-567, Title VI (Dec. 27, 2000).

Contents

Introduction 1

Executive Order 12333 4

The Foreign Intelligence Surveillance Act 5
The Statutory Framework 5

Conclusion 20

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance

Introduction

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests.[1] The stage was set for legislation to address these competing concerns in part by Supreme Court decisions on related issues. In *Katz v. United States*, 389 U.S. 347 (1967), the Court held that the protections of the Fourth Amendment extended to circumstances involving electronic surveillance of oral communications without physical intrusion.[2] The *Katz* Court stated, however, that its holding did not extend to cases involving national security.[3] In *United States v. United States District Court*, 407 U.S. 297 (1972) (the *Keith* case), the Court regarded *Katz* as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[4] Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

> The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from

---

[1]The Fourth Amendment to the United States Constitution states:

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

[2]*Katz v. United States*, 389 U.S. 347, 353 (1967).

[3]*Id.*, at 359, n. 23.

[4]*United States v. United States District Court*, 407 U.S. 297, 313-14 (1972).

> unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.[5]

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.[6] Justice Powell emphasized that the case before it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country."[7] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents."[8] However, the guidance which the Court provided in *Keith* with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. The *Keith* Court observed in part:

> . . . We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes. Given these 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 specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. . . . It may be that Congress, for example, would judge

---

[5]407 U.S. at 299.

[6]*Id.*, at 391-321. Justice Powell also observed that,

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961). . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . . .

[7]*Id.*, at 308.

[8]*Id.*, at 321-22.

> that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . .; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.[9]

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom, Ivanov v. United States*, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."

With the passage of the Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified as amended at 50 U.S.C. § 1801 *et seq.*, Congress sought to strike a delicate balance between these interests when the gathering of foreign intelligence involved the use of electronic surveillance.[10] Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12333.[11] This report will examine the provisions of FISA

---

[9]407 U.S. at 323-24.

[10]For an examination of the legislative history of P.L. 95-511, see S. Rept. 95-604, Senate Committee on the Judiciary, Parts I and II (Nov. 15, 22, 1977); S. Rept. 95-701, Senate Select Committee on Intelligence (March 14, 1978); H. Rept. 95-1283, House Permanent Select Committee on Intelligence (June 8, 1978); H. Conf. Rept. 97-1720 (Oct. 5, 1978); Senate Reports and House Conference Report are reprinted in 1978 *U.S. Code Cong. & Admin. News* 3904.

[11] Physical searches for foreign intelligence information are governed by 50 U.S.C. § 1821 *et seq.*, P.L. 103-359, Title VIII, amending P.L. 95-511, October 14, 1994, 108 Stat. 3443;

(continued...)

which deal with electronic surveillance in the foreign intelligence context. As the provisions of E.O. 12333 to some extent set the broader context within which FISA operates, we will briefly examine its pertinent provisions first.

Executive Order 12333

Under Part 2.3 of E.O. 12333, the agencies within the Intelligence Community are to "collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. . . ." Among the types of information that can be collected, retained or disseminated under this section are:

> (a) Information that is publicly available or collected with the consent of the person concerned;
>
> (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
>
> (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;
>
> (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;
>
> (e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting;
>
> (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
>
> (g) Information arising out of a lawful personnel, physical or communications security investigation;
>
> . . .
>
> (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and
>
> (j) Information necessary for administrative purposes.

---

[11](...continued)
while the use of pen registers and trap and trace devices in connection with foreign intelligence investigations is addressed in 50 U.S.C. § 1841 *et seq.*, P.L. 105-272, Title VI, adding a new Title IV to P.L. 95-511 on October 20, 1998, 112 Stat. 2405. Access to certain business records for foreign intelligence or international terrorism investigative purposes is covered by 50 U.S.C. § 1861 *et seq.*, P.L. 105-272, Title VI, adding a new Title V to P.L. 95-511 on October 20, 1998, 112 Stat. 2411.

> In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

In discussing collections techniques, Part 2.4 of E.O. 12333 indicates that agencies withing the Intelligence Community are to use

> the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. . . .

Part 2.5 of the Executive Order 12333 states that:

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978 [section 1801 et seq. of this title], shall be conducted in accordance with that Act, as well as this Order.

The Foreign Intelligence Surveillance Act

The Statutory Framework

The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, as amended, provides a framework for the use of electronic surveillance to acquire foreign intelligence information. This measure seeks to strike a balance between national security needs in the context of foreign intelligence gathering and privacy rights. Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance to acquire foreign intelligence information for up to one year without a court order if two criteria are satisfied. First, to utilize this authority, the Attorney General must certify in writing under oath that:

> (A) the electronic surveillance is solely directed at —
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
>
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open

and exclusive control of a foreign power, as defined in section 1801(a)(1), (2) or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title;[12]

---

[12]Minimization procedures with respect to electronic surveillance are defined in 50 U.S.C. § 1801(h) to mean:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

"United States person" is defined in 50 U.S.C. § 1801(i) to mean

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power" is defined in 50 U.S.C. § 1801(a) to mean:

> (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

(continued...)

. . . .

Second, in order for the President, through the Attorney General, to use this authority

> . . . the Attorney General [must report] such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization and the reason for their becoming effective immediately.

Such electronic surveillance must be conducted only in accordance with the Attorney General's certification and minimization procedures adopted by him. A copy of his certification must be transmitted by the Attorney General to the court established

---

[12](...continued)
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.

"Agent of a foreign power" is defined in 50 U.S.C. § 1801(b) to mean:

> (1) any person other than a United States person, who--
>
> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
>
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
>
> (2) any person who--
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

under 50 U.S.C. § 1803(a) (hereinafter the FISC). This certification remains under seal unless an application for a court order for surveillance authority is made under 50 U.S.C. §§ 1801(h)(4) and 1804,[13] or the certification is necessary to determine the legality of the surveillance under 50 U.S.C. § 1806(f).[14] 50 U.S.C. § 1802(a)(2) and (a)(3).

In connection with electronic surveillance so authorized, the Attorney General may direct a specified communications common carrier to furnish all information, facilities, or technical assistance needed for the electronic surveillance to be accomplished in a way that would protect its secrecy and minimize interference with the services provided by the carrier to its customers. 50 U.S.C. § 1802(a)(4)(A). In addition, the Attorney General may direct the specified communications common carrier to maintain any records, under security procedures approved by the Attorney General and the Director of Central Intelligence, concerning the surveillance or the assistance provided which the carrier wishes to retain. 50 U.S.C. § 1802(a)(4)(B). Compensation at the prevailing rate must be made to the carrier by the Government for providing such aid.

If the President, by written authorization, empowers the Attorney General to approve applications to the FISC, an application for a court order may be made pursuant to 50 U.S.C. § 1802(b). A judge receiving such an application may grant an order under 50 U.S.C. § 1805 approving electronic surveillance of a foreign power or an agent of a foreign power to obtain foreign intelligence information. There is an exception to this, however. Under 50 U.S.C. § 1802(b), a court does not have jurisdiction to grant an order approving electronic surveillance directed solely as described in 50 U.S.C. § 1802(a)(1)(A) (that is, at acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, or acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power), unless the surveillance may involve the acquisition of communications of a United States person. 50 U.S.C. § 1802(b).

An application for a court order authorizing electronic surveillance for foreign intelligence purposes may be sought under 50 U.S.C. § 1804. An application for such a court order must be made by a federal officer in writing on oath or affirmation to an FISC judge. The application must be approved by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 *et seq.* have been met. Section 1804(a) sets out what must be included in the application:

> (1) the identity of the Federal officer making the application;
> (2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
> (3) the identity, if known, or a description of the target of the electronic surveillance;

---

[13] 50 U.S.C. § 1804 is discussed at pages 8-10 of this report, *infra.*

[14] 50 U.S.C. § 1806 is discussed at pages 14-18 of this report, *infra.*

(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that —

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

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

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate[15]—

(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 according to the categories described in 1801(e) of this title; 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;

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more that one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

---

[15]Under Section 1-103 of Executive Order 12139, the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the FBI, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence were designated to make such certifications in support of applications to engage in electronic surveillance for foreign intelligence purposes. Neither these officials nor anyone acting in those capacities may make such certifications unless they are appointed by the President with the advice and consent of the Senate.

The application for a court order need not contain the information required in Subsections 1804(6), (7)(E), (8), and (11) above if the target of the electronic surveillance is a foreign power and each of the facilities or places at which surveillance is directed is owned, leased, or exclusively used by that foreign power. However, in those circumstances, the application must indicate whether physical entry is needed to effect the surveillance, and must also contain such information about the surveillance techniques and communications or other information regarding United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures. 50 U.S.C. § 1804(b).

Where an application for electronic surveillance under 50 U.S.C. § 1804(a) involves a target described in 50 U.S.C. § 1801(b)(2),[16] the Attorney General must personally review the application if requested to do so, in writing, by the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of Central Intelligence.[17] The authority to make such a request may not be delegated unless the official involved is disabled or otherwise unavailable.[18] Each such official must make appropriate arrangements, in advance, to ensure that such a delegation of authority is clearly established in case of disability or other unavailability.[19] If the Attorney General determines that an application should not be approved, he must give the official requesting the Attorney General's personal review of the application written notice of the determination. Except in cases where the Attorney General is disabled or otherwise unavailable, the responsibility for such a determination may not be delegated. The Attorney General must make advance plans to ensure that the delegation of such responsibility where the Attorney General is disabled or otherwise unavailable is clearly established.[20] Notice of the Attorney General's determination that an application should not be approved must indicate what modifications, if any, should be made in the application needed to make it meet with the Attorney General's approval.[21] The official receiving the Attorney General's notice of modifications which would make the application acceptable must modify the application if the official deems such modifications warranted. Except in cases of disability or other unavailability, the responsibility to supervise any such modifications is also a non-delegable responsibility.[22]

If a judge makes the findings required under 50 U.S.C. § 1805(a), then he or she must enter an ex parte order as requested or as modified approving the electronic surveillance. The necessary findings must include that:

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

---

[16]For a list of those covered in 50 U.S.C. § 102(b)(2), see footnote 12, *supra*.

[17]50 U.S.C. § 1804(e)(1)(A).

[18]50 U.S.C. § 1804(e)(1)(B).

[19]50 U.S.C. § 1804(e)(1)(C).

[20]50 U.S.C. § 1804(e)(2)(A).

[21]50 U.S.C. § 1804(e)(2)(B).

[22]50 U.S.C. § 1804(e)(2)(C).

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

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that —

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is 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 section 1801(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

In making a probable cause determination under 50 U.S.C. § 1805(a)(3), the judge may consider past activities of the target as well as facts and circumstances relating to the target's current or future activities.[23] An order approving an electronic surveillance under Section 1805 must:

(1) specify–

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the device involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct–

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

---

[23] 50 U.S.C. § 1805(b).

> (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
>
> (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.[24]

If the target of the electronic surveillance is a foreign power and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order does not need to include the information covered by Section 1805(c)(1)(C), (D), and (F), but must generally describe the information sought, the communications or activities subject to surveillance, the type of electronic surveillance used, and whether physical entry is needed. 50 U.S.C. § 1805(d).

Such an order may approve an electronic surveillance for the period of time necessary to achieve its purpose or for ninety days, whichever is less, unless the order is targeted against a foreign power. In that event, the order shall approve an electronic surveillance for the period specified in the order or for one year, whichever is less. Generally, upon application for an extension, a court may grant an extension of an order on the same basis as an original order. An extension must include new findings made in the same manner as that required for the original order. However, an extension of an order for a surveillance targeting a foreign power that is not a United States person may be for a period of up to one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period involved. 50 U.S.C. § 1805(e).

Emergency situations are addressed in 50 U.S.C. § 1805(f).[25] Notwithstanding other provisions of this subchapter, if the Attorney General reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained and that the factual basis for issuance of an order under this subchapter to approve such surveillance exists, he may authorize electronic surveillance if specified steps are taken. At the time of the Attorney General's emergency authorization, he or his designee must inform an FISC judge that the decision to employ emergency electronic surveillance has been made. An application for a court order under Section 1804 must be made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorized such surveillance. If the Attorney General authorizes emergency electronic surveillance, he must require compliance with the minimization procedures required

---

[24] 50 U.S.C. § 1805(c).

[25] 50 U.S.C. § 1805(g) authorizes officers, employees, or agents of the United States to conduct electronic surveillance in the normal course of their official duties to test electronic equipment, determine the existence and capability of equipment used for unauthorized electronic surveillance, or to train intelligence personnel in the use of electronic surveillance equipment. Under 50 U.S.C. § 1805(g), the certifications of the Attorney General pursuant to 50 U.S.C. § 1802(a) and applications made and orders granted for electronic surveillance under FISA must be retained for at least 10 years.

for the issuance of a judicial order under this subchapter. Absent a judicial order approving the emergency electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after 24 hours from the time of the Attorney General's authorization, whichever is earliest. If no judicial order approving the surveillance is issued, the information garnered may not be received in evidence or otherwise disclosed in any court proceeding, or proceeding in or before any grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof. No information concerning any United States person acquired through such surveillance may be disclosed by any Federal officer or employee without the consent of that person, unless the Attorney General approves of such disclosure or use where the information indicates a threat of death or serious bodily harm to any person.[26]

---

[26] Some of the provisions dealing with interception of wire, oral, or electronic communications in the context of criminal law investigations, 18 U.S.C. §§ 2510 *et seq.*, may also be worthy of note. With certain exceptions, these provisions, among other things, prohibit any person from engaging in intentional interception; attempted interception; or procuring others to intercept or endeavor to intercept wire, oral, or electronic communication; or intentional disclosure; attempting to disclose; using or endeavoring to use the contents of a wire, oral or electronic communication, knowing or having reason to know that the information was obtained by such an unlawful interception. 18 U.S.C. § 2511. "Person" is defined in 18 U.S.C. § 2510(6) to include "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." Among the exceptions to Section 2511 are two of particular note:

> (2)(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.
>
> (2)(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

Among other things, Section 2512 prohibits any person from intentionally manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing that its design renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. It also prohibits any person from intentionally sending such a device through the mail or sending or carrying such a device in interstate or foreign commerce,

(continued...)

[25](...continued)
knowing that such surreptitious interception is its primary purpose. Similarly, intentionally advertising such a device, knowing or having reason to know that the advertisement will be sent through the mail or transported in interstate or foreign commerce is foreclosed. Again an exception to these general prohibitions in Section 2512 may be of particular interest:

> (2) It shall not be unlawful under this section for—
> (a) . . .
> (b) an officer, agent, or employee of, or a person under contract with, the United States . . . in the normal course of the activities of the United States . . .,
> to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

In addition, Section 107 of the Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1858, October 21, 1986, [which enacted 18 U.S.C. §§ 1367, 2621, 2701 to 2711, 3117, and 3121 to 3126; and amended 18 U.S.C. §§ 2232, 2511-2513, and 2516-2520], provided generally that, "[n]othing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity." It also stated:

> (b) Certain Activities Under Procedures Approved by the Attorney General.--Nothing in chapter 119 [interception of wire, oral or electronic communications] or chapter 121 [stored wire and electronic communications and transactional records access] of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to--
> (1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;
> (2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.]; or
> (3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.].

In addition, Chapter 121 of title 18 of the United States Code deals with stored wire and electronic communications and transactional records. Under 18 U.S.C. § 2701, intentionally accessing without authorization a facility through which an electronic communication service is provided, or intentionally exceeding an authorization to access such a facility and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such system is prohibited. Upon compliance with statutory requirements in 18 U.S.C. § 2709, the Director of the FBI or his designee in a position not lower than deputy Assistant Director may seek access to telephone toll and transactional records for foreign counterintelligence purposes. The FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations

(continued...)

The uses to which information gathered under FISA may be put are addressed under 50 U.S.C. § 1806.[27] Under these provisions, disclosure, without the

---

[26](...continued)
conducted by the FBI, and, "with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency." 18 U.S.C. § 2709(d).

[27]The provisions of Section 1806 are as follows:

> (a) Compliance with minimization procedures; privileged communications; lawful purposes
>
> Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with or in violation of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.
>
> (b) Statement for disclosure
>
> No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.
>
> (c) Notification by United States
>
> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.
>
> (d) Notification by States or political subdivisions
>
> Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof intends to so disclose or so use such information.
>
> (e) Motion to suppress
>
> Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to

(continued...)

[27](...continued)

suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement

(continued...)

consent of the person involved, of information lawfully acquired under FISA which concerns a United States person must be in compliance with the statutorily mandated minimization procedures. Communications which were privileged when intercepted remain privileged. Where information acquired under FISA is disclosed for law enforcement purposes, neither that information nor any information derived therefrom may be used in a criminal proceeding without prior authorization of the Attorney General. If the United States Government intends to disclose information acquired under FISA or derived therefrom in any proceeding before a court, department, officer regulatory body or other authority of the United States against an aggrieved person,[28] then the Government must give prior notice of its intent to disclose to the aggrieved person and to the court or other authority involved. Similarly, a State or political subdivision of a State that intends to disclose such information against an aggrieved person in a proceeding before a State or local authority must give prior notice of its intent to the aggrieved person, the court or other authority, and the Attorney General.

Section 1806 also sets out in camera and ex parte district court review procedures to be followed where such notification is received, or where the aggrieved person seeks to discover or obtain orders or applications relating to FISA electronic surveillance, or to discover, obtain, or suppress evidence or information obtained or derived from the electronic surveillance, and the Attorney General files an affidavit under oath that such disclosure would harm U.S. national security. The focus of this review would be to determine whether the surveillance was lawfully conducted and authorized. Only where needed to make an accurate determination of these issues does the section permit the court to disclose to the aggrieved person, under appropriate security measures and protective orders, parts of the application, order,

---

[27](...continued)

> purposes, and if both the sender and all intended recipients are located within the United States, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.
>
> (j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination
>
> If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application or on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--
>
> (1) the fact of the application;
>
> (2) the period of the surveillance; and
>
> (3) the fact that during the period information was or was not obtained.
>
> On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forgo ordering the serving of the notice required under this subsection.

The term "aggrieved person" as used in FISA, is defined under 50 U.S.C. § 1801(k) to mean "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."

[28]For the definition of "aggrieved person" as that term is used in FISA, see fn. 6, *supra*.

or other materials related to the surveillance. If, as a result of its review, the district court determines that the surveillance was unlawful, the resulting evidence must be suppressed. If the surveillance was lawfully authorized and conducted, the motion of the aggrieved person must be denied except to the extent that due process requires discovery or disclosure. Resultant court orders granting motions or requests of the aggrieved person for a determination that the surveillance was not lawfully conducted or authorized, and court orders requiring review or granting disclosure are final orders binding on all Federal and State courts except a U.S. Court of Appeals and the U.S. Supreme Court.

If the contents of any radio communication are unintentionally acquired by an electronic, mechanical, or other surveillance device in circumstances where there is a reasonable expectation of privacy and where a warrant would be required if the surveillance were to be pursued for law enforcement purposes, then the contents must be destroyed when recognized, unless the Attorney General finds that the contents indicate a threat of death or serious bodily harm to any person.

As noted above, Section 1805 provides for emergency electronic surveillance in limited circumstances, and requires the subsequent prompt filing of an application for court authorization to the FISC in such a situation. Under Section 1806, if the application is unsuccessful in obtaining court approval for the surveillance, notice must be served upon any United States person named in the application and such other U.S. persons subject to electronic surveillance as the judge determines, in the exercise of his discretion, is in the interests of justice. This notice includes the fact of the application, the period of surveillance, and the fact that information was or was not obtained during this period. Section 1806 permits postponement or suspension of service of notice for up to ninety days upon ex parte good cause shown. Upon a further ex parte showing of good cause thereafter, the court will forego ordering such service of notice.[29]

Reporting requirements are included in Sections 1807 and 1808. Under Section 1807, each year in April, the Attorney General is directed to transmit to the Administrative Office of the United States Courts and to the Congress a report covering the total number of applications made for orders and extensions of orders

---

[29] *Cf., United States Attorney's Manual*, §§ 1-2.106 (Office of Intelligence Policy and Review organization and functions). This section indicates, in part, that the Office of Intelligence Policy and Review

> . . . prepares certifications and applications for electronic surveillance under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., and represents the United States before the United States Foreign Intelligence Surveillance Court. It processes requests for Attorney General Authority to use FISA material in adjudicatory proceedings and assists in responding to challenges to the legality of FISA surveillances.

See also, 28 C.F.R. § 0.33 (functions of the Counsel for Intelligence Policy); *United States Attorneys' Criminal Resource Manual*, §§ 1073 (FISA–50 U.S.C. § 1809) and 1075 (elements of the offense under 50 U.S.C. § 1809(a)); *cf., United States Attorney's Manual* § 9-7.301 (consensual monitoring in the context of electronic surveillance).

approving electronic surveillance under FISA during the previous year, and the total number of orders and extensions granted, modified, or denied during that time period. Section 1808(a) requires the Attorney General to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence semiannually about all electronic surveillance under FISA.[30] Each such report must contain a description of each criminal case in which information acquired under FISA "has been passed for law enforcement purposes" during the period covered by the report, and each criminal case in which information acquired under FISA has been authorized to be used at trial during the reporting period.[31]

Section 1809 provides criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute; or for disclosing or using information obtained under color of law by electronic surveillance, knowing or having reason to know that surveillance was not authorized by statute.[32] The provision makes it a defense to prosecution under this subsection if the defendant is a law enforcement officer or investigative officer in the course of his official duties and the electronic surveillance was authorized by and conducted under a search warrant or court order of a court of competent jurisdiction. Section 1809 provides for Federal jurisdiction over such an offense if the defendant is a Federal officer or employee at the time of the offense. Civil liability is also provided for under Section 1810, where an aggrieved person, who is neither a foreign power nor an agent of a foreign power, has been subjected to electronic surveillance, or where information gathered by electronic surveillance about an aggrieved person has been disclosed or used in violation of Section 1809.

---

[30]Subsection 1808(b) directed these committees to report annually for five years after the date of enactment to the House and the Senate respectively concerning implementation of FISA, including any recommendations for amendment, repeal, or continuation without amendment. P.L. 106-567, Title VI, Sec. 604(b) (Dec. 27, 2000), 114 Stat. 2853, required the Attorney General to submit to the Senate Select Committee on Intelligence, the Senate Judiciary Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee a report on the authorities and procedures utilized by the Department of Justice to determine whether or not to disclose information acquired under FISA for law enforcement purposes. 50 U.S.C. § 1806 note.

[31]50 U.S.C. § 1808(a)(2).

[32]Section 1075 of the *United States Attorneys' Criminal Resource Manual* indicates that Section 1809(a) "reaches two distinct acts: (1) engaging in unauthorized electronic surveillance under color of law; and (2) using or disclosing information obtained under color of law through unauthorized electronic surveillance. Each offense involves an "intentional" state of mind and unauthorized "electronic surveillance." Section 1075 further notes:

> Even though none of these elements mentions foreign intelligence, one court has explained that "the FISA applies only to surveillance designed to gather information relevant to foreign intelligence." *United States v. Koyomejian*, 970 F. 2d 536, 540 (9th Cir. 1992) (en banc), cert denied, 506 U.S. 1005 (1992). In fact, all applications for an order from the Foreign Intelligence Surveillance Court require a certification from a presidentially designated official that the purpose of the surveillance is to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7).

Finally, Section 1811 provides that, notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order to acquire foreign intelligence information for up to 15 calendar days following a declaration of war by Congress.

Conclusion

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, provides a statutory structure to be followed where electronic surveillance for foreign intelligence gathering purposes is contemplated. It creates enhanced procedural protections where a United States person is involved, while setting somewhat less stringent standards where the surveillance involves foreign powers or agents of foreign powers. With its detailed statutory structure, it seeks to protect personal liberties protected by the Fourth Amendment while providing a means to ensure national security interests.