Order Code RL30465

CRS Report for Congress
Received through the CRS Web

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions

Updated April 21, 2005

Elizabeth B. Bazan
Legislative Attorney
American Law Division

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions

Summary

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, (FISA) as passed in 1978, provided a statutory framework for the use of 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. Subsequent legislation expanded federal laws dealing with foreign intelligence gathering to address physical searches, pen registers and trap and trace devices, and access to certain business records. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56, made significant changes to some of these provisions. Further amendments were included in the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, and the Homeland Security Act of 2002, P.L. 107-296, and the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458. In addressing international terrorism or espionage, the same factual situation may be the focus of both criminal investigations and foreign intelligence collection efforts. Changes in FISA under these public laws are intended to facilitate information sharing between law enforcement and intelligence elements. In its Final Report, the 9/11 Commission noted that the removal of the pre-9/11 "wall" between intelligence and law enforcement "has opened up new opportunities for cooperative action within the FBI."

On May 17, 2002, the U.S. Foreign Intelligence Surveillance Court (FISC) issued a memorandum opinion and order written by the then Presiding Judge of the court, and concurred in by all of the other judges then on the court. The unclassified opinion and order were provided to the Senate Judiciary Committee in response to a letter from Senator Leahy, Senator Grassley, and Senator Specter, who released them to the public on August 22, 2002. In its decision, the FISC considered a motion by the U.S. Department of Justice "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion." The FISC granted the Department's motion, but modified part of the what it saw as proposed minimization procedures. This decision was not appealed directly, but the Department of Justice did seek review of a FISC order authorizing electronic surveillance of an agent of a foreign power and of a FISC order renewing that surveillance, both subject to restrictions based upon the May 17th memorandum opinion and order by the FISC. The U.S. Foreign Intelligence Surveillance Court of Review reversed and remanded the FISC orders on November 18, 2002.

This report will examine the detailed statutory structure provided by FISA and related provisions of E.O. 12333. In addition, it will discuss the decisions of the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review.

Contents

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions

Introduction

On October 26, 2001, President George W. Bush signed P.L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act or the USA PATRIOT Act. Among its provisions are a number which impacted or amended the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* (FISA). For example, the law expanded the number of United States district court judges on the Foreign Intelligence Surveillance Court and provided for roving or multipoint electronic surveillance authority under FISA. It also amended FISA provisions with respect to pen registers and trap and trace devices and access to business records. In addition, FISA, as amended, substantially expanded the reach of the business records provisions. The amended language changed the certification demanded of a federal officer applying for a FISA order for electronic surveillance or a physical search from requiring a certification that *the* purpose of the surveillance or physical search is to obtain foreign intelligence information to requiring certification that *a significant purpose* of the surveillance or search is to obtain foreign intelligence information. FISA, as amended, also affords persons aggrieved by inappropriate use or disclosure of information gathered in or derived from a FISA surveillance, physical search or use of a pen register or trap and trace device a private right of action. Of the amendments made by the USA PATRIOT Act, all but the section which increased the number of judges on the Foreign Intelligence Surveillance Court will sunset on December 31, 2005. Subsequent amendments to FISA were made by the Intelligence Authorization Act for Fiscal Year 2003, P.L. 107-108; the Homeland Security Act of 2002, P.L. 107-296; and the Intelligence Reform and Terrorism Protection Act of 2004, P.L. 108-458.

On May 17, 2002, the U.S. Foreign Intelligence Surveillance Court (FISC) issued an opinion and order[1] written by the then Presiding Judge of the court, U.S. District Judge Royce C. Lamberth. All of the other judges then on the FISC concurred in the order. The opinion was provided by the current Presiding Judge of the FISC, U.S. District Judge Colleen Kollar-Kotelly, to the Senate Judiciary Committee in response to a July 31 letter from Senator Leahy, Senator Grassley and

---

[1] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611(U.S. Foreign Intell. Surveil. Ct. 2002) (hereinafter *FISC op.*).

Senator Specter.[2] On August 22, 2002, the unclassified opinion was released to the public by Senator Leahy, Senator Grassley and Senator Specter.

In the memorandum opinion and order, the FISC considered a motion by the U.S. Department of Justice "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion."[3] In its memorandum and accompanying order, the FISC granted the Department of Justice's motion, but modified the second and third paragraphs of section II.B of the proposed minimization procedures.[4]

The FISC's May 17th memorandum opinion and order were not appealed directly. However, the Justice Department sought review in the U.S. Foreign Intelligence Court of Review (Court of Review) of an FISC order authorizing electronic surveillance of an agent of a foreign power, subject to restrictions flowing from the May 17th decision, and of an FISC order renewing that surveillance subject to the same restrictions.[5] The Court of Review reversed and remanded the FISC orders.[6] This opinion, the first issued by the U.S. Foreign Intelligence Surveillance

---

[2] *See,* Statement of Sen. Patrick Leahy, Chairman, Committee on the Judiciary, "The USA PATRIOT Act in Practice: Shedding Light on the FISA Process" (Sept. 10, 2002), [http://judiciary.senate.gov/member_statement.cfm?id=398&wit_id=50]; "Courts," *National Journal's Technology Daily* (August 22, 2002, PM Edition); "Secret Court Rebuffs Ashcroft; Justice Dept. Chided on Misinformation," by Dan Eggen and Susan Schmidt, *Washington Post*, p. A1 (August 23, 2002).

[3] *FISC op.*, 218 F. Supp. 2d at 613.

[4] *Id.* at 624-27.

[5] In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (hereinafter *Court of Review op.*).

[6] The Foreign Intelligence Surveillance Act, P.L. 95-511, as amended (hereinafter FISA), Title I, § 103, 50 U.S.C. § 1803, created both the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review. As originally constituted the FISC was made up of 7 U.S. district court judges publicly designated by the Chief Justice of the United States. As amended by the USA PATRIOT Act, P.L. 107-56, § 208, the membership in the FISC was expanded to 11 members, at least 3 of whom must live within a 20 mile radius of the District of Columbia. The U.S. Foreign Intelligence Surveillance Court of Review is made up of 3 U.S. district court or U.S. court of appeals judges publicly designated by the Chief Justice.

The current language of 50 U.S.C. § 1803 provides:

§ 1803. Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review

The Chief Justice of the United States shall publicly designate 11 district court judges from seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall

(continued...)

[6] (...continued)

> constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established under subsection (b) of this section.
>
> (b) Court of review; record, transmittal to Supreme Court
>
> The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.
>
> (c) Expeditious conduct of proceedings; security measures for maintenance of records
>
> Proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.
>
> (d) Tenure
>
> Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated for terms from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years.

The reference in subsection (a), (b), and (c) to "this chapter" refers to chapter 36 of Title 50, U.S.C., where the Foreign Intelligence Surveillance Act, as amended, is codified. This Act, as amended, deals with electronic surveillance (50 U.S.C. § 1801 *et seq.*), physical searches (50 U.S.C. § 1821 *et seq.*), pen registers and trap and trace devices (50 U.S.C. § 1841 *et seq.*), and "access to certain business records for foreign intelligence and international terrorism investigations" (50 U.S.C. § 1861). The judges of the FISC are given jurisdiction over applications for physical searches for the purpose of obtaining foreign intelligence information anywhere in the United States under 50 U.S.C. § 1822(c). Under 50 U.S.C. § 1842(b), an application for an order authorizing or approving the installation and use of a pen register or trap and trace device for foreign intelligence or international terrorism investigations may be made to either a judge of the FISC or to a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders on behalf of an FISC judge approving such installation and use. Similarly, under 50 U.S.C. § 1861(b), an application for an order for production of tangible things under the "business records" provision may be made either to an FISC judge or to a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States

(continued...)

Court of Review since its creation in 1978, was also released to the public. This report will provide background on the Foreign Intelligence Surveillance Act, discuss its statutory framework, and review these two decisions.

Background

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.[7] 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.[8] The *Katz* Court stated, however, that its holding did not extend to cases involving national security.[9] 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."[10] 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 unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.[11]

---

[6] (...continued)
to hear such an application and to grant such an order on behalf of an FISC judge.

[7] 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.

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

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

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

[11] 407 U.S. at 299.

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.[12] 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."[13] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents."[14] 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 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

---

[12] *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." . . . .

[13] *Id.*, at 308.

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

> 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.[15]

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.[16] Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12333.[17] This report will examine the provisions of FISA which deal with electronic surveillance, in the foreign intelligence context, as well as those applicable to physical searches, the use of pen registers and trap and trace devices under FISA, and access to business records and other tangible things for foreign intelligence purposes. As the provisions of E.O. 12333 to some extent set

---

[15] 407 U.S. at 323-24.

[16] 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. 95-1720 (Oct. 5, 1978); Senate Reports and House Conference Report are reprinted in 1978 *U.S. Code Cong. & Admin. News* 3904.

[17] Physical searches for foreign intelligence information are governed by 50 U.S.C. § 1821 *et seq.*, 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.* Access to certain business records for foreign intelligence or international terrorism investigative purposes is covered by 50 U.S.C. § 1861 *et seq.*

the broader context within which FISA operates, we will briefly examine its pertinent provisions first.

Executive Order 12333

Executive Order 12333 (December 4, 1981), as amended, 50 U.S.C. § 401 note, deals with "United States Intelligence Activities." Under Section 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.
>
> 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, Section 2.4 of E.O. 12333 indicates that agencies within 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. . . .

Section 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

Electronic surveillance under FISA. 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,[18] physical searches, pen registers and trap and trace devices

---

[18] 50 U.S.C. § 1801(f)(2) defines "electronic surveillance" to mean:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any person thereto, if such acquisition occurs in the United States, *but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18*;
> (3) the intentional 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 purposes, and if both the sender and all intended

(continued...)

to acquire foreign intelligence information.[19] This measure seeks to strike a balance between national security needs in the context of foreign intelligence gathering and privacy rights.[20]

---

[18] (...continued)

> recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

The italicized portion of Subsection 1801(f)(2) was added by Sec. 1003 of P.L. 107-56.

[19] "Foreign intelligence information" is defined in 50 U.S.C. § 1801(e) to mean:

> (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;
> (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.

"International terrorism" is defined in 50 U.S.C. § 1801(c) to mean activities that:

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

"Sabotage" is defined in 50 U.S.C. § 1801(d) to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."

[20] In addition to the provisions dealing with electronic surveillance, physical searches and pen registers and trap and trace devices, FISA includes a section which permits the Director of the FBI or his designee (whose rank may be no lower than an Assistant Special Agent in Charge) to apply for an order requiring "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign

(continued...)

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;[21] . . . .

---

[20] (...continued)
intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . ." 50 U.S.C. § 1861(a)(1). Where such an investigation is of a United States person, it may not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution." *Id.* Although this section is entitled "access to certain business records for foreign intelligence and international terrorism investigations," it encompasses substantially more than just business records. The current language of 50 U.S.C. §§ 1861 and 1862 (which deals with congressional oversight of all such requests for production of tangible things under § 1861) was added by the USA PATRIOT Act, and amended by P.L. 107-108. It replaced former 50 U.S.C. §§ 1861-1863, added by P.L. 105-272, title VI, § 602, 112 Stat. 2411 (Oct. 20, 1998), which defined various terms, provided for applications for orders for access to certain limited types of business records (relating to records in the possession of common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities) for foreign intelligence and international terrorism investigations, and provided for congressional oversight of such records requests.

[21] 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

(continued...)

[21] (...continued)

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 *72* 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.

Sec. 314(a)(1) of H.Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002 to accompany H.R. 2883, amended 50 U.S.C. § 1801(h)(4) to change to 72 hours what was previously a 24 hour period beyond which the contents of any communication to which a U.S. person is a party may not be retained absent a court order under 50 U.S.C. § 1805 or a finding by the Attorney General that the information indicates a threat of death or serious bodily injury. The conference version of H.R. 2883 received the approbation of both houses of Congress, and was forwarded to the President on December 18, 2001, for his signature. Signed by the President ten days later, it became P.L. 107-108.

"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 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

(continued...)

[21] (...continued)

> 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
>
> *(C) engages in international terrorism or activities in preparation therefore* [sic]; *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).

The italicized language in 50 U.S.C. § 1801(b)(1)(C) was added to the definition of "agent of a foreign power" in Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458. This provision would be "subject to the sunset provision in section 224 of the USA PATRIOT Act of 2001 (Public Law 107-56, 115 Stat. 295), including the exception provided in subsection (b) of such section 224." The sunset provision in Section 224 of P.L. 107-56, would take effect on December 31, 2005, except for any foreign intelligence investigation begun before that date or any criminal offense or potential offense that began or occurred before that date. For a more in depth discussion of this so-called "lone wolf" provision, see CRS Report for Congress RS22011, *Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act*, by Elizabeth B. Bazan (December 29, 2004). For an examination of this and other legislative measures related to FISA from the 108th Congress, see CRS Report for Congress RL32608, *Foreign Intelligence Surveillance Act: Selected Legislation from the 108th Congress*, by Elizabeth B. Bazan (updated January 11, 2005).

Several other provisions of Intelligence Reform and Terrorism Prevention Act also impacted FISA. Section 1011 of the measure amended Title I of the National Security Act of 1947, 50 U.S.C. § 402 *et seq*., to strike the previous Sections 102 through 104 of the Act 50 U.S.C. §§ 403, 403-1, 403-3, and 403-4, and insert new Sections 102 through 104A. The new Section 102 created the position of Director of National Intelligence (DNI). Section 102A outlined authorities and responsibilities of the position. Under the new Section 102A(f)(6) of the National Security Act, the DNI was given responsibility "to establish requirements and priorities for foreign intelligence information to be collected under [FISA],

(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.

---

[21] (...continued)
and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that act is disseminated so that it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that act unless otherwise authorized by statute or Executive order." New Section 102A(f)(8) of the National Security Act, as enacted by P.L. 108-458, Section 1011, provided that, "Nothing in this act shall be construed as affecting the role of the Department of Justice or the Attorney General with respect to applications under the Foreign Intelligence Surveillance Act."

Section 1071(e) of P.L. 108-458, amended FISA to insert "Director of National Intelligence" in lieu of "Director of Central Intelligence" in each place in which it appeared.

Section 6002 created additional semiannual reporting requirements under FISA. Under the new language, the Attorney General, on a semiannual basis, must submit to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee, in a manner consistent with protection of national security, reports setting forth with respect to the preceding six month period:

> (1) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for–
>
> (A) electronic surveillance under section 105 [50 U.S.C. § 1805];
>
> (B) physical searches under section 304 [50 U.S.C. § 1824];
>
> (C) pen registers under section 402 [50 U.S.C. § 1842]; and
>
> (D) access to records under section 501 [50 U.S.C. § 1861];
>
> (2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C) [50 U.S.C. § 1801(b)(1)(C)];
>
> (3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;
>
> (4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Court of Review by the Department of Justice; and
>
> (5) copies of all decisions (not including orders) or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this Act.

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 under 50 U.S.C. § 1803(a) (hereinafter the FISC).[22] 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,[23] or the certification is necessary to determine the legality of the surveillance under 50 U.S.C. § 1806(f).[24] 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 National 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

---

[22] Under 50 U.S.C. § 1803(a), as amended by Section 208 of P.L. 107-56, the Chief Justice of the United States must publicly designate eleven U.S. district court judges from seven of the United States judicial circuits, of whom no fewer than three must reside within 20 miles of the District of Columbia. These eleven judges constitute the court which has jurisdiction over applications for and orders approving electronic surveillance anywhere within the United States under FISA. If an application for electronic surveillance under this act is denied by one judge of this court, it may not then be considered by another judge on the court. If a judge denies such an application, he or she must immediately provide a written statement for the record of the reason(s) for this decision. If the United States so moves, this record must then be transmitted under seal to a court of review established under 50 U.S.C. § 1803(b). The Chief Justice also publicly designates the three U.S. district court or U.S. court of appeals judges who together make up the court of review having jurisdiction to review any denial of an order under FISA. If that court determines that an application was properly denied, again a written record of the reason(s) for the court of review's decision must be provided for the record, and the United States may petition for a writ of certiorari to the United States Supreme Court. All proceedings under this Act must be conducted expeditiously, and the record of all proceedings including applications and orders granted, must be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence. 50 U.S.C. § 1803(c).

[23] 50 U.S.C. § 1804 is discussed at pages 15-19 of this report, *infra*.

[24] 50 U.S.C. § 1806 is discussed at pages 25-32 of this report, *infra*.

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;
> (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[25] —
>
> (A) that the certifying official deems the information sought to be foreign intelligence information;

[25] 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.

(B) that *a significant*[26] purpose of the surveillance is to obtain foreign

---

[26] Section 218 of P.L. 107-56 amended the requisite certifications to be made by the Assistant to the President for National Security Affairs, or other designated official (see footnote 25). Heretofore, the certifying official had to certify, among other things, that *the* purpose of the electronic surveillance under FISA was to obtain foreign intelligence information. Under the new language, the certifying official must certify that *a significant* purpose of such electronic surveillance is to obtain foreign intelligence information. This change may have the effect of somewhat blurring the line between electronic surveillance for foreign intelligence purposes and that engaged in for criminal law enforcement purposes. Indeed, as interpreted by the Court of Review in In re Sealed Case, 310 F.3d 717, 728-38 (U.S. Foreign Intell. Surveil.Ct. Rev. 2002), this language appears to exclude FISA as a vehicle for authorizing electronic surveillance where the sole purpose of an investigation is criminal prosecution. The government must have a measurable foreign intelligence purpose other than criminal prosecution, even of foreign intelligence crimes, in order to satisfy the "significant purpose" standard. The Court's analysis appears to suggest that the primary purpose of the investigation under FISA may be criminal prosecution, so long as collection of foreign intelligence information is also a significant purpose of the electronic surveillance. This issue was not addressed directly in the opinion of the U.S. Foreign Intelligence Surveillance Court in In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611(U.S. Foreign Intell. Surveil. Ct. 2002). *Id.*, at 615 n.2. Both opinions are addressed later in this report in the section entitled "Recent Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review."

Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, United States v. Megahey, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), *aff'd* 729 F.2d 1444 (2d Cir. 1982); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States. v Badia, 827 F. 2d 1458, 1464 (11th Cir. 1987). *See also*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *rehearing and cert. denied*, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); United States v. Pelton, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard — i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense — for issuance of a search warrant was violative of the 4th Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); United States v. Rahman, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). *Cf.*, United States v. Bin Laden, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); United States v. Bin Laden, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or

(continued...)

[26] (...continued)
agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection. . . . If foreign intelligence collection is merely *a* purpose and not the *primary* purpose of a search, the exception does not apply.") *Cf.*, United States v. Sarkissian, 841 F.2d 959, 964-65 (9th Cir. 1988) (FISA court order authorizing electronic surveillance, which resulted in the discovery of plan to bomb the Honorary Turkish Consulate in Philadelphia, and of the fact that bomb components were being transported by plane from Los Angeles. The FBI identified the likely airlines, flight plans, anticipated time of arrival, and suspected courier. Shortly before the arrival of one of those flights, the investigation focused upon an individual anticipated to be a passenger on a particular flight meeting all of the previously identified criteria. An undercover police officer spotted a man matching the suspected courier's description on that flight. The luggage from that flight was sniffed by a trained dog and x-rayed. A warrantless search was conducted of a suitcase that had been shown by x-ray to contain an unassembled bomb. Defendants unsuccessfully moved to suppress the evidence from the FISA wiretap and the warrantless search. On appeal the court upheld the warrantless suitcase search as supported by exigent circumstances. Defendants contended that the FBI's primary purpose for the surveillance had shifted at the time of the wiretap from an intelligence investigation to a criminal investigation and that court approval for the wiretap therefore should have been sought under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*, rather than FISA. The court, while noting that in other cases it had stated that "the purpose of [electronic] surveillance" under FISA "must be to secure foreign intelligence information", "not to ferret out criminal activity," declined to decide the issue of whether the standard under FISA required "the purpose" or "the primary purpose" of the surveillance to be gathering of foreign intelligence information. The court stated, "Regardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces us that it is met in this case. . . . We refuse to draw too fine a distinction between criminal and intelligence investigations. "International terrorism ," by definition, requires the investigation of activities that constitute crimes. 50 U.S.C. § 1806(f). That the government may later choose to prosecute is irrelevant. FISA contemplates prosecution based on evidence gathered through surveillance. . . . "Surveillances . . . need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." S. Rep. No. 701, 95th Cong., 1st Sess. 11 . . . .[(1978)]. . . .FISA is meant to take into account "the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities . . ." *Id.* . . . . At no point was this case an ordinary criminal investigation."). *Cf.*, United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (distinguishing United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980); and United States v. Butenko, 494 F.2d 593, 606 (3d Cir.) (*en banc*), *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), which held that, while warrantless electronic surveillance for foreign intelligence purposes was permissible, when the purpose or primary purpose of the surveillance is to obtain evidence of criminal activity, evidence obtained by warrantless electronic surveillance is inadmissible at trial, 540 F. Supp. at 1313; on the theory that the evidence in the case before it was obtained pursuant to a warrant — a lawfully obtained court order under FISA, *id.* at 1314. The court noted that the "bottom line of *Truong* is that evidence derived from *warrantless* foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information." *Id*. at 1313-14. After noting that Congress, in enacting FISA, "expected that evidence derived from FISA surveillances could then be used in a criminal proceeding," the court concluded that "it was proper for the FISA judge to issue the order in this case because of the on-going nature of the foreign
(continued...)

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.

---

[26] (...continued)
intelligence investigation. . . . The fact that evidence of criminal activity was thereafter uncovered during the investigation does not render the evidence inadmissible. There is no question in [the court's] mind that the purpose of the surveillance, pursuant to the order, was the acquisition of foreign intelligence information. Accordingly, [the court found] that the FISA procedures on their face satisfy the Fourth Amendment warrant requirement, and that FISA was properly implemented in this case." *Id.* at 1314.).

It is worthy of note that none of these decisions were handed down by the U.S. Foreign Intelligence Surveillance Court or the U.S. Foreign Intelligence Surveillance Court of Review. For a discussion of the recent decisions of those two courts regarding the Attorney General's 2002 minimization procedures, please see the discussion in the portion of this report regarding "Recent Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review," *infra*. Nor do these decisions of the U.S. district courts and U.S. courts of appeal reflect recent legislative amendments to the FISA statute. However, the FISC, in its decision, did not address potential Fourth Amendment implications, and the U.S. Foreign Intelligence Court of Review, in its decision, appears to imply that some Fourth Amendment issues in the FISA context may be non-justiciable. Alternatively, the language in the Court of Review opinion might mean that the issue has not yet been considered by the courts. Using a balancing test it derived from *Keith* between foreign intelligence crimes and ordinary crimes, the Court of Review found surveillances under FISA, as amended by the USA PATRIOT Act, to be reasonable and therefore constitutional, while at the same time acknowledging that the constitutional question presented by the case before it — "whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment — has no definitive jurisprudential answer." *Court of Review op.*, 301 F.3d at 746.

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),[27] 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 National Intelligence.[28] The authority to make such a request may not be delegated unless the official involved is disabled or otherwise unavailable.[29] 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.[30] 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.[31] 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.[32] 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.[33]

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;

---

[27] For a list of those covered in 50 U.S.C. § 1801(b)(2), see fn. 25, *supra*.

[28] 50 U.S.C. § 1804(e)(1)(A).

[29] 50 U.S.C. § 1804(e)(1)(B).

[30] 50 U.S.C. § 1804(e)(1)(C).

[31] 50 U.S.C. § 1804(e)(2)(A).

[32] 50 U.S.C. § 1804(e)(2)(B).

[33] 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.[34] An order approving an electronic surveillance under Section 1805(c) 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, *if known*;[35]

(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, *or in circumstances where the Court finds that the actions of the target of the*

---

[34] 50 U.S.C. § 1805(b).

[35] Section 314(a)(2)(A) of H.Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002, to accompany H.R. 2883, added "if known" to the end of Section 1805(c)(1)(B) before the semi-colon. The conference version of the bill passed both the House and the Senate, and was signed by the President on December 28, 2001, as P.L. 107-108.

> *application may have the effect of thwarting the identification of a specified person, such other persons,* 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;
>
> (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National 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.[36]

The italicized portions of Section 1805(c)(1)(B) and Section 1805(c)(2)(B) reflect changes, added by P.L. 107-108 and P.L. 107-56 respectively, intended to provide authority for "multipoint" or "roving" electronic surveillance where the actions of the target of the surveillance, such as switching phones and locations repeatedly, may thwart that surveillance. The Conference Report on H.R. 2338, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), H.Rept. 107-328, at page 24, provided the following explanation of these changes:

> The multipoint wiretap amendment to FISA in the USA PATRIOT Act (section 206) allows the FISA court to issue generic orders of assistance to any communications provider or similar person, instead of to a particular communications provider. This change permits the Government to implement new surveillance immediately if the FISA target changes providers in an effort to thwart surveillance. The amendment was directed at persons who, for example, attempt to defeat surveillance by changing wireless telephone providers or using pay phones.
>
> Currently, FISA requires the court to "specify" the "nature and location of each of the facilities or places at which the electronic surveillance will be directed." 50 U.S.C. § 105(c)(1)(B). Obviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and electronic mail may be accessed from any number of locations.
>
> To avoid any ambiguity and clarify Congress' intent, the conferees agreed to a provision which adds the phrase, "if known," to the end of 50 U.S.C. § 1805(c)(1)(B). The "if known" language, which follows the model of 50 U.S.C. § 1805(c)(1)(A), is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.

---

[36] 50 U.S.C. § 1805(c). The italics in 50 U.S.C. § 1805(c)(2)(B), above, indicate new language added by Section 206 of P.L. 107-56. Where circumstances suggest that a target's actions may prevent identification of a specified person, this new language appears to permit the Foreign Intelligence Surveillance Court to require a service provider, other common carrier, landlord, custodian or other persons to provide necessary assistance to the applicant for a FISA order for electronic surveillance. The heading to Section 6 of P.L. 107-56 refers to this as "roving surveillance authority." H.Rept. 107-328 calls this a "multipoint" wiretap. *Intelligence Authorization Act for Fiscal Year 2002*, 107th Cong., 1st Sess., H.Rept. 107-328, Conference Report, at 24 (Dec. 6, 2001).

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. An order under FISA for surveillance targeted against an agent of a foreign power who acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor, may be for the period specified in the order or 120 days, whichever is less.[37] 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. In addition, an extension of an order for surveillance targeted at an agent of a foreign power who acts in the United States as an officer or employee of a foreign power or as a member of a group engaged in international terrorism or activities in preparation therefore may be extended to a period not exceeding one year. 50 U.S.C. § 1805(e)(2)(A) and (B).[38]

---

[37] 50 U.S.C. § 1805(e)(1)(B), as added by Section 207 of P.L. 107-56.

[38] Section 207 of P.L. 107-56 appears to have included a mistaken citation here, referring to 50 U.S.C. § *1805(d)(2)* instead of 50 U.S.C. § *1805(e)(2)* (emphasis added). Section 314(c)(1) of P.L. 107-108 corrected the apparent error from P.L. 107-56, Section 207, so that the reference is now to 50 U.S.C. § 1805(e)(2).

Emergency situations are addressed in 50 U.S.C. § 1805(f).[39] 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 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes emergency electronic surveillance, he must require compliance with the minimization procedures required 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 72 hours from the time of the Attorney General's authorization, whichever is earliest.[40] If no judicial order approving the surveillance is issued, the information garnered may not be received in evidence or otherwise disclosed in any court

---

[39] 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, to 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(h), 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.

Section 225 of P.L. 107-56 appears to create a second subsection 1805(h), which precludes any cause of action in any court "against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA. This immunity provision is included in 50 U.S.C. § 1805, and was denominated "Immunity for Compliance with FISA Wiretap" in Section 225 of the USA PATRIOT Act, both facts which might lead one to conclude that it applied only to electronic surveillance under FISA, but this does not appear to be the view of expressed in H.Rept. 107-328, the conference report accompanying H.R. 2883, which became P.L. 107-108. P.L. 107-108 redesignated 50 U.S.C. § 1805(h) as 50 U.S.C. § 1805(i). In H.Rept. 107-328, the conferees expressed the view that "the text of section 225 refers to court orders and requests for emergency assistance 'under this act,' which makes clear that it applies to physical searches (and pen-trap requests — for which there already exists an immunity provision, 50 U.S.C. § 1842(f) — and subpoenas) as well as electronic surveillance." *Id.* at 25.

Section 314(a)(2)(C) of P.L. 107-108 changed subsection (h), which was added to 50 U.S.C. § 1805 by Section 225 of P.L. 107-56, to subsection (i). In addition, Section 314(a)(2)(D) of P.L. 107-108 added "for electronic surveillance or physical search" to the end of the newly designated 50 U.S.C. § 1805(i) before the final period.

[40] Section 314(a)(2)(B) of P.L. 107-108, the Intelligence Authorization Act for Fiscal Year 2002, H.Rept. 107-328, replaced 24 hours with 72 hours in each place that it appears in 50 U.S.C. § 1805(f).

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.[41]

---

[41] 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, 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 —

(continued...)

The uses to which information gathered under FISA may be put are addressed under 50 U.S.C. § 1806.[42] Under these provisions, disclosure, without the

---

[41] (...continued)

> (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 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).

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

(continued...)

[42] (...continued)

(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 shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that 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 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

(continued...)

[42] (...continued)

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 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

(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,[43]

---

[42] (...continued)

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.

(k) Consultation with Federal law enforcement officer

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers *or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)* to coordinate efforts to investigate or 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.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) [50 U.S.C. § 1804(a)(7)(B) (referring to a certification by the Assistant to the President for National Security Affairs or other designated certifying authority "that a significant purpose of the surveillance is to obtain foreign intelligence information")] or the entry of an order under section 105 [50 U.S.C. § 1805].

(Emphasis added.) Subsection 1806(k) was added by Section 504 of P.L. 107-56. The italicized portion of subsection 1806(k)(1), above, was added by Section 898 of the Homeland Security Act of 2002, P.L. 107-296. The term "aggrieved person," as used in connection with electronic surveillance under 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."

[43] For the definition of "aggrieved person" as that term is used with respect to targets of (continued...)

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.[44]

---

[43] (...continued)
electronic surveillance under FISA, see fn. 42, *supra*.

[44] It is worthy of note that Section 892 of the Homeland Security Act of 2002, P.L. 107-296, while not expressly amending FISA, addressed procedures for the sharing of homeland security information. It required the President to prescribe and implement procedures under which relevant federal agencies, including those in the intelligence community, would share relevant and appropriate homeland security information with other federal agencies and, where appropriate, with State and local personnel. Section 892 provided, in part:

> Sec. 892. Facilitating Homeland Security Information Sharing Procedures.
>
> (a) Procedures for Determining Extent of Sharing of Homeland Security Information. —
>
> (1) The President shall prescribe and implement procedures under which relevant Federal agencies —
>
> (A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;
>
> (B) identify and safeguard homeland security information that is sensitive but unclassified; and
>
> (C) to the extent that such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.
>
> (2) The President shall ensure that such procedures apply to all agencies of the Federal Government.
>
> (3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.
>
> (4) Such procedures shall not change the requirements and authorities to protect sources and methods.
>
> (b) Procedures for Sharing of Homeland Security Information. —
>
> (1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.
>
> (2) Each information sharing system through which information is shared under paragraph (1) shall —
>
> (A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;
>
> (B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization,

(continued...)

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

---

[44] (...continued)

> position of a recipient within an organization, or a recipient's need to know such information;
>
> (C) be configured to allow the efficient and effective sharing of information; and
>
> (D) be accessible to appropriate State and local personnel.
>
> (3) The procedures prescribed in paragraph (1) shall establish conditions on the use of information shared under paragraph (1) —
>
> (A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;
>
> (B) to ensure the security and confidentiality of such information;
>
> (C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and
>
> (D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.
>
> (4) . . . .
>
> (5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.
>
> (6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information systems —
>
> (A) to access information shared with such personnel; and
>
> (B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.
>
> (7) Under procedures prescribed jointly by the Director of National Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.
>
> . . . .

Subsection (f)(1) of Section 892 of P.L. 107-296, defined "homeland security information" to mean "information possessed by a Federal, State, or local agency" that "relates to the threat of terrorist activity;" "relates to the ability to prevent, interdict, or disrupt terrorist activity;" "would improve the identification or investigation of a suspected terrorist or terrorist organization;" "or would improve the response to a terrorist act." "State and local personnel" is defined to mean persons involved in prevention, preparation, or response for terrorist attack who fall within the following categories: "State Governors, mayors, and other locally elected officials;" "State and local law enforcement personnel and firefighters;" "public health and medical professionals;" "regional, State, and local emergency management agency personnel, including State adjutant generals;" "other appropriate emergency response agency personnel;" and "employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section."

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, 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.[45] 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.

---

[45] *But see*, United States v. Thomson, 752 F. Supp. 75, 77 (W.D. N.Y. 1990), stating that,

> If the Court determines that the surveillance was unlawfully authorized or conducted, it must order disclosure of the FISA material. 50 U.S.C. § 1806(g) . . . . In *United States v. Belfield*, 692 F.2d 141 (D.C. Cir. 1982), the court stated that "even when the government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the FISA surveillance material to ensure that no fruits thereof are being used against him." Id. at 146.

It may be noted that the Section 1806(g) does not state that a court must order disclosure of the FISA material if the court finds that the FISA electronic surveillance was unlawfully authorized or conducted. Rather, the provision in question states in pertinent part that, "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. . . ." While a district court will normally consider in camera and ex parte a motion to suppress under Subsection 1806(e) or other statute or rule to discover, disclose, or suppress information relating to a FISA electronic surveillance, Subsection 1806(f) does permit a district court, in determining the legality of a FISA electronic surveillance, to 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 to the extent necessary to make an accurate determination of the legality of the surveillance. *Belfield* indicated that a criminal defendant may seek to discover FISA surveillance material to ensure that no fruits of an illegal surveillance are being used against him, but it appears to stop short of saying that in every instance where the court finds an illegal surveillance disclosure must be forthcoming. "The language of section 1806(f) clearly anticipates that an ex parte, in camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary." *Belfield*, *supra*, 692 F.2d at 147. *See also*, United States v. Squillacote, 221 F.3d 542, 552-554 (4th Cir. 2000), *cert. denied*, 532 U.S. 971 (2001).

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.

P.L. 107-56, Section 504, added a new subsection 1806(k)(1). Under this new subsection, federal officers who conduct electronic surveillance to acquire foreign intelligence under FISA are permitted to consult with Federal law enforcement officers to coordinate investigative efforts or 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.

This new subsection indicates further that such coordination would not preclude certification as required by 50 U.S.C. § 1804(a)(7)(B) or entry of a court order under 50 U.S.C. § 1805.

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 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.[46] Each such report must

---

[46] 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 (continued...)

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.[47]

Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, created additional semiannual reporting requirements under FISA. Under the new language, the Attorney General, on a semiannual basis, must submit to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee, in a manner consistent with protection of national security, reports setting forth with respect to the preceding six month period:

> (1) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for–
>
> (A) electronic surveillance under section 105 [50 U.S.C. § 1805];
>
> (B) physical searches under section 304 [50 U.S.C. § 1824];
>
> (C) pen registers under section 402 [50 U.S.C. § 1842]; and
>
> (D) access to records under section 501 [50 U.S.C. § 1861];
>
> (2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C) [50 U.S.C. § 1801(b)(1)(C)];
>
> (3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;
>
> (4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Court of Review by the Department of Justice; and
>
> (5) copies of all decisions (not including orders) or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this Act.[48]

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. The provision makes it a defense to prosecution under this subsection if the defendant is a law

---

[46] (...continued)
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.

[47] 50 U.S.C. § 1808(a)(2).

[48] These new reporting requirements were added to the Foreign Intelligence Surveillance Act, as amended, as a new Title VI of the Act.

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.

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.

Physical searches for foreign intelligence gathering purposes. Physical searches for foreign intelligence purposes are addressed in 50 U.S.C. § 1821 *et seq.*[49] While tailored for physical searches, the provisions in many respects follow a pattern similar to that created for electronic surveillance. The definitions from 50 U.S.C. § 1801 for the terms "foreign power," "agent of a foreign power," "international terrorism," "sabotage," "foreign intelligence information," "Attorney General," "United States person," "United States," "person," and "State" also apply to foreign intelligence physical searches except where specifically provided otherwise. A "physical search" under this title means:

> any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 1801(f) of this title [50 U.S.C.], or (B) 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 1801(f) of this title.[50]

Minimization procedures also apply to physical searches for foreign intelligence purposes. Those defined under 50 U.S.C. § 1821(4) are tailored to such physical searches and, like those applicable to electronic surveillance under 50 U.S.C. § 1801(h), these procedures are designed to minimize acquisition and retention, and to prohibit dissemination, of nonpublicly available information concerning unconsenting

---

[49] The physical search provisions of FISA were added as Title III of that Act by P.L. 103-359, Title VIII, on October 14, 1994, 108 Stat. 3443. Some of these provisions were subsequently amended by P.L. 106-567, Title VI, on December 27, 2000, 114 Stat. 2852-53; and by P.L. 107-56.

[50] 50 U.S.C. § 1821(5).

U.S. persons, consistent with the needs of the United States to obtain, produce and disseminate foreign intelligence.[51]

Under 50 U.S.C. § 1822, the President, acting through the Attorney General may authorize physical searches to acquire foreign intelligence information without a court order for up to one year if the Attorney General certifies under oath that the search is solely directed at premises, property, information or materials owned by or under the open and exclusive control of a foreign power or powers.[52] For these purposes, "foreign power or powers" means a foreign government or component of a foreign government, whether or not recognized by the United States, a faction of a foreign nation or nations, not substantially composed of U.S. persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.[53] In addition, the Attorney General must certify that there is no substantial likelihood that the physical search will involve the premises, information, material or property of a U.S. person, and that the proposed minimization procedures with respect to the physical search are

---

[51] Specifically, 50 U.S.C. § 1821(4) defines "minimization procedures" with respect to physical search to mean:

> (A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, 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;
>
> (B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, 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 such foreign intelligence information or assess its importance;
>
> (C) notwithstanding subparagraphs (A) and (B), 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
>
> (D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours, unless a court order under section 1824 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.

Section 314(a)(3) of P.L. 107-108, the Intelligence Authorization Act of 2002, changed the previous 24 hour period in the minimization procedures under 50 U.S.C. § 1821(4)(D) to a 72 hour period.

[52] The President provided such authority to the Attorney General by Executive Order 12949, Section 1, 60 *Fed. Reg.* 8169 (February 9, 1995), if the Attorney General makes the certifications necessary under 50 U.S.C. § 1822(a)(1).

[53] *See* 50 U.S.C. § 1801(a)(1), (2), or (3).

consistent with 50 U.S.C. § 1821(4)(1)-(4).[54] Under normal circumstances, these minimization procedures and any changes to them are reported to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence by the Attorney General at least 30 days before their effective date. However, if the Attorney General determines that immediate action is required, the statute mandates that he advise these committees immediately of the minimization procedures and the need for them to become effective immediately. In addition, the Attorney General must assess compliance with these minimization procedures and report such assessments to these congressional committees.

The certification of the Attorney General for a search under 50 U.S.C. § 1822 is immediately transmitted under seal to the Foreign Intelligence Surveillance Court, and maintained there under security measures established by the Chief Justice of the United States with the Attorney General's concurrence, in consultation with the Director of National Intelligence. Such a certification remains under seal unless one of two circumstances arise: (1) either an application for a court order with respect to the physical search is made to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1821(4) (dealing with minimization procedures) and § 1823 (dealing with the process by which a federal officer, with the approval of the Attorney General, may apply for an order from the FISC approving a physical search for foreign intelligence gathering purposes); or (2) the certification is needed to determine the legality of a physical search under 50 U.S.C. § 1825 (dealing with use of the information so gathered).

In connection with physical searches under 50 U.S.C. § 1822, the Attorney General may direct a landlord, custodian or other specified person to furnish all necessary assistance needed to accomplish the physical search in a way that would both protect its secrecy and minimize interference with the services such person provides the target of the search. Such person may also be directed to maintain any records regarding the search or the aid provided under security procedures approved by the Attorney General and the Director of National Intelligence. The provision of any such aid must be compensated by the Government.[55] As in the case of applications for electronic surveillance under FISA, the Foreign Intelligence Surveillance Court (FISC) has jurisdiction to hear applications and grant applications with respect to physical searches under 50 U.S.C. § 1821 *et seq*. No FISC judge may hear an application already denied by another FISC judge. If an application for an order authorizing a physical search under FISA is denied, the judge denying the application must immediately provide a written statement of reasons for the denial. If the United States so moves, the record is then transmitted under seal to the court of review established under 50 U.S.C. § 1803(b). If the court of review determines that the application was properly denied, it, in turn, must provide a written statement of the reasons for its decision, which must be transmitted under seal to the Supreme

---

[54] While this is the citation cross-referenced in Section 1822, it appears that the cross-reference should read 50 U.S.C. § 1821(4)(A)-(D).

[55] 50 U.S.C. § 1822(a)(4).

Court upon petition for certiorari by the United States.[56] Any of the proceedings with respect to an application for a physical search under FISA must be conducted expeditiously, and the record of such proceedings must be kept under appropriate security measures.

The requirements for application for an order for a physical search under FISA are included in 50 U.S.C. § 1823. While tailored to a physical search, the requirements strongly parallel those applicable to electronic surveillance under 50 U.S.C. § 1804(a)(1)-(9).[57] Like Section 1804(a)(7)(B) with respect to required

---

[56] 50 U.S.C. § 1822(c), (d).

[57] Each application for an order approving such a physical search, having been approved by the Attorney General based upon his understanding that the application satisfies the criteria and requirements of 50 U.S.C. § 1821 *et seq.*, must be made by a Federal officer in writing upon oath or affirmation to a FISC judge. Under subsection (a) of Section 1823, the application must include:

> (1) the identity of the Federal officer making the application;
> (2) the authority conferred on the Attorney General by the President and the approval of the Attorney General to make the application;
> (3) the identity, if known, or a description of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
> (4) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that —
> (A) the target of the physical search is a foreign power or an agent of a foreign power;
> (B) the premises or property to be searched contains foreign intelligence information; and
> (C) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;
> (5) a statement of the proposed minimization procedures;
> (6) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;
> (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 branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate —
> (A) that the certifying official deems the information sought to be foreign intelligence information;
> (B) that *a significant purpose* of the search 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 section 1801(e) of this title; and
> (E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);

(continued...)

certifications for an application for electronic surveillance under FISA, Section 1823(a)(7)(B) was amended by P.L. 107-56, Section 218, to require that the Assistant to the President for National Security Affairs or designated Executive Branch official[58] certify, among other things, that a significant purpose (rather than "that the purpose") of the physical search is to obtain foreign intelligence information.[59] Section 1823(d) also parallels Section 1804(e) (dealing with requirements for some applications for electronic surveillance under FISA), in that, if requested in writing by the Director of the FBI, the Secretary of Defense, the Secretary of State, or the

---

[57] (...continued)

> (8) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information; and
>
> (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, premises, or property specified in the application, and the action taken on each previous application. (Emphasis added.)

Under Section 1823(b), the Attorney General may require any other affidavit or certification from any other officer in connection with an application for a physical search that he deems appropriate. Under Section 1823(c), the FISC judge to whom the application is submitted may also require that the applicant provide other information as needed to make the determinations necessary under 50 U.S.C. § 1824.

[58] In Section 2 of E.O. 12949, 60 *Fed. Reg.* 8169 (February 9, 1995), the President authorized the Attorney General to approve applications to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1823, to obtain court orders for physical searches for the purpose of collecting foreign intelligence information. In Section 3 of that executive order, the President designated the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence to make the certifications required by 50 U.S.C. § 1823(a)(7), in support of an application for a court order for a physical search for foreign intelligence purposes. None of these officials may exercise this authority to make the appropriate certifications unless he or she is appointed by the President, with the advice and consent of the Senate.

[59] Section 303(a)(7)(B) of FISA, 50 U.S.C. § 1823(a)(7)(B) (see italicized language in the quote of the statutory section in fn. 57, *supra*). Extrapolating from the U.S. Foreign Intelligence Surveillance Court of Review's interpretation of the "significant purpose" language as applied to electronic surveillance under FISA in In re Sealed Case, 310 F.3d 717, 728-38 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002), this language appears to exclude FISA as authority for a physical search where the sole purpose of an investigation is criminal prosecution. The government must have a measurable foreign intelligence purpose other than criminal prosecution, even of foreign intelligence crimes, in order to satisfy the "significant purpose" standard. This reasoning suggests that the primary purpose of the investigation may be criminal prosecution, so long as collection of foreign intelligence information is also a significant purpose of the search. As in the case of the change from "the purpose" to "a significant purpose" in the case of electronic surveillance, the parallel language change in Section 1823 with respect to physical searches may also have the effect of blurring the distinction between physical searches for foreign intelligence purposes and those engaged in for law enforcement purposes.

Director of National Intelligence,[60] the Attorney General must personally review an application for a FISA physical search if the target is one described by Section 1801(b)(2). 50 U.S.C. § 1801(b)(2) deals with targets who knowingly engage in clandestine intelligence gathering activities involving or possibly involving violations of federal criminal laws by or on behalf of a foreign power; targets who, at the direction of an intelligence service or network of a foreign power, engage in other clandestine intelligence activities involving or potentially involving federal crimes by or on behalf of a foreign power; targets who knowingly engage in sabotage or international terrorism, activities in preparation for sabotage or international terrorism, or activities on behalf of a foreign power; targets who knowingly aid, abet, or conspire with anyone to engage in any of the previously listed categories of activities; or targets who knowingly enter the United States under false identification by or on behalf or a foreign power or who assume a false identity on behalf of a foreign power while present in the United States.[61]

Should the Attorney General, after reviewing an application, decide not to approve it, he must provide written notice of his determination to the official requesting the review of the application, setting forth any modifications needed for the Attorney General to approve it. The official so notified must supervise the making of the suggested modifications if the official deems them warranted. Unless the Attorney General or the official involved is disabled or otherwise unable to carry out his or her respective responsibilities under Section 1823, those responsibilities are non-delegable.

As in the case of the issuance of an order approving electronic surveillance under 50 U.S.C. § 1805(a), certain findings by the FISC judge are required before an order may be forthcoming authorizing a physical search for foreign intelligence information under 50 U.S.C. § 1824(a). Once an application under Section 1823 has been filed, an FISC judge must enter an ex parte order, either as requested or as modified, approving the physical search if the requisite findings are made. These include findings that:

> (1) the President has authorized the Attorney General to approve applications for physical searches for foreign intelligence purposes;
> (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 physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
> > (B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;

---

[60] The authority of these officials to make such a written request is non-delegable except where such official is disabled or unavailable. Each must make provision in advance for delegation of this authority should he or she become disabled or unavailable. 50 U.S.C. § 1823(d)(1)(B) and (C).

[61] See fn. 21, *supra*.

> (4) the proposed minimization procedures meet the definition of minimization contained in this subchapter; and
>
> (5) the application which has been filed contains all statements and certifications required by section 1823 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 1823(a)(7)(E) of this title and any other information furnished under section 1823(c) of this title.

Like Section 1805(b) regarding electronic surveillance under FISA, a FISC judge making a probable cause determination under Section 1824 may consider the target's past activities, plus facts and circumstances pertinent to the target's present or future activities.[62]

As in the case of an order under 50 U.S.C. § 1805(c) with respect to electronic surveillance, an order granting an application for a physical search under FISA must meet statutory requirements in 50 U.S.C. § 1824(c) as to specifications and directions. An order approving a physical search must specify:

> (A) the identity, if known, or a description of the target of the physical search;
>
> (B) the nature and location of each of the premises of property to be searched;
>
> (C) the type of information, material, or property to be seized, altered, or reproduced;
>
> (D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and
>
> (E) the period of time during which the physical searches are approved; . . . .

In addition, the order must direct:

> (A) that the minimization procedures be followed;
>
> (B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing to the target of the physical search;
>
> (C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence[63] any records concerning the search or the aid furnished that such person wishes to retain;
>
> (D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and

---

[62] 50 U.S.C. § 1824(b).

[63] Section 1071(e) replaced "Director of Central Intelligence" with "Director of National Intelligence" in each place where it appeared in FISA. This was one of those locations.

> (E) that the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.[64]

Subsection 1824(d) sets the limits on the duration of orders under this section and makes provision for extensions of such orders if certain criteria are met.[65] Subsection 1824(e) deals with emergency orders for physical searches. It permits the Attorney General, under certain circumstances, to authorize execution of a physical search if the Attorney General or his designee informs a FISC judge that the decision to execute an emergency search has been made, and an application under 50 U.S.C. § 1821 *et seq.* is made to that judge as soon as possible, within 72 hours[66] after the Attorney General authorizes the search. The Attorney General's decision to authorize such a search must be premised upon a determination that "an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence

---

[64] 50 U.S.C. § 1824(c)(1), (2).

[65] P.L. 107-56, Section 207(a)(2), amended 50 U.S.C. § 1824(d)(1) so that it provided:

> (1) An order under this section may approve a physical search for the period necessary to achieve its purpose, or for *90* days, whichever is less, except that *(A)* an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a) [50 U.S.C. § 1801(b)(1)(A)], for the period specified in the application or for one year, whichever is less, *and (B) an order under this section for a physical search against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)] may be for the period specified in the application or for 120 days, whichever is less*.

The language in italics reflects the changes made by P.L. 107-56. The 90 day time period reflected in the first sentence replaced earlier language which provided for 45 days.

Section 207(b)(2) of P.L. 107-56 amended 50 U.S.C. § 1824(d)(2) to provide:

> (2) Extensions of an order issued under this title [50 U.S.C. §§ 1821 et seq.] may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in section 101(a)(5) or (6) [50 U.S.C. § 1801(a)(5) or (6)], or against a foreign power, as defined in section 101(a)(4) [50 U.S.C. § 1801(a)(4)] , that is not a United States person, *or against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)]*, may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(Emphasis added.) Under subsection 1824(d)(3), the judge, at or before the end of the time approved for a physical search or for an extension, or at any time after the physical search is carried out, may review circumstances under which information regarding U.S. persons was acquired, retained, or disseminated to assess compliance with minimization techniques.

[66] Section 314(a)(4) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, amended 50 U.S.C. § 1824(e) by striking "24 hours" where it occurred and replacing it with "72 hours."

information before an order authorizing such search can with due diligence be obtained," and "the factual basis for issuance of an order under this title [50 U.S.C. § 1821 *et seq.*] to approve such a search exists."[67] If such an emergency search is authorized by the Attorney General, he must require that the minimization procedures required for issuance of a judicial order for a physical search under 18 U.S.C. § 1821 *et seq.* be followed.[68] If there is no judicial order for a such a physical search, then the search must terminate on the earliest of the date on which the information sought is obtained, the date on which the application for the order is denied, or the expiration of the 72 hour period from the Attorney General's authorization of the emergency search.[69] If an application for approval is denied or if the search is terminated and no order approving the search is issued, then neither information obtained from the search nor evidence derived from the search may be used in evidence or disclosed in any

> . . . trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 302 [50 U.S.C. § 1822].[70]

Subsection 1824(f) requires retention of applications made and orders granted under 50 U.S.C. § 1821 *et seq.*, for a minimum of 10 years from the date of the application.

Like 50 U.S.C. § 1806 with respect to electronic surveillance under FISA, 50 U.S.C. § 1825 restricts and regulates the uses of information secured under a FISA physical search. Such information may only be used or disclosed by Federal officers or employees for lawful purposes. Federal officers and employees must comply with minimization procedures if they use or disclose information gathered from a physical search under FISA concerning a United States person.[71] If a physical search involving the residence of a United States person is authorized and conducted under 50 U.S.C. § 1824, and at any time thereafter the Attorney General determines that there is no national security interest in continuing to maintain the search's secrecy, the Attorney General must provide notice to the United States person whose residence was searched. This notice must include both the fact that the search pursuant to FISA was conducted and the identification of any property of that person which was seized,

---

[67] 50 U.S.C. § 1824(e)(1)(A)(i) and (ii). *See* fn.66, *supra*, regarding substitution of "72 hours" for "24 hours" in Subsection 50 U.S.C. § 1824(e)(3)(C) by P.L. 107-108, Sec. 314(a)(4).

[68] 50 U.S.C. § 1824(e)(2).

[69] 50 U.S.C. § 1824(e)(3).

[70] 50 U.S.C. § 1824(e)(4).

[71] 50 U.S.C. § 1825(a).

altered, or reproduced during the search.[72] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1821 *et seq.*, must be accompanied by a statement that such information and any derivative information may only be used in a criminal proceeding with advance authorization from the Attorney General.[73]

The notice requirements relevant to intended use or disclosure of information gleaned from a FISA physical search or derivative information, are similar to those applicable where disclosure or use of information garnered from electronic surveillance is intended. If the United States intends to use or disclose information gathered during or derived from a FISA physical search in a trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body or other authority of the United States against an aggrieved person, the United States must first give notice to the aggrieved person, and the court or other authority.[74] Similarly, if a State or political subdivision of a state intends to use or disclose any information obtained or derived from a FISA physical search in any trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body, or other State or political subdivision against an aggrieved person, the State or locality must notify the aggrieved person, the pertinent court or other authority where the information is to be used, and the Attorney General of the United States of its intention to use or disclose the information.[75] An aggrieved person may move to suppress evidence obtained or derived from a FISA physical search on one of two grounds: that the information was unlawfully acquired; or that the physical search was not made in conformity with an order of authorization or approval. Such a motion to suppress must be made before the trial, hearing or other proceeding involved unless the aggrieved person had no opportunity to make the motion or was not aware of the grounds of the motion.[76]

In camera, ex parte review by a United States district court may be triggered by receipt of notice under Subsections 1825(d) or (e) by a court or other authority; the making of a motion to suppress by an aggrieved person under Subsection 1825(f); or the making of a motion or request by an aggrieved person under any other federal or state law or rule before any federal or state court or authority to discover or obtain applications, orders, or other materials pertaining to a physical search authorized under FISA or to discover, obtain, or suppress evidence or information obtained or derived from a FISA physical search. If the Attorney General files an affidavit under oath that disclosure of any adversary hearing would harm U.S. national security, the U.S. district court receiving notice or before whom a motion or request is pending, or, if the motion is made to another authority, the U.S. district court in the same district as that authority, shall review in camera and ex parte the application, order,

---

[72] 50 U.S.C. § 1825(b).

[73] 50 U.S.C. § 1825(c).

[74] 50 U.S.C. § 1825(d). "Aggrieved person," as defined in 50 U.S.C. § 1821(2), "means a person whose premises, property, information, or material is the target of a physical search or any other person whose premises, property, information, or material was subject to physical search."

[75] 50 U.S.C. § 1825(e).

[76] 50 U.S.C. § 1825(f).

and such other materials relating to the physical search at issue needed to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. If the court finds it necessary to make an accurate determination of the legality of the search, the court may disclose portions of the application, order, or other pertinent materials to the aggrieved person under appropriate security procedures and protective orders, or may require the Attorney General to provide a summary of such materials to the aggrieved person.[77]

If the U.S. district court makes a determination that the physical search was not lawfully authorized or conducted, then it must "suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person." If, on the other hand, the court finds that the physical search was lawfully authorized or conducted, the motion of the aggrieved person will be denied except to the extent that due process requires discovery or disclosure.[78]

If the U.S. district court grants a motion to suppress under 50 U.S.C. § 1825(h); deems a FISA physical search unlawfully authorized or conducted; or orders review or grants disclosure of applications, orders or other materials pertinent to a FISA physical search, that court order is final and binding on all federal and state courts except a U.S. Court of Appeals or the U.S. Supreme Court.[79]

As a general matter, where an emergency physical search is authorized under 50 U.S.C. § 1824(d), and a subsequent order approving the resulting search is not obtained, any U.S. person named in the application and any other U.S. persons subject to the search that the FISC judge deems appropriate in the interests of justice must be served with notice of the fact of the application and the period of the search, and must be advised as to whether information was or was not obtained during that period.[80] However, such notice may be postponed or suspended for a period not to exceed 90 days upon an ex parte showing of good cause to the judge, and, upon further good cause shown, the court must forego such notice altogether.[81]

Section 504(b) of P.L. 107-56, added a new 50 U.S.C. § 1825(k) to the statute, which deals with consultation by federal officers doing FISA searches with federal law enforcement officers. Section 899 of the Homeland Security Act of 2002, P.L. 107-296 expanded this authority to also permit consultation with "law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)." Under this new language, as amended, federal officers "who conduct physical searches to acquire

---

[77] 50 U.S.C. § 1825(g).

[78] 50 U.S.C. § 1825(h).

[79] 50 U.S.C. § 1825(i).

[80] 50 U.S.C. § 1825(j)(1).

[81] 50 U.S.C. § 1825(j)(2).

foreign intelligence information" under 50 U.S.C. § 1821 *et seq.*, may consult with federal law enforcement officers or state or local law enforcement personnel:

> . . . to coordinate efforts to investigate or 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.[82]

Such coordination does not preclude certification required under 50 U.S.C. § 1823(a)(7) or entry of an order under 50 U.S.C. § 1824.[83]

50 U.S.C. § 1826 provides for semiannual congressional oversight of physical searches under FISA.[84] The Attorney General is directed to "fully inform" the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate with respect to all physical searches conducted under 50 U.S.C. § 1821 *et seq.* Also on a semiannual basis, the Attorney General is required to provide a report to those committees and to the House and Senate Judiciary Committees setting forth: the total number of applications for orders approving FISA physical searches during the preceding six month period; the total number of those orders granted, modified, or denied; the number of such physical searches involving the residences, offices, or personal property of United States persons; and the number of occasions, if any, the Attorney General gave notice under 50 U.S.C. § 1825(b).[85]

Section 1827 imposes criminal sanctions for intentionally executing a physical search for foreign intelligence gathering purposes under color of law within the United States except as authorized by statute. In addition, criminal penalties attach to a conviction for intentionally disclosing or using information obtained by a physical search under color of law within the United States for the purpose of gathering intelligence information, where the offender knows or has reason to know that the information was obtained by a physical search not authorized by statute. In either case, this section provides that a person convicted of such an offense faces a fine of not more than $10,000,[86] imprisonment for not more than five years or both. Federal jurisdiction attaches where the offense is committed by an officer or

---

[82] 50 U.S.C. § 1825(k)(1).

[83] 50 U.S.C. § 1825(k)(2).

[84] See also the discussion of new reporting requirements added by Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, discussed at fn. 48, *supra*, and accompanying text.

[85] *See* fn. 72, *supra*, and accompanying text.

[86] This section was added in 1994 as Title III, Section 307 of P.L. 95-511, by P.L. 103-359, Title VIII, § 807(a)(3), 108 Stat. 3452. If a fine were to be imposed under the general fine provisions 18 U.S.C. § 3571, rather than under the offense provision, the maximum fine would be $250,000 for an individual.

employee of the United States. It is a defense to such a prosecution if the defendant was a law enforcement or investigative officer engaged in official duties and the physical search was authorized and conducted pursuant to a search warrant or court order by a court of competent jurisdiction.

In addition, an aggrieved person other than a foreign power or an agent of a foreign power as defined under section 1801(a) or 1801(b)(1)(A),[87] whose premises, property, information, or material within the United States was physically searched under FISA; or about whom information obtained by such a search was disclosed or used in violation of 50 U.S.C. § 1827, may bring a civil action for actual damages, punitive damages, and reasonable attorney's fees and other investigative and litigation costs reasonably incurred.[88]

In times of war, the President, through the Attorney General, may authorize physical searches under FISA without a court order to obtain foreign intelligence information for up to 15 days following a declaration of war by Congress.[89]

Pen registers or trap and trace devices[90] used for foreign intelligence gathering purposes. Title IV of FISA, 50 U.S.C. § 1841 *et seq.*, was added in 1998, amended by P.L. 107-56,[91] and amended further by Section 314(5) of P.L. 107-108. Under 50 U.S.C. § 1842(a)(1), notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may apply for an order or extension of an order authorizing or approving the installation and use of a pen register or trap and trace device "*for any investigation to protect against international terrorism or clandestine intelligence activities, provided such investigation of a United States person is not conducted solely upon*

---

[87] For definitions, *see* fn. 21, *supra.*

[88] 50 U.S.C. § 1828. Actual damages are defined to be "not less than liquidated damages of $1,000 or $100 per day for each violation, whichever is greater." 50 U.S.C. § 1828(1).

[89] 50 U.S.C. § 1829.

[90] Under 50 U.S.C. § 1841(2), the terms "pen register" and "trap and trace device" are given the meanings in 18 U.S.C. § 3127. Under Section 3127, "pen register"

> . . . means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; . . . .

As defined by 18 U.S.C. § 3127(4), "trap and trace device" "means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 50 U.S.C. § 1841 is the section that defines terms applicable to the pen register and trap and trace device portions of FISA.

[91] Title IV of FISA was added by Title VI, Sec. 601(2) of P.L. 105-272, on October 20, 1998, 112 Stat. 2405-2410, and amended by P.L. 107-56 and by P.L. 107-108.

the basis of activities protected by the first amendment to the Constitution" conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to E.O. 12333 or a successor order.[92] This authority is separate from the authority to conduct electronic surveillance under 50 U.S.C. § 1801 *et seq.*[93]

Each such application is made in writing upon oath or affirmation to a FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant orders approving installation of pen registers or trap and trace devices on behalf of a FISC judge. The application must be approved by the Attorney General or a designated attorney for the Government. Each application must identify the federal officer seeking to use the pen register or trap and trace device covered by the application. It must also include a certification by the applicant "*that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.*"[94]

Under 50 U.S.C. § 1842, as amended by P.L. 107-56, pen registers and trap and trace devices may now be installed and used not only to track telephone calls, but also other forms of electronic communication such as e-mail. Once an application is made under Section 1842, the judge[95] must enter an ex parte order[96]as requested or as

---

[92] The italicized language was added by P.L. 107-56, Section 214(a)(1), replacing language which had read "for any investigation to gather foreign intelligence information or information concerning international terrorism."

[93] 50 U.S.C. § 1842(a)(2).

[94] This language, added by P.L. 107-56, Section 214(a)(2), replaced stricken language which read:

> (2) a certification by the applicant that the information to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General; and
> (3) information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with —
>
> (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or
>
> (B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

[95] This section refers simply to "judge." In light of 50 U.S.C. § 1842(b), it would appear that this may refer to either a FISC judge or a U.S. magistrate judge designated by the Chief Justice under Section 1842(b)(2) to hear applications for and grant orders approving (continued...)

[95] (...continued)
installation and use of pen registers or trap and trace devices on behalf of a FISC judge. The legislative history on this provision does not appear to clarify this point. The language was included in the bill reported out as an original measure by the Senate Select Committee on Intelligence, S. 2052, as Sec. 601. The Committee's report, S.Rept. 105-185, indicates that magistrate judges were included in the legislation to parallel their use in connection with receipt of applications and approval of pen registers and trap and trace devices in the context of criminal investigations, but reflected the Committee's understanding that the authority provided in the legislation to designate magistrate judges to consider applications for pen registers and trap and trace devices in the foreign intelligence gathering context would be closely monitored by the Department of Justice and this designation authority would not be exercised until the Committee was briefed on the compelling need for such designations, as reflected, for example, through statistical information on the frequency of applications to the FISC under the new procedure. S.Rept. 105-185, at 28 (May 7, 1998). The provision authorizing the use of pen registers and trap and trace devices in foreign intelligence and international terrorism investigations, Sec. 601 of the bill as passed, was among those included in the conference version of H.R. 3694 which was passed in lieu of S. 2052. H. Conference Rept. 105-80, at 32 (October 5, 1998).

[96] Under 50 U.S.C. § 1842(d)(2)(A), such an order

> *(A) shall specify —*
>
> *(i) the identity, if known, of the person who is the subject of the investigation;*
>
> *(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;*
>
> *(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.*
>
> (B) shall direct that —
>
> (i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;
>
> (ii) such provider, landlord, custodian, or other person —
>
> (I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and
>
> (II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and
>
> (iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance.

(continued...)

modified approving the installation and use of a pen register or trap and trace device if the application meets the requirements of that section.

Section 1843 of Title 18 of the United States Code focuses upon authorization for installation and use of a pen register or trap and trace device under FISA during specified types of emergencies. This provision applies when the Attorney General makes a reasonable determination that:

> (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain *foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution* before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and
>
> (2) the factual basis for issuance of an order under section 1842(c) of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.[97]

Upon making such a determination, the Attorney General may authorize the installation and use of a pen register or trap and trace device for this purpose if two criteria are met. First, the Attorney General or his designee must inform a judge

---

[96] (...continued)
The italicized portions of this section reflect amended language from P.L. 107-56, Section 214 (a)(4). In 50 U.S.C. § 1842(d)(2)(B)(ii)(II), the reference to the "Director of National Intelligence" replaced a reference to the "Director of Central Intelligence" pursuant to Section 1071(e) of P.L. 108-458.

P.L. 107-108, Section 314(a)(5)(B), replaced "of a court" at the end of 50 U.S.C. § 1842(f) with "of an order issued," so that the language now reads:

> (f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance with the terms *of an order issued* under this section.

(Emphasis added.) *Cf.*, 50 U.S.C. § 1805(i), which contains an immunity grant which, at first blush would appear to apply only to electronic surveillance under FISA, but which has been interpreted at page 25 of H.Rept. 107-328, the conference report accompanying H.R. 2883 (the conference version of which became P.L. 107-108) to apply to electronic surveillance, physical searches and pen register and trap and trace devices. This subsection was added as 50 U.S.C. § 1805(h) by Section 225 of P.L. 107-56, and redesignated 50 U.S.C. § 1805(i) by Section 314(a)(2)(C) of P.L. 107-108. See discussion at fn. 39, *supra*.

[97] 50 U.S.C. § 1843(b) (italics reflect language added by P.L. 107-56, § 214(b)(2), in place of language which read "foreign intelligence information or information concerning international terrorism.") Similar language was inserted in 50 U.S.C. § 1843(a) by P.L. 107-56, § 214(b)(1), in place of language that paralleled that stricken from subsection 1843(b).

referred to in Section 1842(b)[98] at the time of the emergency authorization that the decision to install and use the pen register or trap and trace device has been made. Second, an application for a court order authorizing a pen register or trap and trace device under 50 U.S.C. § 1842(a)(1) must be made to the judge as soon as practicable, but no later that 48 hours after the emergency authorization.[99] If no order approving the installation and use of a pen register or trap and trace device is forthcoming, then the installation and use of such pen register or trap and trace device must terminate at the earlier of the time when the information sought is obtained, the time when the application for the order is denied under 50 U.S.C. § 1842, or the expiration of 48 hours from the time the Attorney General made his emergency authorization.[100]

If an application for an order sought under Section 1843(a)(2) is denied, or if the installation and use of the pen register or trap and trace device is terminated, and no order approving it is issued under 50 U.S.C. § 1842(b)(2), then no information obtained or evidence derived from the use of the pen register or trap and trace device may be received in evidence or disclosed in any trial, hearing or other proceeding in any court, grand jury, department, office, agency, regulatory body, legislative committee or other federal state or local authority. Furthermore, in such circumstances, no information concerning a United States person acquired from the use of the pen register or trap and trace device may later be used or disclosed in any other way by federal officers or employees without consent of the U.S. person involved, with one exception. If the Attorney General approves the disclosure because the information indicates a threat of death or serious bodily harm to anyone, then disclosure without consent of the U.S. person involved is permitted.[101]

If Congress declares war, then, notwithstanding any other provision of law, the President, through the Attorney General, may authorize use of a pen register or trap and trace device without a court order to acquire foreign intelligence information for up to 15 calendar days after the declaration of war.[102]

50 U.S.C. § 1845 sets parameters with respect to the use of information obtained through the use of a pen register or trap and trace device under 50 U.S.C. § 1841 *et seq.* Federal officers and employees may only use or disclose such information with respect to a U.S. person without the consent of that person in accordance with Section 1845.[103] Any disclosure by a Federal officer or employee of information acquired pursuant to FISA from a pen register or trap and trace device must be for a lawful purpose. [104] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1841 *et seq.* is only permitted where the disclosure is accompanied by a

---

[98] See discussion of the term "judge" as used in Section 1842(b) in fn. 94, *supra*.

[99] 50 U.S.C. § 1843(a).

[100] 50 U.S.C. § 1843(c)(1).

[101] 50 U.S.C. § 1843(c)(2).

[102] 50 U.S.C. § 1844.

[103] 50 U.S.C. § 1845(a)(1).

[104] 50 U.S.C. § 1845(a)(2).

statement that the information and any derivative information may only be used in a criminal proceeding with the advance authorization of the Attorney General.[105]

Under 50 U.S.C. § 1845(c), when the United States intends to enter into evidence, use, or disclose information obtained by or derived from a FISA pen register or trap and trace device against an aggrieved person[106] in any federal trial, hearing, or proceeding, notice requirements must be satisfied. The Government, before the trial, hearing, or proceeding or a reasonable time before the information is to be proffered, used or disclosed, must give notice of its intent both to the aggrieved person involved[107] and to the court or other authority in which the information is to be disclosed or used.

If a state or local government intends to enter into evidence, use, or disclose information obtained or derived from such a trap and trace device against an aggrieved person in a state or local trial, hearing or proceeding, it must give notice to the aggrieved person and to the Attorney General of the United States of the state or local government's intent to disclose or use the information.[108]

The aggrieved person in either case may move to suppress the evidence obtained or derived from a FISA pen register or trap and trace device on one of two grounds: that the information was unlawfully acquired; or that the use of the pen register or trap and trace device was not made in conformity with an order of authorization or approval under 50 U.S.C. § 1841 *et seq*.[109]

If notice is given under 50 U.S.C. §§ 1845(c) or (d), or a motion or request is made to suppress or to discover or obtain any applications, orders, or other materials relating to use of a FISA pen register or trap and trace device or information obtained by or derived from such use, the Attorney General may have national security concerns with respect to the effect of such disclosure or of an adversary hearing. If

---

[105] 50 U.S.C. § 1845(b).

[106] "Aggrieved person" is defined in 50 U.S.C. § 1841(3) for purposes of 50 U.S.C. § 1841 *et seq.* as any person:

> (A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by subchapter IV [50 U.S.C. § 1841 et seq.]; or
>
> (B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by subchapter IV to capture incoming electronic or other communications impulses.

[107] The statute refers to notice to the "aggrieved person." Here it is using this term in the context of a pen register or trap and trace device under FISA (see fn. 90 for the applicable definition of "pen register" and "trap and trace device" in 50 U.S.C. § 1841(2) and fn. 106 for the applicable definition of "aggrieved person" in 50 U.S.C.§ 1841(3), *supra)*. The term "aggrieved person" is also defined in both 50 U.S.C. §§ 1801(k) (in the context of electronic surveillance, see fn. 42, *supra*) and 1825(d) (in the context of a physical search, see fn. 74, *supra*).

[108] 50 U.S.C. § 1845(d).

[109] 50 U.S.C. § 1845(e).

he files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, the United States district court in which the motion or request is made, or where the motion or request is made before another authority, the U.S. district court in the same district, shall review *in camera* and *ex parte* the application, order, and other relevant materials to determine whether the use of the pen register or trap and trace device was lawfully authorized and conducted.[110] In so doing, the court may only disclose portions of the application, order or materials to the aggrieved person or order the Attorney General to provide the aggrieved person with a summary of these materials if that disclosure is necessary to making an accurate determination of the legality of the use of the pen register or trap and trace device.[111]

Should the court find that the pen register or trap and trace device was not lawfully authorized or conducted, it may suppress the unlawfully obtained or derived evidence or "otherwise grant the motion of the aggrieved person."[112] On the other hand, if the court finds the pen register or trap and trace device lawfully authorized and conducted, it may deny the aggrieved person's motion except to the extent discovery or disclosure is required by due process.[113] Any U.S. district court orders granting motions or request under Section 1845(g), finding unlawfully authorized or conducted the use of a pen register or trap and trace device, or requiring review or granting disclosure of applications, orders or other materials regarding installation and use of a pen register or trap and trace device are deemed final orders. They are binding on all federal and state courts except U.S. courts of appeals and the U.S. Supreme Court.[114]

Section 1846 deals with congressional oversight of the use of FISA pen registers and trap and trace devices.[115] It requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all FISA uses of pen registers and trap and trace devices. In addition, the Attorney General, on a semi-annual basis, must report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee on the total number of applications made for orders approving the use of such pen registers and trap and trace devices and the total number of such orders granted, modified, or denied during the previous six month period.

Access to certain business records for foreign intelligence purposes. Added in 1998, Title V of FISA, 50 U.S.C. § 1861 *et seq.*, was

---

[110] 50 U.S.C. § 1845(f)(1).

[111] 50 U.S.C. § 1845(f)(2).

[112] 50 U.S.C. § 1845(g)(1).

[113] 50 U.S.C. § 1845(g)(2).

[114] 50 U.S.C. § 1845(h).

[115] See also Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, which amended FISA to add additional reporting requirements. These new reporting requirements are discussed at fn. 48, *supra*, and accompanying text.

substantially changed by P.L. 107-56 and modified further by P.L. 107-108.[116]

---

[116] Title V of FISA was added by Title VI, Sec. 602, of P.L. 105-272, on October 20, 1998, 112 Stat. 2411-12, and significantly amended by P.L. 107-56 and P.L. 107-108. The prior version of 50 U.S.C. § 1861 provided definitions for "foreign power," "agent of a foreign power," "foreign intelligence information," "international terrorism," and "Attorney General," "common carrier," "physical storage facility," "public accommodation facility," and "vehicle rental facility" for purposes of 50 U.S.C. § 1861 *et seq*. The prior version of Section 1862 was much more narrowly drawn than the new version added in P.L. 107-56 and amended by P.L. 107-108. The earlier version read:

> (a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.
>
> (b) Each application under this section —
>
> (1) shall be made to —
>
> (A) a judge of the court established by section 1803(a) of this title; or
>
> (B) a United States Magistrate Judge under chapter 43 of Title 28 [28 U.S.C. § 631 *et seq.*], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the release of records under this section on behalf of a judge of that court; and
>
> (2) shall specify that —
>
> (A) the records concerned are sought for an investigation described in subsection (a); and
>
> (B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.
>
> (c) (1) Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application satisfied the requirements of this section.
>
> (2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).
>
> (d) (1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).
>
> (2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility , physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of Investigation has sought or obtained records pursuant to an order under this section.

(continued...)

Although denominated "access to certain business records for foreign intelligence and international terrorism investigations," the reach of Section 1861, as amended by the USA PATRIOT Act and P.L. 107-108, is now substantially broader than business records alone. Under 50 U.S.C. § 1861(a)(1), the Director of the FBI, or his designee (who must be at the Assistant Special Agent in Charge level or higher in rank) may apply for an order requiring

> . . . the production of any tangible things (including books, records, papers, documents, and other items) for an investigation *to obtain foreign intelligence information not concerning a United States person or* to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[117]

---

[116] (...continued)
Congressional oversight was covered under the prior provisions by 50 U.S.C. §1863, which was similar, but not identical to the new Section 1862. The former Section 1863 stated:

> (a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all request for records under this subchapter [50 U.S.C. § 1861 *et seq.*].
>
> (b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period —
>
> (1) the total number of applications made for orders approving requests for records under this subchapter [50 U.S.C. § 1861 *et seq.*]; and
>
> (2) the total number of such orders either granted, modified, or denied.

[117] The italicized portion of Section 1861(a)(1) was added by Section 314(a)(6) of P.L. 107-108. H.Rept. 107-328, the conference report to accompany H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), at page 24, describes the purpose of this addition as follows:

> Section 215 of the USA PATRIOT Act of 2001 amended title V of the FISA, adding a new section 501 [50 U.S.C. § 1861]. Section 501(a) now authorizes the director of the FBI to apply for a court order to produce certain records "for an investigation to protect against international terrorism or clandestine intelligence activities." Section 501(b)(2) directs that the application for such records specify that the purpose of the investigation is to "obtain foreign intelligence information not concerning a United States person." However, section 501(a)(1), which generally authorizes the applications, does not contain equivalent language. Thus, subsections (a)(1) and (b)(2) now appear inconsistent.
>
> The conferees agreed to a provision which adds the phrase "to obtain foreign intelligence information not concerning a United States person or" to section 501(a)(1). This would make the language of section 501(a)(1) consistent with the legislative history of section 215 of the USA PATRIOT Act (*see* 147 Cong. Rec. S11006 (daily ed. Oct. 25, 2001) (sectional analysis)) and with the language of section 214 of the USA PATRIOT Act (authorizing an application for an order to use pen registers and trap and trace devices to "obtain foreign

(continued...)

Subsection 1861(a)(2) requires that such an investigation must be conducted under guidelines approved by the Attorney General under E.O. 12333 or a successor order and prohibits such an investigation of a United States person based solely upon First Amendment protected activities.

An application for an order under Section 1861 must be made to an FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant such orders for the production of tangible things on behalf of an FISC judge.[118] The application must specify that the "records"[119] are sought for "an authorized investigation conducted in accordance with [50 U.S.C. § 1862(a)(2)] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[120] When such an application is made, the judge must enter an *ex parte* order "as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section."[121] Such an order shall not disclose that it is issued for purposes of an investigation under 50 U.S.C. § 1861(a).[122] Subsection 1861(d) prohibits any person to disclose that the FBI has sought or obtained tangible things under Section 1861, except where the disclosure is made to persons necessary to the production of tangible things involved. Subsection 1861(e) precludes liability for persons who, in good faith, produce tangible things under such a Section 1861 order. It further indicates that production does not constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1862 deals with congressional oversight.[123] Subsection 1862(a) requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence

---

[117] (...continued)
intelligence information not concerning a United States person.").

[118] 50 U.S.C. § 1861(b)(1).

[119] While the language refers to "records," it is worthy of note that the authority conferred upon the Director of the FBI or his designee under Section 1861(a) encompasses applications for orders requiring production of "any tangible thing (including books, records, papers, documents, and other items)." One might argue, therefore, that for Subsection 1861(a)(1) and Subsection 1861(b)(2) to be read in harmony, a court might interpret "records" more broadly to cover "any tangible thing." On the other hand, if, by virtue of the specific reference in Subsection 1861(a)(1) to "records" as only one of many types of "tangible things," the term "records" in Subsection 1861(b)(2) were to be read narrowly, it might lead to some confusion as to the nature and scope of any specification that might be required where an application seeking production of types of tangible things other than records is involved.

[120] 50 U.S.C. § 1861(b)(2).

[121] 50 U.S.C. § 1861(c)(1).

[122] 50 U.S.C. § 1861(c)(2).

[123] See also Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, which added new reporting requirements. For a discussion of these additional reporting requirements, see fn. 48, *supra*, and accompanying text.

regarding all request for production of tangible things under Section 1861.[124] Subsection 1862(b) requires the Attorney General to report to the House and Senate Judiciary Committees on the total number of applications for Section 1861 orders for production of tangible things and on the total number of such orders granted, modified, or denied during the previous six months.

New Private Right of Action

In addition to provisions which amended FISA explicitly, other provisions of the USA PATRIOT Act touched upon FISA, at least tangentially. For example, Section 223 of the act, among other things, created a new 18 U.S.C. § 2712. This new section, in part, created an exclusive private right of action for any person aggrieved by any willful violation of sections 106(a), 305(a), or 405(a) of FISA (50 U.S.C. §§ 1806(a), 1825(a), 1845(a), respectively) to be brought against the United States in U.S. district court to recover money damages. Such monetary relief would amount to either actual damages or $10,000, whichever is greater; and reasonably incurred litigation costs. It also set forth applicable procedures.[125]

---

[124] Section 314(a)(7) of P.L. 107-108 corrected two references in 50 U.S.C. § 1862 as passed in the USA PATRIOT Act. P.L. 107-108 replaced "section 1842 of this title" with "section 1861 of this title," in both places in 50 U.S.C. § 1862 where it appeared.

[125] Another provision, Section 901 of the USA PATRIOT Act, amended 50 U.S.C. § 403-3(c) (Section 103(c) of the National Security Act of 1947) regarding the responsibilities of the Director of Central Intelligence (DCI). The amendment added to those authorities and responsibilities, placing upon the DCI the responsibility to establish

> . . . requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that Act unless otherwise authorized by statute or Executive order.

Section 1011 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L.108-458, amended Title I of the National Security Act of 1947, 50 U.S.C. § 402 et seq., to strike the previous Sections 102 through 104 of the Act 50 U.S.C. §§ 403, 403-1, 403-3, and 403-4, and insert new Sections 102 through 104A. The new Section 102 created the position of Director of National Intelligence (DNI). Section 102A outlined authorities and responsibilities of the position. Under the new Section 102A(f)(6) of the National Security Act, the DNI was given responsibility:

> to establish requirements and priorities for foreign intelligence information to be collected under [FISA], and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that act is disseminated so that it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that act unless otherwise authorized by statute or Executive order.

(continued...)

USA PATRIOT Act Sunset Provision

Section 224 of the USA PATRIOT Act set a sunset for many of the provisions in P.L. 107-56 of December 31, 2005. Among those provisions which will sunset pursuant to this are all of the amendments to FISA in P.L. 107-56, and subsequent amendments thereto, except the provision which increased the number of FISC judges from 7 to 11 (Section 208 of P.L. 107-56). Section 224 also excepts from the application of the sunset provision any particular foreign intelligence investigations that began before December 31, 2005, or any criminal offenses or potential offenses which began or occurred before December 31, 2005. As to those particular investigations or offenses, applicable provisions would continue in effect. The sunset provision in Section 224 of P.L. 107-56 and the exceptions thereto also apply to the expansion, under Section 6001 of P.L. 108-458, of the definition of "agent of a foreign power" in 50 U.S.C. § 1801(b)(1)(C) to include any person other than a U.S. person who engages in international terrorism or activities in preparation for international terrorism.

Recent Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review

The FISC Decision

Summary. In its May 17, 2002, decision, the FISC considered a government motion for the court "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion."[126] The court viewed the new intelligence sharing procedures under review as proposed new Attorney General minimization procedures. In a memorandum and order written by the then Presiding Judge, U.S. District Court Judge Royce Lamberth, issued on the last day of his tenure on the FISC, and concurred in by all of the judges then sitting on the FISC, the FISC granted the Department of Justice (DOJ) motion with significant modifications to section II.B. of what the FISC characterized as the proposed minimization procedures. The court required a continuation of the Attorney

---

[125] (...continued)
New Section 102A(f)(8) of the National Security Act, as enacted by P.L. 108-458, Section 1011, provided that, "Nothing in this act shall be construed as affecting the role of the Department of Justice or the Attorney General with respect to applications under the Foreign Intelligence Surveillance Act." Section 1071(e) of P.L. 108-458, amended FISA to insert "Director of National Intelligence" in lieu of "Director of Central Intelligence" in each place in which it appeared.

[126] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 613 (U.S. Foreign Intell. Surveil. Ct. 2002). A copy of a March 6, 2002, Memorandum from the Attorney General to the Director, FBI; Assistant Attorney General, Criminal Division; Counsel for Intelligence Policy; and United States Attorneys entitled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" may be found at http://fas.org/irp/agency/doj/fisa/ag030602.html.

General's 1995 minimization procedures, as subsequently modified by the Attorney General and the Deputy Attorney General, and preservation of a "wall" procedure to maintain separation between FBI criminal investigators and DOJ prosecutors and raw FISA investigation data regarding the same facts or individuals, so as to prevent these law enforcement personnel from becoming "de facto partners in FISA surveillances and searches,"[127] while permitting extensive sharing of information between such investigations.

The FISC was particularly concerned with those aspects of section II.B. of the proposed procedures which would permit criminal prosecutors and law enforcement officers to initiate, direct or control electronic surveillance or physical searches under FISA, with an eye towards law enforcement objectives, rather than foreign intelligence information gathering. The FISC set the stage for its analysis by recounting a significant number of past instances where FISA applications had included false, inaccurate or misleading information regarding information sharing or compliance with "wall" procedures in FBI affidavits or, in one case, in a statutorily required certification by the FBI Director; and past occasions where the FISC's orders had been violated in regard to information sharing and unauthorized dissemination of FISA information to criminal investigators and prosecutors. While both the FBI's and DOJ's Offices of Professional Responsibility had been investigating these incidents for over a year at the time of the writing of the opinion, the court had not been advised of any explanations as to how such misrepresentations had occurred. The court's dissatisfaction with these irregularities formed a backdrop for its analysis of the motion and applications before it.

Discussion of the Memorandum Opinion and Order. Its analysis was based upon its reading of the statutory language and premised, in part, on the fact that the USA PATRIOT Act had not amended the provisions of FISA dealing with minimization requirements, although other FISA provisions had been modified. The minimization provisions with respect to both electronic surveillance and physical searches under FISA continue to be designed to "minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons, consistent with the need of the United States to obtain, produce, and disseminate *foreign intelligence information.*"[128] The court regarded the standard it applied to the proposed procedures before it as "mandated in [50 U.S.C.] § 1805(a)(4) and § 1824(a)(4), which state that 'the

---

[127] *Id.* at 620. In Chapter 3 of *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States* 78-80 (W.W. Norton & Co. 2004) (*Final Report*), the Commission perceived the evolution of the "wall" as a result of statutory language, court interpretation, DOJ interpretation of the legislative language and court decisions, DOJ procedures to manage information sharing between Justice Department prosecutors and the FBI, misunderstanding and misapplication of those procedures, DOJ's Office of Intelligence Policy and Review's (OIPR) stringent exercise of its gate-keeping role, and inaccurate perceptions of field agents. In Chapter 8 of the *Final Report*, at 269-72, the Commission recounted some of the effects of what it saw as the confusion surrounding the rules governing the use and sharing of information gathered through intelligence channels.

[128] 50 U.S.C. §§ 1802(h), 1821(4)(A) (emphasis added).

proposed minimization procedures meet the definition of minimization procedures under § 101(h), [§ 1801(h) and §1824(4)] of the act.'"

In its memorandum opinion, the FISC first discussed the court's jurisdiction, noting that the text of the statute "leaves little doubt that the collection of foreign intelligence information is the *raison d'etre* for the FISA."[129] The court found support for this conclusion in a review of pertinent provisions of the act. It found further support in E.O. 12139 and E.O. 12949, which give the Attorney General authority to approve the filing of applications for orders for electronic surveillances and physical searches and authorize the Director of the FBI and other senior executives to make required certifications under FISA for the "purpose of obtaining foreign intelligence information." The FISC therefore concluded that its jurisdiction was limited to granting FISA orders for electronic surveillance and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the act.[130] In reaching this conclusion, the FISC, in a footnote, characterized the issue before it as "whether the FISA authorizes electronic surveillance and physical searches *primarily for law enforcement purposes* so long as the Government also has 'a significant' foreign intelligence purpose." Rejecting the approach taken by the Government in its supplemental brief in the case, the Court stated that "its decision is not based on the issue of its jurisdiction but on the interpretation of minimization procedures."[131] Maintaining its focus upon the minimization procedures, the FISC also declined to reach the question raised by the

---

[129] *FISC op.*, 218 F. Supp. 2d at 613. "Foreign intelligence information" is a term of art in FISA, defined in 50 U.S.C. § 1801(e) to mean:

> (e) (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 U.S. 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.

In reaching its decision, the FISC indicated that it was not addressing directly the Department of Justice argument that, so long as a significant purpose of a FISA surveillance or physical search was to gather foreign intelligence information, the primary purpose of such an investigation could be criminal investigation or prosecution. *FISC op.*, 218 F. Supp. 2d at 615 n.2. The FISC was not receptive to the DOJ theory that a "wall" procedure separating a foreign intelligence investigation under FISA from a criminal investigation involving the same target or factual underpinnings was an artificial separation which was not compelled by FISA.

[130] *FISC op.*, 218 F. Supp. 2d at 614.

[131] *Id.* at 614 n.1(emphasis added).

Attorney General "whether FISA may be used primarily for law enforcement purposes."[132]

The court also regarded the scope of its findings regarding minimization[133] as applicable "only to communications concerning U.S. persons as defined in § 1801(i) of the act: U.S. citizens and permanent resident aliens whether or not they are named targets in the electronic surveillance and physical searches."[134] It emphasized that its opinion was not applicable to communications of foreign powers as defined under 50 U.S.C. § 1801(a), or to non-U.S. persons.[135]

---

[132] *Id.* at 615 n.2.

[133] FISA defines "minimization procedures" with respect to electronic surveillance in 50 U.S.C. § 1801(h). The term is defined under FISA with respect to physical searches in 50 U.S.C. § 1821(4). As the two definitions are similar, the definition from Section 1801(h) is included for illustrative purposes.

> (h) "Minimization procedures", with respect to electronic surveillance, means–
>
> (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 72 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.

[134] *FISC op.*, 218 F. Supp. 2d at 614. This provision defines a "United States person" as follows:

> . . . 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.

[135] *Id.*

After stating its continued approval of the "Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power," the court turned its attention to two sections of supplementary minimization procedures adopted by the Attorney General on March 6, 2002, regarding "II. Intelligence sharing procedures concerning the Criminal Division," and "III. Intelligence sharing procedures concerning a USAO [U.S. Attorney's Office]." The FISC regarded these procedures as minimization procedures as that term is defined under FISA by virtue of the fact that they were adopted by the Attorney General and were "designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[136] Therefore, these procedures were measured against the standard for minimization procedures set forth in 50 U.S.C. §§ 1805(a)(4) and 1824(a)(4):

> . . . The operative language of each section to be applied by the Court provides that minimization procedures must be reasonably designed in light of their purpose and technique, and mean —
>
> > 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, [search] 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. §1801(h)(1) and §1821(4)(A).[137]

The court then reviewed the minimization procedures upon which it had been relying prior to the application before it, to wit, the Attorney General's 1995 "Procedures for Contacts between the FBI and Criminal Division Concerning FI [Foreign Intelligence] and Foreign Counterintelligence Investigations,"as augmented by the Attorney General in January 2000 and expanded further by the Deputy Attorney General in August 2001. The FISC indicated that these procedures permitted the following "substantial consultation and coordination":

a. reasonable indications of significant federal crimes in FISA cases are to be reported to the Criminal Division of the Department of Justice;

b. [t]he Criminal Division may then consult with the FBI and give guidance to the FBI aimed at preserving the option of criminal prosecution, *but may not direct or control* the FISA investigation toward law enforcement objectives;

c. the Criminal Division may consult further with the appropriate U.S. Attorney's Office about such FISA cases;

d. on a monthly basis senior officials of the FBI provide briefings to senior officials of the Justice Department, including OIPR [Office of Intelligence Policy and Review] and the Criminal Division, about intelligence cases, including those in which FISA is or may be used;

---

[136] *Id.* at 616.

[137] *Id.*

e. all FBI 90-day interim reports and annual reports of counterintelligence investigations, including FISA cases, are being provided to the Criminal Division, and must now contain a section explicitly identifying any possible federal criminal violations;

f. all requests for *initiation or renewal of FISA authority* must now contain a section devoted explicitly to identifying any possible federal criminal *violations*;

g. the FBI is to provide monthly briefings directly to the Criminal Division concerning all counterintelligence investigations in which there is a reasonable indication of a significant federal crime;

h. prior to each briefing the Criminal Division is to identify (from FBI reports) those intelligence investigations about which it requires additional information and the FBI is to provide the information requested; and

i. since September 11, 2001, the requirement that OIPR be present at all meetings and discussions between the FBI and Criminal Division involving certain FISA cases has been suspended; instead, OIPR reviews a daily briefing book to inform itself and this Court about those discussions.[138]

The FISC indicated further that it "routinely approved the use of information screening 'walls' proposed by the government in its applications" to maintain both the appearance and the fact that FISA surveillances and searches were not being used "*sub rosa* for criminal investigations."[139] In March 2000, September 2000, and March 2001, the FISC was advised by the Department of Justice of a significant number of erroneous statements or omissions of material facts in FISA applications, almost all of which involved misstatements or omissions as to information sharing and unauthorized disseminations to criminal investigators and prosecutors.[140] Although the FBI and the Department of Justice Office of Professional Responsibility had been investigating the circumstances involved in these misstatements and omissions for over a year, as of the date of the opinion, the court had not been advised of the reasons for these erroneous statements. The court responded to these concerns in 2001 by instituting supervisory measures to assess compliance with "wall" procedures.

In the case before the FISC, the government moved that all "wall" procedures be eliminated in international terrorism surveillances and physical searches under FISA. The FISC indicated that the new 2002 procedures proposed by the Attorney General would apply to two types of cases in which "*FISA is the only effective tool available* to both counterintelligence and criminal investigators" (emphasis supplied) — those involving overlapping investigations (which the court described as cases,

---

[138] *Id.* at 619-20 (emphasis supplied.)

[139] *Id.* at 620.

[140] The September 2000 notification to the FISC from the Department of Justice identified 75 cases of cases involving misstatements or omissions in FISA applications. The court does not indicate the specific number of FISA applications involved in the notifications on the other dates mentioned in the opinion. *See FISC op.*, 218 F. Supp. 2d at 620-21.

usually international terrorism cases, in which separate intelligence and criminal investigations of the same FISA target who is a U.S. person are conducted by different FBI agents, where separation can easily be maintained) and those involving overlapping interests (i.e., cases in which one investigation of a U.S. person FISA target is conducted by a team of FBI agents with both intelligence and criminal interests "usually involving espionage and similar cases in which separation is impractical").[141] In both types of investigations, the FISC indicated that the 2002 proposed minimization procedures provided authority for "extensive consultations between the FBI and criminal prosecutors 'to coordinate efforts to investigate or protect against actual or potential attack, sabotage, international terrorism and clandestine intelligence activities by foreign powers and their agents . . . .'" Such consultation is expressly provided for in 50 U.S.C. §§ 1806(k)(1) and 1825(k)(1).

Under the proposed minimization procedures, those consultations would include providing prosecutors with access to "all information" developed in FBI counterintelligence investigations, including through FISA, among other information. Section II.B. of the proposed minimization techniques would authorize criminal prosecutors to "consult extensively and provide advice and recommendations to intelligence officials about 'all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities.'" The FISC was particularly concerned about the authority given criminal prosecutors under Section II.B. "to advise *FBI intelligence officials concerning 'the initiation, operation, continuation, or expansion of FISA searches or surveillance*.'"[142] The court regarded this provision as "designed to use this Court's orders to enhance criminal investigation and prosecution, consistent with the government's interpretation of the recent amendments that FISA may now be 'used *primarily* for a law enforcement purpose.'"[143] Under section III of the proposed procedures, U.S. attorneys are given the authority to engage in consultations to the same extent as the Criminal Division of DOJ under parts II.A. and II.B. in cases involving international terrorism. The FISC interpreted these procedures as giving criminal prosecutors "a significant role directing FISA surveillances and searches from start to finish in counterintelligence cases involving overlapping intelligence and criminal investigations or interests, guiding them to criminal prosecution."[144]

In light of the court's past experience with FISA searches and surveillances, the FISC found the proposed procedures to be "designed to enhance the acquisition, retention and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*' (emphasis added [by the FISC]) as mandated in § 1801(h) and § 1821(4)."[145] The court regarded the procedures as, in effect, an effort by the government to amend FISA's definition of minimization

---

[141] *FISC op.*, 218 F. Supp. 2d at 622.

[142] *Id.* at 623.

[143] *Id.* (Emphasis added).

[144] *Id.*

[145] *Id.*

procedures in ways that Congress had not and to substitute FISA for the electronic surveillance requirements of Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*, and for the search warrant requirements in Rule 41 of the Federal Rules of Criminal Procedure. The court found this unacceptable. Nor was the court persuaded by the government's contention that the 1995 procedures' prohibition against criminal prosecutors "directing or controlling" FISA cases should be revoked. "If criminal prosecutors direct both the intelligence and criminal investigations, or a single investigation having combined interests, *coordination becomes subordination* of both investigations or interests to law enforcement objectives."[146]

The FISC stated:

> Advising FBI intelligence officials on the initiation, operation, continuation or expansion of FISA surveillances and searches of U.S. persons means that criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute. The 2002 minimization procedures give the Department's criminal prosecutors every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information, . . . based on a standard that the U.S. person is only using or about to use the places to be surveilled or searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants. All of this may be done by use of procedures intended to minimize collection of U.S. person information, consistent with the need of the United States to obtain and produce foreign intelligence information. If direction of counterintelligence cases involving the use of highly intrusive FISA surveillances and searches by criminal prosecutors is necessary to obtain and produce foreign intelligence information, it is yet to be explained to the Court.[147]

Having found section II.B. of the proposed minimization procedures inconsistent with the statutory standard for minimization procedures under 50 U.S.C. §§ 1801(h) and 1821(4), the court substituted its own language in place of the second and third paragraphs of II.B. as submitted by the Attorney General. The substitute language permitted consultation between the FBI, the Criminal Division of DOJ, and the Office of Intelligence Policy and Review of DOJ (OIPR) "to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or [agents of foreign powers]," so that the goals and objectives of both the intelligence and law enforcement investigations or interests may be achieved. However, it prohibited law enforcement officials from making recommendations to intelligence officials regarding initiation, operation, continuation, or expansion of FISA surveillances and searches. In addition, the substitute language foreclosed law enforcement officials from directing or controlling the use of FISA procedures to enhance criminal prosecution; nor was advice intended to preserve the option of

---

[146] *Id*. at 623-24 (emphasis in original).

[147] *Id.* at 624.

criminal prosecution to be permitted to inadvertently result in the Criminal Division directing or controlling an investigation involving FISA surveillance or physical searches to achieve law enforcement objectives.[148] While direct consultation and coordination were permitted, the substitute language required OIPR to be invited to all such consultations and, where OIPR was unable to attend, the language required OIPR to be apprized forthwith in writing of the substance of the consultations, so that the FISC could be notified at the earliest opportunity.[149]

In its order accompanying the FISC memorandum opinion, the court held that the proposed minimization procedures, so modified, would be applicable to all future electronic surveillances and physical searches under FISA, subject to the approval of the court in each instance.[150] In this order, the court also adopted a new administrative rule to monitor compliance. The new Rule 11 regarding criminal investigations in FISA cases provided:

> All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office.[151]

The Decision of the U.S. Foreign Intelligence Surveillance Court of Review

Summary. The FISC memorandum opinion and order discussed above were not appealed directly. Rather, the Department of Justice sought review in the U.S. Foreign Intelligence Surveillance Court of Review (Court of Review) of a FISC order which authorized electronic surveillance of an agent of a foreign power, but imposed restrictions on the government flowing from the FISC's May 17th decision, and of an order renewing that surveillance subject to the same restrictions. Because of the electronic surveillance context of these orders, the Court of Review's analysis was cast primarily in terms of such surveillance, although some aspects of its analysis may have broader application to other aspects of FISA. In its first decision ever, the Court of Review, in a lengthy *per curiam* opinion issued on November 18, 2002, reversed and remanded the FISC orders. In so doing the Court of Review emphasized that the May 17th decision, although never appealed, was "the basic decision before us and it [was] its rationale that the government challenge[d]."[152] After reviewing the briefs of the government and two *amici curiae*, the American Civil Liberties Union (joined on the brief by the Center for Democracy and Technology, the Center for National Security Studies, the Electronic Privacy Information Center, and the Electronic Frontier Foundation) and the National Association of Criminal Defense Lawyers, the Court of Review concluded that "FISA, as amended by the Patriot Act, supports the

---

[148] *Id.* at 625.

[149] *Id.*

[150] *Id.* at 627.

[151] *Id.*

[152] In re Sealed Case, 310 F.3d 717, 721 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (hereinafter *Court of Review op.*).

government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."[153]

Discussion of the Opinion. The Court of Review began its analysis by articulating its view of the May 17th FISC decision. The Court of Review stated that the FISC appeared to proceed in its opinion from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement officers in the Executive Branch, but did not support that assumption with any relevant language from the statute.[154] The Court of Review opined that this "wall" was implicit in the FISC's "apparent" belief that "it can approve applications for electronic surveillance only if the government's objective is *not* primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity," while referencing neither statutory language in FISA nor USA PATRIOT Act amendments, which the government argued altered FISA to permit an application even if criminal prosecution was the primary goal.[155] Instead, the Court of Review noted that the FISC relied upon its statutory authority to approve "minimization procedures" in imposing the restrictions at issue.

The Court of Review stated that the government raised two main arguments: First, DOJ contended that the restriction, recognized by several courts of appeals [156]

---

[153] *Id.* at 719-20.

[154] *Id.* at 721.

[155] *Id.*

[156] The cases to which this appears to refer include decisions by both U.S. courts of appeals and U.S. district courts. Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, United States v. Megahey, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), *aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1982), *re-aff'd post-trial sub nom* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States. v Badia, 827 F. 2d 1458, 1464 (11th Cir. 1987). *See also*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *rehearing and cert. denied*, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); United States v. Pelton, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where the primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard — i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense — for issuance of a search

(continued...)

[156] (...continued)
warrant was violative of the Fourth Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); United States v. Cavanaugh, 807 F.2d 787, 790-91 (9th Cir. 1987) (defendant, convicted of espionage, appealed district court's refusal to suppress fruits of FISA electronic surveillance which intercepted defendant offering to sell defense secrets to representatives of Soviet Union. In affirming conviction, appellate court found FISA procedures had been followed, and upheld FISA against constitutional challenges. Court found, in part, that FISA probable cause requirement was reasonable under Fourth Amendment standard. "The application must state that the target of the electronic surveillance is a foreign power or an agent of a foreign power, and must certify that the purpose of the surveillance is to obtain foreign intelligence information and that the information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C. § 1804(a). It is true, as appellant points out in his brief, that the application need not state that the surveillance is likely to uncover evidence of a crime; but as the purpose of the surveillance is not to ferret out criminal activity but rather to gather intelligence, such a requirement would be illogical. *See United States District Court*, 407 U.S. at 322 (recognizing distinction between surveillance for national security purposes and surveillance of 'ordinary crime'); . . . And . . . there is no merit to the contention that he is entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance not supported by probable cause of criminal activity. *See Duggan*, 743 F.2d at 73n.5.") United States v. Rahman, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). *Cf.*, United States v. Bin Laden, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); United States v. Bin Laden, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection. . . . If foreign intelligence collection is merely *a* purpose and not the *primary* purpose of a search, the exception does not apply.")

Cf., United States v. Sarkissian, 841 F.2d 959, 964-65 (9th Cir. 1988) (FISA court order authorized electronic surveillance, which resulted in the discovery of plan to bomb the Honorary Turkish Consulate in Philadelphia, and of the fact that bomb components were being transported by plane from Los Angeles. The FBI identified likely airlines, flight plans, anticipated time of arrival, and suspected courier. Shortly before the arrival of a flight fitting these parameters, the investigation focused upon an individual anticipated to be a passenger on that flight. An undercover police officer spotted a man matching the suspected courier's description on that flight. The luggage from that flight was sniffed by a trained dog and x-rayed. A warrantless search was conducted of a suitcase that had been shown by x-ray to contain an unassembled bomb. Defendants unsuccessfully moved to suppress the evidence from the FISA wiretap and the warrantless search. On appeal the court upheld the warrantless suitcase search as supported by exigent circumstances. Defendants contended that the FBI's primary purpose for the surveillance had shifted at the time of the wiretap from an intelligence investigation to a criminal investigation and that court approval for the wiretap therefore should have been sought under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*, rather than FISA. The court, while noting that in other cases it had state that "the purpose of [electronic] surveillance" under FISA "must be to secure foreign intelligence information," "not to ferret out criminal activity;" declined to decide the issue of whether the applicable standard was that "the purpose" or that "the primary purpose" of a FISA surveillance must be gathering of foreign intelligence information. The court stated, "Regardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces
(continued...)

prior to the enactment of the USA PATRIOT Act, that FISA could only be used if the government's primary purpose in gathering foreign intelligence information was not criminal prosecution, was not supported by the statutory language or the legislative history of FISA. This argument was not presented to the FISC, but the Court of Review indicated that it could entertain the argument, because proceedings before the FISC and before the Court of Review were *ex parte*.[157] Second, the government argued that, even if the primary purpose test was appropriate prior to the passage of the USA PATRIOT Act, the amendments made by that act eliminated that concept. The government also argued that the FISC's interpretation of the minimization procedures provisions misconstrued those provisions and amounted to "an end run" around the USA PATRIOT Act amendments. DOJ argued further that the FISC minimization procedures so intruded into the Department's operations as to be beyond the constitutional authority of Article III judges. Finally, DOJ contended that application of the primary purpose test in a FISA case was not constitutionally compelled under the Fourth Amendment.

---

[156] (...continued)
us that it is met in this case. . . . We refuse to draw too fine a distinction between criminal and intelligence investigations. "International terrorism," by definition, requires the investigation of activities that constitute crimes. 50 U.S.C. § 1806(f). That the government may later choose to prosecute is irrelevant. FISA contemplates prosecution based on evidence gathered through surveillance. . . . "Surveillances . . . need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." S. Rep. No. 701, 95th Cong., 1st Sess. 11 . . . [(1978)]. . . . FISA is meant to take into account "the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities . . ." *Id.* . . . . At no point was this case an ordinary criminal investigation."). *Cf.*, United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (distinguishing United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980); and United States v. Butenko, 494 F.d 593, 606 (3d Cir.) (*en banc*), *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), which held that, while warrantless electronic surveillance for foreign intelligence purposes was permissible, when the purpose or primary purpose of the surveillance is to obtain evidence of criminal activity, evidence obtained by warrantless electronic surveillance is inadmissible at trial, 540 F. Supp. at 1313. In addressing the theory that the evidence in the case before it was obtained pursuant to a warrant, a lawfully obtained court order under FISA, *id.* at 1314, the court observed that the "bottom line of *Truong* is that evidence derived from *warrantless* foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information." *Id*. at 1313-14. After noting that Congress, in enacting FISA, "expected that evidence derived from FISA surveillances could then be used in a criminal proceeding," the court concluded that "it was proper for the FISA judge to issue the order in this case because of the on-going nature of the foreign intelligence investigation. . . . The fact that evidence of criminal activity was thereafter uncovered during the investigation does not render the evidence inadmissible. There is no question in [the court's] mind that the purpose of the surveillance, pursuant to the order, was the acquisition of foreign intelligence information. Accordingly, [the court found] that the FISA procedures on their face satisfy the Fourth Amendment warrant requirement, and that FISA was properly implemented in this case." *Id.* at 1314.).

[157] *Court of Review op.*, 310 F.3d at 722 n.6.

The Court of Review noted that, as enacted in 1978, FISA authorized the grant of an application for electronic surveillance to obtain foreign intelligence information if there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power,"[158] and that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power."[159] The reviewing court focused upon the close connection between criminal activity and the definitions of "agent of a foreign power" applicable to United States persons contained in 50 U.S.C. §§ 1801(b)(2)(A) and (C), to wit: "any person who 'knowingly engages in clandestine intelligence activities . . . which activities involve or may involve a violation of the *criminal statutes* of the United States,' or 'knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor.'"[160] The court noted further that FISA defined "international terrorism" to mean "activities that 'involve violent acts or acts dangerous to human life that are a violation of the *criminal laws* of the United States or of any State, or that would be a *criminal*

---

[158] The Court of Review did not include in its quotation of 50 U.S.C. § 1805(a)(3)(A) the proviso that follows the quoted language: "*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."

[159] *Court of Review op.*, 310 F.3d at 722, *quoting* portions of 50 U.S.C. § 1805(a)(3).

[160] *Id.* at 723 (emphasis added by the Court of Review). The definitions of "agent of a foreign power" which apply to "any person" (including, by implication, United States persons) are set forth in 50 U.S.C. § 1801(b)(2). This subsection now contains five subparagraphs:

> (b) "Agent of a foreign power" means —
> . . .
> (2) any person who —
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> (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).

The current subparagraph (D) was added in 1999, and the former subparagraph (D) was redesignated subparagraph (E).

violation if committed within the jurisdiction of the United States or any State.'"[161] "Sabotage," as defined by FISA, covers activities that "'involve a violation of chapter 105 of [the criminal code] [18 U.S.C. §§ 2151-2156], or that would involve such a violation if committed against the United States.'"[162] For purposes of its opinion, the Court of Review described these types of crimes as "foreign intelligence crimes."[163]

---

[161] *Id.* at 723, *quoting* 50 U.S.C. § 1801(c)(1) (emphasis added by the Court of Review). The remainder of the definition of "international terrorism" under 50 U.S.C. § 1801(c)(2) and (3) adds two more criteria for activities to be considered to be within this definition:

> (c) "International terrorism" means activities that —
>
> . . .
>
> (2) appear to be intended —
>
> (A) to intimidate or coerce a civilian population;
>
> (B) to influence the policy of a government by intimidation or coercion; or
>
> (C) to affect the conduct of a government by assassination or kidnapping; and
>
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

[162] *Court of Review slip op.* at 10, quoting 50 U.S.C. § 1801(d).

[163] Although later acknowledging the possibility that the Justice Department had accepted the dichotomy between foreign intelligence gathering and law enforcement purposes "in an effort to conform to district court holdings," *Court of Review op.*, 310 F.3d at 727, (most of the published decisions were court of appeals decisions rather than district court decisions) the Court of Review expressed puzzlement that "the Justice Department, at some point during the 1980's, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents — even for foreign intelligence crimes," while noting that 50 U.S.C. § 1804 at the time required that "a national security official in the Executive Branch — typically the Director of the FBI — . . . certify that 'the purpose' of the surveillance was to obtain foreign intelligence information (amended by the Patriot Act to read 'a significant purpose.')" *Id.* at 723. The court did, however, discuss a series of 1982-1991 cases upholding the constitutional sufficiency of electronic surveillance under FISA as long as "the primary purpose" of the surveillance was gathering foreign intelligence information, rather than criminal prosecution. If foreign intelligence gathering was the primary purpose of a FISA electronic surveillance, initially and throughout the surveillance, and FISA was not being used as "an end run around the 4th Amendment," the courts permitted use of the fruits of the surveillance in subsequent criminal prosecutions. See the discussion of these cases at fn. 156, *supra*, of this report. This "primary purpose" approach to these FISA cases appears consistent with the "primary purpose" approach taken in a number of pre-FISA cases involving Fourth Amendment challenges to warrantless foreign intelligence surveillances. See constitutional analyses in United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (5th Cir. 1974); United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974) , *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), and Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976); along with the Supreme Court's analysis, in a domestic surveillance context, in the *Keith* case, United States v. United States District Court, 407 U.S. 297 (1972), discussed in the "Background" section of this report, *supra*. The Court of Review appears to discount the significance of these decisions because the courts involved upheld

(continued...)

The court observed that, as passed in 1978, 50 U.S.C. §1804 required a national security official of the Executive Branch, usually the FBI Director,[164] to certify that "the purpose" of the electronic surveillance under FISA was to obtain foreign intelligence information, and opined that "it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power — if he or she is a U.S. person — is grounded on criminal conduct."[165] It found further support for its view that "foreign intelligence information" included evidence of "foreign intelligence crimes" from the legislative history as reflected in H.Rept. 95-1283 and S.Rept. 95-701, [166] while acknowledging that the House report also stated that FISA surveillances "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns

---

[163] (...continued)
lower court decisions permitting admission of information gathered under FISA in criminal trials. The Court of Review stated, "It may well be that the government itself, in an effort to conform to district court holdings, accepted the dichotomy it now contends is false. Be that as it may, since the cases that "adopt" the dichotomy do affirm district court opinions permitting the introduction of evidence gathered under a FISA order, there was not much need for the courts to focus on the opinion with which we are confronted." *Court of Review op.*, 310 F.3d at 727.

[164] The pertinent language of 50 U.S.C. § 1804(a)(7) as passed in 1978 provided that each application for an order authorizing electronic surveillance under FISA shall include:

> (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 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 —
>
> (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 section 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[.]

Under 50 U.S.C. § 1804(d) as passed in 1978 and under current law, "The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title."

[165] *Court of Review op.*, 310 F.3d at 723.

[166] *Id.* at 724-25, *citing* H.Rept. 95-1283, at 49 (1978) and S.Rept. 95-701, at 10-11 (1978).

United States persons must be necessary to important national concerns."[167] The Court of Review regarded the latter statement as an observation rather than a proscription.[168]

The Court of Review saw the U.S. Court of Appeals for the Fourth Circuit's decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), a decision based upon constitutional analysis rather than FISA provisions, as the springboard for the "primary purpose" test cases interpreting FISA and upholding FISA surveillances against Fourth Amendment challenges.[169] After reviewing a number of the FISA cases applying the primary purpose test, the Court of Review concluded that a dichotomy between foreign intelligence gathering and criminal investigations implicit in the application of the primary purpose test was not statutorily compelled. The court found that FISA, as originally passed, did not "preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[170] In addition, the Court of Review, relying on arguments of the Department of Justice and the language of subsection 1805(a)(5), interpreted 50 U.S.C. §§ 1805 of FISA as originally enacted as not contemplating that the [FISC] would inquire into the government's purpose in seeking foreign intelligence information.[171]

---

[167] H.Rept. 95-1283, at 36 (1978).

[168] *Court of Review op.*, 310 F.3d at 725.

[169] Although *Truong Dinh Hung* was among the cases cited by some of the subsequent FISA cases, a "primary purpose" test had been previously applied in the 1974 Third Circuit decision in *Butenko, supra,* upholding a warrantless electronic surveillance in the face of challenges based upon the Fourth Amendment and Section 605 of the Communications Act where the primary purpose of the investigation was gathering foreign intelligence information. See discussion in the "Background" section of this report, *supra*, as well as the summary of this and other cases at fns. 156 and 163, *supra*.

[170] *Court of Review op.*, 310 F.3d at 727.

[171] *Id*. at 723-24, 728. Section 1805(a), as enacted in 1978, set forth the necessary findings that a judge of the FISC had to make in order to enter an ex parte order as requested or as modified approving electronic surveillance under FISA:

> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
> (2) the application has been made by a Federal officer and approved by the Attorney General;
> (3) 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;

(continued...)

Further, the court rejected the FISC's characterization of the Attorney General's 1995 procedures, as modified and augmented in January 2000 and August 2001, as minimization procedures. These procedures were formally adopted by the FISC as minimization procedures defined in 50 U.S.C. §§ 1801(h) and 1821(4) in November 2001, after passage of the USA PATRIOT Act, and were incorporated in all applicable orders and warrants granted since their adoption by the FISC. On March 6, 2002, the Attorney General adopted new "Intelligence Sharing Procedures," intended to supercede prior procedures, to "allow complete exchange of information and advice between intelligence and law enforcement officials," to "eliminate the 'direction and control' test," and to permit "exchange of advice between the FBI, OIPR, and the Criminal Division regarding 'the initiation, operation, continuation, or expansion of FISA searches or surveillance."[172] The following day, the government filed a motion with the FISC advising the court of the Attorney General's adoption of the 2002 procedures, seeking to have that court adopt the new procedures in all matters before the FISC and asking the court to vacate its orders adopting the prior procedures as minimization procedures and imposing "wall" procedures in certain types of cases. That motion led to the FISC decision to adopt the 2002 procedures with modifications that was, by reference, before the Court of Review in its November 18, 2002, decision.

The Court of Review characterized the FISC's adoption of the Justice Department's 1995 procedures, as modified and augmented, as minimization procedures as follows:

> Essentially, the FISA court took portions of the Attorney General's augmented 1995 Procedures — adopted to deal with the primary purpose standard — and imposed them generically as minimization procedures. In doing so, the FISA court erred. It did not provide any constitutional basis for its action — we think there is none — and misconstrued the main statutory provision on which it relied. The court mistakenly categorized the augmented 1995 Procedures as FISA minimization procedures and then compelled the government to utilize a modified version of those procedures in a way that is clearly inconsistent with the statutory purpose.[173]

The Court of Review interpreted "minimization procedures" under 50 U.S.C. § 1801(h) to be designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. In light of the Court of Review's interpretation of "minimization procedures" under 50 U.S.C. § 1801(h), the court found no basis for

---

[171] (...continued)

> (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title;
>
> (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.

[172] *Court of Review op.*, 310 F.3d at 729.

[173] *Id.* at 730.

the FISC's reliance upon that section "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime."[174]

In addition, the Court of Review found that the FISC had misconstrued its authority under 50 U.S.C. § 1805 and misinterpreted the definition of minimization procedures under 50 U.S.C. § 1801(h). The Court of Review expressed approbation for the Government's argument that the FISC, in imposing the modified 1995 procedures upon the Department of Justice as minimization procedures, "may well have exceeded the constitutional bounds that restrict an Article III court. The FISA court asserted authority to govern the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I)."[175]

The Court of Review deemed the FISC's "refusal . . . to consider the legal significance of the Patriot Act's crucial amendments [to be] error."[176] The appellate court noted that, as amended by the USA PATRIOT Act, the requirement in 50 U.S.C. § 1804(a)(7)(B) that the Executive Branch officer certify that "the purpose" of the FISA surveillance or physical search was to gather foreign intelligence information had been changed to "a significant purpose."[177] The court noted that floor statements indicated that this would break down traditional barriers between law enforcement and foreign intelligence gathering,[178] making it easier for law enforcement to obtain FISA court orders for surveillance or physical searches where the subject of the surveillance "is both a potential source of valuable intelligence and the potential target of a criminal prosecution."[179] The court noted that some Members raised concerns about the Fourth Amendment implications of this language change which permitted the Government to obtain a court order under FISA "even if the

---

[174] *Id.* at 731.

[175] *Id.* at 731-32.

[176] *Id.* at 732.

[177] *Id.* at 728-29, 732-33.

[178] *Id.* at 732, *quoting* Sen. Leahy, 147 Cong. Rec. S10992 (Oct. 25, 2001).

[179] *Id.* at 733, *quoting* Sen. Feinstein, 147 Cong. Rec. S10591 (Oct. 11, 2001). In Section 13.5 of Chapter 13 of its *Final Report*, at 424, the 9/11 Commission, in discussing the future role of the FBI, observes in part:

> Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action. Because the FBI can have agents working criminal matters and agents working intelligence investigations concerning the same international terrorism target, the full range of investigative tools against a suspected terrorist can be considered within one agency. The removal of the "wall" that existed before 9/11 between intelligence and law enforcement has opened up new opportunities for cooperative action within the FBI.

primary purpose is a criminal investigation."[180] Interestingly, although the Court of Review did not regard a dichotomy between foreign intelligence gathering and law enforcement purposes as necessarily implied by the 1978 version of 50 U.S.C. § 1804(a)(7)(B), the court viewed the statutory change from "the purpose" to "a significant purpose" in the USA PATRIOT Act as recognizing such a dichotomy.[181]

The Court of Review disagreed with the FISC interpretation of the consultation authority under 50 U.S.C. § 1806(k).[182] The Court of Review saw this provision as one which reflected the elimination of barriers between law enforcement and intelligence or counterintelligence gathering, without a limitation on law enforcement officers directing or controlling FISA surveillances. "[W]hen Congress explicitly authorizes consultation and coordination between different offices in the government, without even suggesting a limitation on who is to direct and control, it necessarily implies that either could take the lead."[183]

In analyzing the "significant purpose" amendment to 50 U.S.C. § 1804(a)(7)(B), the Court of Review deemed this a clear rejection of the primary purpose test. If gathering foreign intelligence information is a significant purpose, another purpose such as criminal prosecution could be primary.[184]Further, the court found that the term "significant" "imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes. . . . Although section 1805(a)(5) . . . may well have been intended to authorize the FISA court to review only the question whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804, it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information."[185] The Court of Review saw the "significant purpose" language as "excluding from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution."[186] If the government, at the commencement of a FISA surveillance has not yet determined whether to prosecute the target, "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[187] Under the Court of Review's analysis:

> If the certification of the application's purpose articulates a broader objective than criminal prosecution — such as stopping an ongoing conspiracy — and includes other potential non-prosecutorial responses, the government meets the

---

[180] *Court of Review op.*, 310 F.3d at 733, *quoting* Sen. Feingold, 147 Cong. Rec. S11021 (Oct. 25, 2001).

[181] *Id.* at 734-35.

[182] *Id.* at 733-34.

[183] *Id.* at 734.

[184] *Id.* at 734.

[185] *Id.* at 735.

[186] *Id.*

[187] *Id.*

> statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct — even foreign intelligence crimes — to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.[188]

The court stated further that, while ordinary crimes may be intertwined with foreign intelligence crimes, the FISA process may not be utilized to investigate wholly unrelated ordinary crimes.[189] The Court of Review emphasized that the government's purpose as reflected in the Section 1804(a)(7)(B) certification is to be judged by the FISC on the basis of

> . . .the national security officer's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved. It is up to the Director of the FBI, who typically certifies, to determine the government's national security purpose, as approved by the Attorney General or Deputy Attorney General. . . . That means, perforce, if the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose — or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval. The important point is that the relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's national security needs."[190]

Turning from its statutory analysis to its examination of whether the statute, as amended, satisfied Fourth Amendment parameters, the Court of Review compared the FISA procedures with those applicable to criminal investigations of "ordinary crimes" under Supreme Court jurisprudence and under the wiretap provisions of Title III of the Omnibus Crime Control and Safe Streets Act. Relying upon *Dalia v. United States*, 441 U.S. 238, 255 (1979), the court indicated that in criminal investigations, beyond requiring that searches and seizures be reasonable, the Supreme Court has interpreted the Fourth Amendment's warrant requirement to demand satisfaction of three criteria: a warrant must be issued by a neutral, detached magistrate; those seeking the warrant must demonstrate to the magistrate that there is probable cause to believe that the evidence sought will assist in a particular apprehension or conviction for a particular offense; and the warrant must describe with particularity the things to be seized and the place to be searched.[191]

The Court of Review compared the procedures in Title III with those in FISA, finding in some respects that Title III had higher standards, while in others FISA included additional safeguards. In both, there was provision for a detached, neutral magistrate. The probable cause standard in Title III for criminal investigations was deemed more demanding than that in FISA. Title III requires a showing of probable cause that a specific individual has committed, is committing, or is about to commit a particular criminal offense. FISA requires a showing of probable cause that the

---

[188] *Id.*

[189] *Id.* at 736.

[190] *Id.*

[191] *Id.* at 738.

target of the FISA investigative technique is a foreign power or an agent of a foreign power. A foreign power is not defined solely in terms of criminal activity. In the case of a target who is a U.S. person, the definition of "agent of a foreign power" contemplates, in part, the involvement of or, in the case of clandestine intelligence activities for a foreign power, the possibility of criminal conduct. The court regarded the lesser requirement with respect to criminal activity in the context of clandestine intelligence activities as to some extent balanced by the safeguard provided by FISA's requirement that there be probable cause to believe that the target is acting "for or on behalf of a foreign power."[192]

With regard to the particularity requirement, as to the first element, Title III requires a finding of probable cause to believe that the interception will obtain particular communications regarding a specified crime. In contrast, FISA requires an official to designate the type of foreign intelligence information being sought and to certify that the information being sought is foreign intelligence information. When the target of the FISA investigation is a U.S. person, the standard of review applied by the FISC is whether there is clear error in the certification, a lower standard that a judicial finding of probable cause. While the FISC can demand that the government provide further information needed for the court to make its determination as to whether the certification is clearly erroneous, the statute relies also upon internal checks on Executive Branch decisions through the requirement that the certification must be made by a national security officer and approved by the Attorney General or Deputy Attorney General.

In connection with the second particularity element, Title III

> . . . requires probable cause to believe that the facilities subject to surveillance are being used or are about to be used in connection with commission of a crime or are leased to, listed in the name of, or used by the individual committing the crime, 18 U.S.C. § 2518(3)(d), [while] FISA requires probable cause to believe that each of the facilities or places at which the surveillance is directed is being used, or is about to be used by a foreign power or agent [of a foreign power]. 50 U.S.C. § 1805(a)(3)(B). . . . Simply put, FISA requires less of a nexus between the facility and the pertinent communications that Title III, but more of a nexus between the target and the pertinent communications."[193]

The Court of Review also compared Title III to FISA with respect to necessity (both statutes require that the information sought is not available through normal investigative procedures, although the standards differ somewhat),[194] duration of

---

[192] *Id.* at 738-39.

[193] *Id.* at 740.

[194] For electronic surveillance to be approved, Title III requires a judicial finding that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. 18 U.S.C. § 2518(3)(c). FISA requires certification by the national security officer involved that the foreign intelligence information sought cannot reasonably be obtained by normal investigative means. 50 U.S.C. § 1804(a)(7)(C). The certification must include a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated; and

(continued...)

surveillance (30 days under Title III, 18 U.S.C. § 2518(3)(c), as opposed to 90 days under FISA for U.S. persons, 50 U.S.C. § 1805(e)(1)),[195] minimization and notice.

With respect to minimization, the Court of Review noted that Title III, under 18 U.S.C. § 2518(5), required minimization of what was acquired, directing that surveillance be carried out "in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." FISA, on the other hand, "requires minimization of what is acquired, retained, and disseminated."[196] Observing that the FISC had found "in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications," the Court of Review deemed the reasonableness of such an approach to be dependent upon the facts and circumstances of each case:[197]

> Less minimization in the acquisition stage may well be justified to the extent the intercepted communications are "ambiguous in nature or apparently involve[] guarded or coded language," or "the investigation is focusing on what is thought to be a widespread conspiracy [where] more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise." . . . Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots. . . .[198]

With respect to notice, the Court of Review observed that under 18 U.S.C. § 2518(8)(d), Title III mandated notice to the target of the surveillance and, in the judge's discretion, to other persons whose communications were intercepted, after the surveillance has expired. In contrast, under 50 U.S.C. § 1806(c) and (d), FISA does not require notice to a person whose communications were intercepted unless the government intends to use, disclose, or enter into evidence those communications or derivative information in a trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other federal, state or local authority

---

[194] (...continued)
that such information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C. § 1804(a)(7)(E)(i) and (ii). In issuing an ex parte order granting an application for electronic surveillance, the FISC judge must find that, in the case of a target who is a U.S. person, the certifications are not clearly erroneous on the basis of the statement made under 50 U.S.C. § 1804(a)(7)(e) and any other information furnished under Section 1804(d). Thus, the relevant findings to be made by the courts under the two statutes differ.

[195] *Court of Review op.*, 310 F.3d at 740. The difference, in the court's view, was "based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.' *Keith*, 407 U.S. at 322; *see also* S. Rep. at 16, 56." The court also noted that in FISA the "longer surveillance period is balanced by continuing FISA court oversight of minimization procedures during that period. 50 U.S.C. § 1805(e)(3); *see also* S Rep. at 56."

[196] *Id.*

[197] *Id.*

[198] *Id.* at 740-41.

against that person. The Court of Review noted that where such information was to be used against a criminal defendant, he or she would be given notice, and stated that "where such evidence is not ultimately going to be used for law enforcement," Congress had observed that "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement."[199] In a footnote, the court noted that the Amici had drawn attention to the difference in the nature of the notice given the defendant or aggrieved person under Title III as opposed to FISA. Under Title III, a defendant is generally entitled under 18 U.S.C. § 2518(9) to obtain the application and order to challenge the legality of the surveillance. However, under FISA, the government must give the aggrieved person and the court or other authority (or in the case of a state or local use, the state or political subdivision must give notice to the aggrieved person, the court or other authority, and the Attorney General) of their intent to so disclose or use communications obtained from the surveillance or derivative information. In addition, under 50 U.S.C. §§ 1806(f) and (g), if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm national security, the U.S. district court may review in camera and ex parte the application, order, and other materials related to the surveillance, to determine whether the surveillance was lawfully authorized and conducted, whether disclosure or discovery is necessary, and whether to grant a motion to suppress. The Court of Review noted that these determinations are to be made by the U.S. district judge on a case by case basis, and stated that "whether such a decision protects a defendant's constitutional rights in a given case is not before us."[200]

Based on this comparison of Title III and FISA, the Court of Review found that "to the extent that the two statutes diverge in constitutionally relevant areas — in particular, in their probable cause and particularity showings — a FISA order may not be a 'warrant' contemplated by the Fourth Amendment. . . . Ultimately, the question becomes whether FISA, as amended by the Patriot Act, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[201]

The court framed the question as follows: "does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable." In its analysis, the court first considered whether the *Truong* case articulated the correct standard. *Truong* held that the President had inherent authority to conduct warrantless searches to obtain foreign intelligence information, but did not squarely address FISA. Starting from the perspective that *Truong* deemed the primary purpose test to be constitutionally compelled as an application of the *Keith* case balancing standard, the Court of Review found that the *Truong* determination that "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause

---

[199] *Id.* at 741, *quoting* S.Rept. 95-701 at 12.

[200] *Id.*

[201] *Id.* at 741-42.

determination, and . . . individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis of a criminal investigation."[202] The Court of Review found that this analysis was based upon a faulty premise that in the context of criminal prosecution "foreign policy concerns recede," and found further that the line the *Truong* court "sought to draw was inherently unstable, unrealistic, and confusing."[203] The Court of Review opined that in the context of counterintelligence, foreign policy concerns did not recede when the government moved to prosecute. Rather "the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts."[204]

In addition, the court found that the method of determining when an investigation became primarily criminal by looking to when the Criminal Division of the Department of Justice assumed the lead role, had led over time to the "quite intrusive organizational and personnel tasking the FISA court [had] adopted."[205] The court found the "wall" procedure to generate dangerous confusion and create perverse organizational incentives that discouraged wholehearted cooperation of "all the government's personnel who can be brought to the task."[206] This the court suggested could be thought to be dangerous to national security and could be thought to discourage desirable initiatives.

In addition, the court saw the primary purpose test as administered by the FISC, "by focusing on the subjective motivation of those who initiate investigations . . . was at odds with the Supreme Court's Fourth Amendment cases which regard subjective motivation of an officer conducting a search or seizure as irrelevant." [207]

Assuming *arguendo* that FISA orders were not warrants within the scope of the Fourth Amendment, the Court of Review returned to the question of whether searches under FISA are constitutionally reasonable. While the Supreme Court has not considered directly the constitutionality of warrantless government searches for foreign intelligence purposes, the balance between the government's interest and personal privacy interests is key to an examination of this question. The Court of

---

[202] *Id.* at 742-43, *citing Truong*, *supra*, 629 F.2d at 914-15.

[203] *Id.* at 743.

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] *Id.*, *citing* Whren v. United States, 517 U.S. 806, 13 (1996). *See also*, Arkansas v. Sullivan, 532 U.S. 769, 770-72 (2001); Scott v. United States, 438 U.S. 128, 135-138 (1978). In these cases, the Court has held that, in a Fourth Amendment probable cause analysis of a warrantless search or seizure, the fact that an otherwise lawful search or seizure may have been made as a pretext for searching for evidence of other criminal behavior does not render that search or seizure unconstitutional. One might note that the probable cause standard applicable to a search or seizure in a criminal investigation is different from that under FISA, so that the pretextual search criminal cases may not be directly analogous to the FISA situation.

Review viewed *Keith* as suggesting that a somewhat relaxed standard might be appropriate in foreign intelligence crimes as opposed to ordinary crimes.[208]

The Court of Review then briefly touched upon the Supreme Court's "special needs" cases, where the Court upheld searches not based on a warrant or individualized suspicion in extraordinary circumstances involving "special needs, beyond the normal need for law enforcement." In *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000), the U.S. Supreme Court held that a highway check point program designed to catch drug dealers was not within the "special needs" exception to the requirement that a search be based upon individualized suspicion, because "the government's 'primary purpose' was merely 'to uncover evidence of ordinary criminal wrongdoing.'" The Court stated that "the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."[209] The Court relied upon an examination of the primary purpose of the program, but not the motivations of individual officers, to determine whether the "special needs" standard had been met. The Supreme Court noted that an appropriately tailored road block could be used "to thwart an imminent terrorist attack."[210]

After summarizing *Edmond*, the Court of Review emphasized that it is the nature of the threat or emergency that took the matter beyond the realm of ordinary crime control.[211] It concluded that, while the gravity of the threat alone cannot be dispositive of the reasonableness of a search under the Fourth Amendment standard, it is a critical factor in the analysis. In its view, the "programmatic purpose" of FISA, "to protect the nation against terrorists and espionage threats directed by foreign powers," was one which, from FISA's inception, was distinguishable from "ordinary crime control."[212] The Court of Review also concluded that, "[e]ven without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close."[213] Applying the balancing test that it had drawn from *Keith* between foreign intelligence crimes and ordinary crimes, the Court of Review held surveillances under FISA, as amended by the USA PATRIOT Act, were reasonable and therefore constitutional. In so doing, however, the Court of Review

> acknowledge[d] . . . that the constitutional question presented by this case — whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment — has no definitive jurisprudential answer. The Supreme Court's special needs cases involve random stops (seizures) not electronic searches. In one sense, they can be thought of as a greater encroachment into personal privacy because they are not based on any particular suspicion. On the

---

[208] *Id.* at 744.

[209] 531 U.S. at 42, *cited in Court of Review op.*, 310 F.3d at 745.

[210] 531 U.S. at 44, *cited in Court of Review op.*, 310 F.3d at 746.

[211] *Court of Review op.*, 301 F.3d at 746.

[212] *Id.*

[213] *Id.*

> other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning.[214]

The Court of Review reversed the FISC's orders before it for electronic surveillance "to the extent they imposed conditions on the grant of the government's applications, vacate[d] the FISA court's Rule 11, and remand[ed] with instructions to grant the applications as submitted and proceed henceforth in accordance with this opinion."[215]

50 U.S.C. § 1803(b) provides that, where the Court of Review upholds a denial by the FISC of a FISA application, the United States may file a petition for certiorari to the United States Supreme Court. Since consideration of applications for FISA orders is ex parte, there is no provision in FISA for an appeal to the United States Supreme Court from a decision of the Court of Review by anyone other than the United States. Nevertheless, on February 18, 2003, a petition for leave to intervene and a petition for writ of certiorari to the U.S. Foreign Intelligence Surveillance Court of Review was filed in this case in the U.S. Supreme Court by the American Civil Liberties Union, National Association of Criminal Defense Lawyers, American-Arab Anti-Discrimination Committee, and the Arab Community Center for Economic and Social Services. On March 14, 2003, the Bar Association of San Francisco filed a motion to file an amicus curiae brief in support of the motion to intervene and petition for certiorari. On March 24, 2003, the Supreme Court denied the motion for leave to intervene in order to file a petition for a writ of certiorari and denied the motion for leave to file an amicus curiae brief.[216]

Conclusion

The Foreign Intelligence Surveillance Act, as amended, provides a statutory structure to be followed where electronic surveillance, 50 U.S.C. § 1801 *et seq.*, physical searches, 50 U.S.C. § 1821 *et seq.*, or pen registers or trap and trace devices, 50 U.S.C. § 1841 *et seq.*, for foreign intelligence gathering purposes are contemplated. In addition, it provides a statutory mechanism for the FBI to seek production of "any tangible things" for an investigation seeking foreign intelligence information not involving a U.S. person or to protect against international terrorism or clandestine intelligence with respect to any person under 50 U.S.C. § 1861. FISA 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 appears intended to protect personal liberties safeguarded by the First and Fourth Amendments while providing a means to ensure national security interests.

---

[214] *Id.*

[215] *Id.*

[216] American Civil Liberties Union v. United States, Docket No. 02M69, 538 U.S. 920 (March 24, 2003). The disposition of the case appears on the Supreme Court's Order List for that date. It is interesting to note that both the Petition for Leave to Intervene and Petition for a Writ of Certiorari filed by the American Civil Liberties Union, et al., and the motion to file an amicus curiae brief of the Bar Association of San Francisco were filed under the name In re: Sealed Case of the Foreign Intelligence Surveillance Court of Review No. 02-001.

The USA PATRIOT Act, P.L. 107-56, increased the number of FISC judges from 7 to 11, while expanding the availability of FISA electronic surveillance, physical searches and pen registers and trap and trace devices. For example, under P.L. 107-56, an application for a court order permitting electronic surveillance or a physical search under FISA is now permissible where "a significant purpose" of the surveillance or physical search, rather than "the purpose" or, as interpreted by some courts, "the primary purpose" of the surveillance or physical search, is to gather foreign intelligence information. While the previous language withstood constitutional challenge, the Supreme Court has not yet determined the constitutional sufficiency of the change in the FISA procedures under the Fourth Amendment. On the other hand, the U.S. Foreign Intelligence Court of Review has examined a number of constitutional issues in *In re Sealed Case*, finding that FISA orders, if not satisfying the constitutional warrant requirement, are close to doing so; and finding that, even if a FISA order does not qualify as a warrant for Fourth Amendment purposes, electronic surveillance under FISA as amended by the USA PATRIOT Act is reasonable and therefore constitutional. At the same time, however, the Court of Review acknowledged that the constitutional question of whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment "has no definitive jurisprudential answer."[217]

The USA PATRIOT Act also amended FISA to allow court orders permitting so-called multipoint or "roving" electronic surveillance, where the orders do not require particularity with respect to the identification of the instrument, place, or facility to be intercepted, upon a finding by the court that the actions of the target of the surveillance are likely to thwart such identification. P.L. 107-108 further clarified this authority.

Under P.L. 107-56, pen registers and trap and trace devices may now be authorized for e-mails as well as telephone conversations. In addition, the act expanded the previous FBI access to business records, permitting court ordered access in connection with a foreign intelligence or international terrorism investigation not just to business records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities, but to any tangible things.

While expanding the authorities available for foreign intelligence investigations, FISA, as amended by the USA PATRIOT Act and the Intelligence Authorization Act for FY2002, also contains broader protections for those who may be the target of the various investigative techniques involved. For example, whether the circumstances involve electronic surveillance, physical searches, pen registers or trap and trace devices or access to business records and other tangible items, FISA, as amended by the USA PATRIOT Act, does not permit the court to grant orders based solely upon a United States person's exercise of First Amendment rights.[218]

In addition, P.L. 107-56 created a new private right of action for persons aggrieved by inappropriate disclosure or use of information gleaned or derived from

---

[217] *Court of Review op.*, 310 F.3d at 746.

[218] *See, e.g.*,50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A), 1842(a)(1), 1843(b), 1861(a)(1), and 1861(a)(2).

electronic surveillance, physical searches or the use of pen registers or trap and trace devices. These claims can be brought against the United States for certain willful violations by government personnel.

Finally, the inclusion of a sunset provision for the FISA changes made in the USA PATRIOT Act, with the exception of the increase in the number of FISC judges, provides an opportunity for the new authorities to be utilized and considered, and an opportunity for the Congress to revisit them in light of that experience.

Sections 898 and 899 of the Homeland Security Act of 2002, P.L. 107-296, amended FISA, 50 U.S.C. §§1806(k)(1) and 1825(k)(1) respectively, to permit federal officers conducting electronic surveillance or physical searches to acquire foreign intelligence information under FISA to consult with federal law enforcement officers "or law enforcement personnel of a state or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)." Such consultations are to coordinate efforts to investigate or protect against actual or potential attacks or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage or international terrorism by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or an agent of a foreign power. These sections also state that such consultations do not preclude the Assistant to the President for National Security Affairs or other designated Executive Branch officials from making the necessary certifications as part of the application process for a FISA court order under 50 U.S.C. §§ 1804(a)(7) or 1823(a)(7), nor are these consultations to preclude entry of an order under 50 U.S.C. §§ 1805 or 1824.[219]

---

[219] Section 897 of the Homeland Security Act of 2002, which dealt with "Foreign Intelligence Information," amended Section 203(d)(1) of the USA PATRIOT Act, 50 U.S.C. § 403-5d(1), to provide authority, consistent with the responsibility of the DCI to protect intelligence sources and methods and that of the Attorney General to protect sensitive law enforcement information,

> for information revealing a threat of an actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of an foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and the Director of Central Intelligence shall jointly issue.

In light of the Court of Review's interpretation of "foreign intelligence information" under FISA as including investigations of what the Court of Review termed "foreign intelligence

(continued...)

Section 6001 of Title VI of FISA, as added by the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, expanded the definition of "agent of a foreign power" in the context of non-U.S. persons to encompass those who engage in international terrorism or in activities in preparation for international terrorism, regardless of whether they have any connection or affiliation with a foreign government or other foreign organization or entity. This new definition is included among those FISA provisions subject to the sunset provisions in Section 224 of the USA PATRIOT Act. Section 6002 of the new Title VI of FISA also imposed new, detailed semiannual reporting requirements to facilitate congressional oversight of the implementation of the Act.

In addition to examining the statutory structure in FISA, as amended, this report has explored two published decisions, one from the FISC in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court* and one from the U.S. Foreign Intelligence Court of Review in *In re Sealed Case*. Because historically the decisions of the FISC have not been made public, and because the opinion of the U.S. Foreign Intelligence Surveillance Court of Review discussed in this report was the first decision ever made by that court, the recent decisions of the FISC and the Court of Review provided a unique opportunity to observe the decision-making processes and differing perspectives of the two courts created by FISA.

The FISC's decision was set against a backdrop of a significant number of instances in which the Department of Justice had failed to maintain a "wall" between foreign intelligence gathering and criminal investigations. All seven of the then sitting members of the FISC concurred in the May 17, 2002, order of the court, written by the then presiding judge of the court. The FISC, in its May 17th opinion and order, treated the Attorney General's proposed 2002 "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" as minimization procedures, and approved them as modified. The modifications made by the Court permitted the FBI, the Criminal Division, and OIPR to consult with one another "to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or their agents." In so doing, the FISC permitted such cooperation and coordination to address, among other things, the exchange of information already acquired, identification of categories of information needed and being sought, prevention of either foreign intelligence gathering or criminal law enforcement investigation or interest from obstructing or hindering the other; compromise of either investigation, and long term objectives and

---

[219] (...continued)
crimes," it is not clear whether this section might be interpreted as applicable to sharing of information gleaned from FISA surveillances, searches, pen registers, trap and trace devices, or business record requests, particularly where criminal prosecution is a goal of the investigation.

P.L. 108-458, after creating the new position of Director of National Intelligence in Section 1101 of the Act, included conforming amendments, which replaced references to the "Director of Central Intelligence" with "Director of National Intelligence" in a broad range of provisions. However, P.L. 108-458 does not appear to have replaced "Director of Central Intelligence"with "Director of National Intelligence" in 50 U.S.C. § 403-5d.

overall strategy of both investigations to insure that overlapping intelligence and criminal interests of the United States are both achieved.[220] While permitting direct consultation and coordination between components, the FISC required that OIPR be invited to all consultations and, if OIPR was unable to attend, the modified procedures required that OIPR be "forthwith" informed in writing of the substance of the meeting so that the FISC could be notified promptly.[221] In addition, under the procedures as modified by the FISC, law enforcement officials were prohibited from making recommendations to intelligence officials regarding the initiation, operation, continuation or expansion of FISA searches or surveillances. Nor could law enforcement officials direct or control the use of FISA procedures to enhance criminal prosecution. The FBI and the Criminal Division were given the responsibility to ensure that this did not occur, and were also required to make certain that advice intended to preserve the criminal prosecution option did not inadvertently result in the Criminal Division directing or controlling the investigation using FISA tools to further law enforcement objectives.[222] In addition, the FISC adopted a new Rule 11, dealing with criminal investigations in FISA cases, to facilitate monitoring of compliance with its May 17, 2002 order. This rule required all FISA applications to include informative descriptions of ongoing criminal investigations of FISA targets, as well as the substance of consultations between the FBI and criminal prosecutors at the Department of Justice or a U.S. Attorney's office.

In its November 18, 2002 opinion, the Court of Review took a starkly different view of the Attorney General's proposed procedures and firmly rejected the FISC analysis and conclusions. The issue came before the Court of Review as an appeal of two FISC orders, one granting an application to authorize electronic surveillance of an agent of a foreign power subject to restrictions stemming from the FISC May 17th opinion and order and the other renewing the authorization for electronic surveillance subject to the same conditions.

The Court of Review held that the FISC's interpretation of the augmented 1995 procedures and the proposed 2002 procedures as minimization procedures under 50 U.S.C. § 1801(h) was in error. The Court of Review found that the FISC had misconstrued 50 U.S.C. §§ 1801(h) and 1805 and may have overstepped its constitutional authority by asserting authority to govern the internal organization and investigative procedures of the Justice Department.

It found that FISA, as originally enacted, did not create a dichotomy between foreign intelligence information gathering and law enforcement investigations, nor did it require maintenance of a "wall" between such investigations. While FISA as enacted in 1978 required that a national security official certify that "the purpose" of the investigation was to gather foreign intelligence information, the court regarded the definition of "foreign intelligence information" as including evidence of criminal wrongdoing where a U.S. person is the target of the FISA investigation. In light of the fact that the definition of "agent of a foreign power" applicable to U.S. persons

---

[220] *FISC op.*, 218 F. Supp. 2d at 626.

[221] *Id.*

[222] *Id.*

involved criminal conduct, or, in the context of clandestine intelligence operations, the possibility of criminal conduct, the court distinguished "foreign intelligence crimes" from "ordinary crimes." In foreign intelligence crimes, intelligence gathering and criminal investigations may become intertwined.

The Court of Review reviewed past court decisions requiring that, in seeking a FISA order authorizing electronic surveillance, the government must demonstrate that the "primary purpose" of the surveillance was to gather foreign intelligence information and not to further law enforcement purposes. Rejecting the "primary purpose test" as applied by the FISC and the courts of appeals of several circuits, the Court of Review did not find it to be compelled by the statutory language of FISA as originally enacted or by the Fourth Amendment.

The Court of Review also held the FISC to have been in error in its refusal "to consider the legal significance of the Patriot Act's crucial amendments . . . ." In particular, the court focused upon the change of the required certification by the national security official from a certification that "the purpose" of the surveillance was to obtain foreign intelligence information to a certification that "a significant purpose" of the surveillance was to obtain foreign intelligence information in 50 U.S.C. § 1804(a)(7)(B); and the enactment of 50 U.S.C. § 1806(k), authorizing consultation and coordination by federal officers engaged in electronic surveillance to acquire foreign intelligence information with federal law enforcement officers.

Finding that the "significant purpose" amendment recognized the existence of a dichotomy between intelligence gathering and law enforcement purposes, the Court of Review concluded that this test was satisfied if the government had "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[223] While the gathering of foreign intelligence information for the sole objective of criminal prosecution would be precluded by the "significant purpose" language, if "the government entertains a realistic option of dealing with the agent [of a foreign power] other than through criminal prosecution," the court found the "significant purpose" test satisfied.[224] Although the court was of the view that, prior to passage of the USA PATRIOT Act, the FISC may well not have had authority under 50 U.S.C. § 1805(a)(5) to inquire into anything other than the issue of "whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804" the Court of Review concluded that "it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information."[225] The court held that the government's purpose under 50 U.S.C. § 1804(a)(7)(B) was "to be judged by the national security official's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved. . . . [I]f the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into

---

[223] *Id.* at 735.

[224] *Id.*

[225] *Id.*

the certifying officer's purpose — or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval."[226]

The Court of Review also considered whether FISA, as amended, passed constitutional muster under the Fourth Amendment. It deemed the procedures and government showings required under FISA to come close to the minimum requirements for a warrant under the Fourth Amendment, if not meeting such requirements. Assuming *arguendo* that a FISA order was not a warrant for Fourth Amendment purposes, the Court of Review found FISA constitutional because the surveillances authorized thereunder were reasonable.

[226] *Id.* at 736.