No.

In the Supreme Court of the United States

IN RE: SEALED CASE OF THE FOREIGN INTELLIGENCE
SURVEILLANCE COURT OF REVIEW NO. 02-001

AMERICAN CIVIL LIBERTIES UNION, NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS, AMERICAN-ARAB ANTI-DISCRIMINATION
COMMITTEE, *and* ARAB COMMUNITY CENTER FOR ECONOMIC AND SOCIAL SERVICES, *Petitioners.*

ON PETITION FOR LEAVE TO INTERVENE AND PETITION FOR A WRIT OF CERTIORARI TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

PETITION FOR LEAVE TO INTERVENE AND PETITION FOR A WRIT OF CERTIORARI

ANN BEESON
Counsel of Record
JAMEEL JAFFER
STEVEN R. SHAPIRO
American Civil Liberties Union Foundation
125 Broad Street

New York, NY 10004
(212) 549-2601

JOSHUA L. DRATEL
JOHN D. CLINE
TOM GOLDSTEIN
National Association of
Criminal Defense Lawyers
14 Wall Street, 28th Floor
New York, NY 10005
(212) 732-0707

Counsel for Petitioners

PARTIES TO THE PROCEEDINGS

Petitioners are the American Civil Liberties Union, the National Association of Criminal Defense Lawyers, American-Arab Anti-Discrimination Committee, and the Arab Community Center for Economic and Social Services. Respondent is the United States.

CORPORATE DISCLOSURE STATEMENT

In accordance with United States Supreme Court Rule 29.6, petitioners confirm that none of the petitioners have parent companies nor do any publicly held companies own ten percent or more of their stock.

In the Supreme Court of the United States

No.

IN RE: SEALED CASE OF THE FOREIGN
INTELLIGENCE SURVEILLANCE COURT OF REVIEW
NO. 02-001

AMERICAN CIVIL LIBERTIES UNION, ET AL., *Petitioners.*

PETITION FOR A WRIT OF CERTIORARI

QUESTIONS PRESENTED

(1) Does the USA PATRIOT Act ("Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), authorize the government to conduct surveillance under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq*., even where the government's primary purpose is law enforcement rather than foreign intelligence?

(2) If the Patriot Act authorizes the government to conduct surveillance under FISA even where the government's primary purpose is law enforcement, does FISA as amended by the Patriot Act contravene the First or Fourth Amendment of the United States Constitution?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Legislative Materials

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioners respectfully petition for a writ of *certiorari* to review the judgment of the Foreign Intelligence Surveillance Court of Review in this case.

INTRODUCTION

Petitioners seek this Court's review of the first-ever decision of the Foreign Intelligence Surveillance Court of Review ("Court of Review"), a decision that seriously compromises the privacy and free-speech rights of people living in the United States. In an extraordinary and far-reaching ruling that conflicts with decisions of this Court and a number of lower courts, the Court of Review construed provisions of the USA Patriot Act ("Patriot Act") to allow the government vastly to expand its surveillance of Americans by using the Foreign Intelligence Surveillance Act ("FISA") even in investigations whose primary purpose is law enforcement rather than foreign intelligence. The Court of Review's decision effectively overturned a decision of the Foreign Intelligence Surveillance Court ("FISA Court") that had avoided the constitutional question by interpreting the amended FISA more narrowly, though the Court of Review acknowledged that "the constitutional question presented in this case . . . has no definitive jurisprudential answer." App. 52a. Petitioners urge this Court to grant review in order to clarify that the government cannot constitutionally conduct surveillance under lower foreign-intelligence standards where its primary purpose is law enforcement rather than foreign intelligence.

OPINIONS BELOW

The opinion of the Foreign Intelligence Surveillance Court of Review in *In re: Sealed Case No. 02-001* is reprinted as Appendix A hereto. *See* App. 1a-53a. The

opinion of the Foreign Intelligence Surveillance Court is reprinted as Appendix B hereto. *See* App. 54a-86a.

JURISDICTION

The judgment of the Court of Review was entered on November 18, 2002. This Court has jurisdiction under 50 U.S.C. § 1803(b), under 28 U.S.C. § 1254(1), and under the All Writs Act, 28 U.S.C. § 1651(a).

Section 1803(b) of Title 50 creates jurisdiction in this Court to review, on petition of the government for a writ of *certiorari*, any Court of Review decision upholding the denial of a government surveillance application.[1] The statute is silent as to whether a party *other* than the government may petition for a writ of *certiorari* where the government *prevails* in the Court of Review. Petitioners urge the Court to construe the statute generously. A reading that would disallow parties other than the government from petitioning for a writ of *certiorari* would effectively foreclose this Court from reviewing any decision by the Court of Review in favor of the government. Yet nothing in the statute suggests that Congress intended that result. On the contrary, the apparent intent of the statute is to ensure that this Court will be able to correct the Court of Review when necessary. Congress's failure specifically to authorize parties other than the government to seek this Court's review is easily explained by the fact that, in litigation originating in the FISA Court, the government is ordinarily the only party. If Congress had intended that in certain cases the Court of Review rather than this Court would be the final arbiter of difficult constitutional

[1] Section 1803(b) provides, in relevant part, "If [the Court of Review] 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."

questions, it would surely have manifested its intent in clear language.

This Court also has jurisdiction under 28 U.S.C. § 1254, which provides that "[c]ases in the courts of appeals may be reviewed by the Supreme Court . . . [b]y writ of *certiorari* granted upon the petition of any party to any civil or criminal case . . . ." The Court of Review is a "court[] of appeals" within the meaning of this provision. *See Tully v. Mobil Oil Corp.*, 455 U.S. 245 (1982) (per curiam) (holding that the Temporary Emergency Court of Appeals was a 'court of appeals' for purposes of § 1254(2)).

Finally, if neither of the provisions cited above provides jurisdiction, this Court has jurisdiction under the All Writs Act, 28 U.S.C. § 1651(a), which provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." In *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985), this Court stated that "[w]here a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling." It also stated, however, that the All Writs Act "fill[s] the interstices of federal judicial power when those gaps threate[n] to thwart the otherwise proper exercise of federal courts' jurisdiction." *Id.* at 41.

Petitioners submit that the All Writs Act provides jurisdiction here. First, FISA does not "specifically address[]" the question whether a party other than the government may petition for a writ of *certiorari*. Second, if jurisdiction did not exist under the All Writs Act, this Court's authority to review a decision of the Court of Review would depend on whether the decision was favorable or unfavorable to the government. Finally, jurisdiction under the All Writs Act is appropriate in this extraordinary case for a number of other reasons. The FISA Court, sitting *en banc* for the first

time in its history, ruled unanimously against the government. The Court of Review, which ultimately reversed the FISA Court, convened for the first time to hear the government's appeal. Both the lower court and the Court of Review recognized the broad impact of their rulings and published their decisions. Though some of petitioners here were permitted to file briefs *amicus curiae* in the lower court proceedings, the government was the only party. The litigation clearly involves important constitutional issues concerning FISA itself and not simply the legal sufficiency of a particular surveillance application.

CONSTITUTIONAL AND STATUTORY PROVISIONS

The First Amendment to the United States Constitution provides in relevant part that "Congress shall make no law . . . abridging the freedom of speech, or of the press." The Fourth Amendment provides that "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." The pertinent provisions of FISA, as amended by the Patriot Act, are reprinted in Appendix C hereto. *See* App. 87a-105a.

STATEMENT OF THE CASE

This case involves the meaning and constitutionality of certain amendments made by the Patriot Act to FISA. The Court of Review held that the Patriot Act constitutionally authorizes the government to rely on FISA even when the primary purpose of an investigation is law enforcement rather than foreign intelligence.

FISA was enacted in 1978 to govern surveillance of foreign powers and their agents inside the United States. The statute created the FISA Court, a court composed of seven (now eleven) federal district court judges, and empowered

the FISA Court to grant or deny government applications for surveillance orders.[2] FISA also set out the conditions that the government is required to satisfy before the FISA Court will issue a surveillance order. These standards are substantially less stringent than those that the Fourth Amendment ordinarily requires. In order to obtain a FISA surveillance warrant, the government must show probable cause to believe that the prospective surveillance target is a "foreign power" or an "agent of a foreign power," 50 U.S.C. § 1804(a)(4)(A), and it must certify, among other things, that "the purpose" (now, "significant purpose") of the surveillance is to obtain "foreign intelligence information," *id*. § 1804(a)(7)(B). The government is *not* required, however, to articulate any suspicion that the target is engaged in criminal activity. It is not required to show (or even to certify) that the facilities to be targeted are being used for the kinds of communications that are sought to be intercepted. It is not required to provide the target with even delayed notice that her privacy has been compromised – even if the target is ultimately determined to have been inappropriately or illegally targeted. In essence, FISA allows the government to conduct electronic surveillance and physical searches without complying with the ordinary requirements of the Fourth Amendment.

According to the government, the Patriot Act dramatically expanded the class of investigations in which FISA is available. Prior to the Patriot Act, the government could invoke FISA only by certifying that "the purpose" of the surveillance was to obtain foreign intelligence information. The Patriot Act replaced "the purpose" with "a significant purpose." 115 Stat. 272, § 218 (amending 50

[2] In its current form, FISA comprises four Subchapters. The first and second address electronic surveillance and physical searches, respectively. The third addresses "pen register" and "trap and trace" devices. The fourth addresses government access to certain business records and other tangible things. Only the first and second of FISA's Subchapters are at issue in this litigation.

U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)). On the government's theory, that change allows it to obtain surveillance warrants under FISA's undemanding standards even where its primary purpose is law enforcement rather than foreign intelligence.

In March of last year, the Attorney General requested that the FISA Court adopt a new set of procedures (the "2002 Procedures") for all FISA investigations concerning United States persons.[3] The 2002 Procedures were to supersede procedures that had been in place since 1995 (the "1995 Procedures"). Although styled as "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," the 2002 Procedures in fact sought to implement the Attorney General's expansive interpretation of the Patriot Act's amendments to FISA. Most relevant to this litigation, the 2002 Procedures endorsed the use of FISA in investigations whose primary purpose is law enforcement rather than foreign intelligence. They also stated that FISA surveillance could now be initiated, directed, and controlled by law enforcement rather than intelligence officials.

In a decision dated May 17, 2002, the FISA Court rejected the 2002 Procedures. *See* App. 54a-86a. The court noted that, while the 1995 Procedures "permit[ted] substantial consultation and coordination" between the intelligence and criminal officials, the court had closely supervised such consultation and coordination to ensure that FISA was "not being used *sub rosa* for criminal investigations." *Id.* 68a. Notwithstanding this close supervision, the government had abused its FISA authority in "an alarming number of instances." *Id.*[4] The Court found

---

[3] "United States person" is defined in 50 U.S.C. § 1801(i). *See* App. 91a.

[4] For example, the government came forward in September 2000 "to confess error in some 75 applications related to major terrorist attacks

that the 2002 Procedures, far from addressing the government's history of abuse, would eliminate altogether the safeguards that prevented the government from using FISA as a means of evading ordinary Fourth Amendment requirements in routine criminal investigations. *See id*. 72a. The March 2002 Procedures, the Court wrote,

> mean[] 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.

Id. 76a. Rather than denying the Attorney General's motion, however, the Court modified the proposed procedures, first by requiring that consultations between criminal and intelligence investigators be monitored by officials of the Office of Intelligence Policy Review, and second by adding a proviso that prohibited law enforcement officials from "directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives." *Id*. 77a.

The Attorney General appealed the FISA Court's decision to the Court of Review, which convened for the first

---

directed [against] the United States." App. 69a. In November 2000, after "a special meeting to consider the troubling number of inaccurate FBI affidavits in so many FISA applications," the FISA Court barred one FBI agent from appearing before it as a FISA affiant. *Id.* In March 2001, the government reported further abuses in a different series of applications. "In virtually every instance," the Court noted, "the government's misstatements and omissions in FISA applications and violations of the Court's orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors." *Id*. 70a.

time in order to hear the appeal.[5] On appeal, the government advanced two arguments. The first of these, which the government had not presented to the FISA Court (and indeed had never before advanced before Congress or any court), was that there had never been any statutory basis for the view – adopted by the Fourth Circuit in *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980), and then by several other courts – that FISA is available only where the government's primary purpose is foreign intelligence. After examining the relevant FISA provisions as they existed before the Patriot Act, the Court of Review agreed. In the Court's view, FISA as originally enacted did not envision a dichotomy between law enforcement and foreign intelligence. Indeed, the Court noted, "[t]he definition of an agent of a foreign power, if it pertains to a U.S. person (which is the only category relevant to this case), is closely tied to criminal activity." App. 8a. Thus, the Court accepted the government's view that the primary-purpose restriction did not have a statutory basis before the Patriot Act. It proceeded to find, however, that the Patriot Act's "significant purpose" amendment had endorsed the relevance of a judicial inquiry into the government's purpose:

> [E]ven though we agree that the original FISA did not contemplate the "false dichotomy" [between foreign intelligence and law enforcement], the Patriot Act actually did – which makes it no

[5] The Attorney General did not appeal the FISA Court May 17 order directly, presumably because that decision did not pertain to a specific surveillance order. Instead, the Attorney General submitted a surveillance application on July 19, proposing the 2002 Procedures without modification. The FISA judge hearing that application granted the order but modified the proposed procedures in accordance with the FISA Court's May 17 order. The Attorney General then appealed the July 19 order, along with an October 17 order granting, with modifications, the government's application for renewal of the July 19 surveillance order. *See* App. 22a.

> longer false. . . . [I]n light of the significant purpose amendment . . . it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information.

Id. 32a.

Having concluded that the "significant purpose" amendment had endorsed the dichotomy between foreign intelligence and law enforcement, the Court could not accept the government's principal argument. It was sympathetic, however, to the government's alternative argument – that the "significant purpose" amendment had been intended to "eliminate[] any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses." *Id*. 33a. After the Patriot Act, the Court reasoned, the government meets its statutory obligation as long as "the certification of the application's purpose articulates a broader objective than criminal prosecution . . . and includes other non-prosecutorial responses." *Id*. "So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test." *Id*. 32a.

The Court thus made clear its view that the Patriot Act amendments license the use of FISA even if the government's primary purpose is law enforcement. Indeed, the Court reasoned that the government may use FISA even for the primary purpose of prosecuting ordinary, *non*-"foreign-intelligence crimes," so long as the crime is not "wholly unrelated" to foreign intelligence. *Id.* 34a.

The Court dedicated the remainder of its opinion to addressing the constitutionality of the Patriot Act

amendments.[6] The Court acknowledged the significant differences between FISA's procedural requirements and those of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), Pub. L. 90-351, tit. III, 82 Stat. 211, the statute that governs electronic surveillance in criminal investigations. The Court wrote, "to the extent the two statutes diverge in constitutionally relevant areas . . . a FISA order may not be a 'warrant' contemplated by the Fourth Amendment," i*d*. 44a, but declined to decide the issue. Instead, it proceeded directly to the question whether FISA searches are reasonable.

The Court expressly rejected *Truong* and other Court of Appeals cases holding that the government cannot constitutionally invoke any foreign-intelligence exception to the Fourth Amendment's usual requirements where its primary purpose is law enforcement. The Court of Review held that these cases were misguided because "criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts." *Id.* 46a. The Court also rejected *amici*'s reliance on this Court's "special needs" cases. *See id.* 50a-51a. The Court held that these cases were inapposite because, whatever the purpose of any particular FISA investigation, FISA is a statute whose "programmatic purpose" is not law enforcement but foreign intelligence. *Id*. 52a. The Court concluded:

> [W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant

[6] The Court recognized at the outset that "some of the very senators who fashioned the Patriot Act amendments" had expressed concern that the "significant purpose" amendment would give rise to serious constitutional questions. App. 35a. For example, Senator Leahy stated that "[n]o matter what statutory change is made . . . the court may impose a constitutional requirement of 'primary purpose' based on the appellate court decisions upholding FISA against constitutional challenges over the past 20 years." *Id.* (internal quotation marks omitted).

> standards, certainly come close. We, therefore, believe firmly . . . that FISA as amended is constitutional because the surveillance it authorizes are reasonable.

Id. 53a.

REASONS FOR GRANTING THE WRIT

Although FISA was enacted in 1978, this Court has never considered the statute's constitutionality. The question has become extraordinarily important in light of the Court of Review's interpretation of the Patriot Act. This Court should accept review in order to make clear that the government may not constitutionally rely on any foreign-intelligence exception to the Fourth Amendment's usual requirements in investigations whose primary purpose is law enforcement rather than foreign intelligence.

The Court of Review's decision, which upheld the constitutionality of the relevant Patriot Act amendment, need not have addressed the constitutional question at all, because the statute supports a narrower construction that would avoid the constitutional question altogether. In any event, the Court of Review's answer to the constitutional question was incorrect. The decision conflicts with the clear rulings of this Court by sanctioning warrantless and unreasonable searches in routine criminal investigations, by allowing the government to conduct searches for law enforcement purposes without providing notice or establishing criminal probable cause, and by foreclosing meaningful judicial review of FISA surveillance applications. It also conflicts with decisions of numerous lower federal courts that limited any foreign-intelligence exception to investigations whose primary purpose is foreign intelligence. Finally, it contravenes this Court's jurisprudence by undermining Fourth Amendment safeguards that previously inhibited the government from infringing First Amendment rights.

For these reasons, petitioners urge the Court to grant review in this case.

I. THE COURT OF REVIEW'S DECISION PRESENTS AN IMPORTANT STATUTORY AND CONSTITUTIONAL QUESTION CONCERNING THE SCOPE OF ANY FOREIGN-INTELLIGENCE EXCEPTION TO THE FOURTH AMENDMENT'S USUAL REQUIREMENTS

FISA was enacted to establish a framework within which the Executive Branch may conduct intelligence surveillance of foreign powers and their agents inside the United States. The statute allows the government to conduct surveillance on less demanding standards than are ordinarily required by the Fourth Amendment. Although FISA has now governed foreign-intelligence surveillance for twenty-five years, this Court has never before reviewed the statute's constitutionality.

FISA was enacted in response to rampant abuse of executive surveillance powers. During the Cold War and the McCarthy era, the FBI routinely installed electronic surveillance devices on private property in order to monitor the conversations of suspected communists. *See* S. Rep. 95-604, at 11 (1977). The FBI's COINTELPRO, authorized by President Nixon in the 1970s, wiretapped Martin Luther King, Jr. and other dissidents and anti-war protesters solely because of their political beliefs. *See generally* 2 Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, Final Report ("Church Committee Report"), S. Rep. 94-755 (1976). The CIA illegally surveilled as many as seven thousand Americans in Operation CHAOS, including individuals involved in the peace movement, student activists, and black nationalists. *See generally Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982). The Church Committee Report, issued in 1976,

concluded that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature." Church Committee Report, at 2.

While FISA was enacted in part as a response to such abuse, the standards that govern FISA surveillance have always been substantially less stringent than the Fourth Amendment requires in criminal investigations. When FISA was first enacted, however, it applied only to a relatively narrow and strictly delineated class of investigations. This is no longer the case. Since 1978, Congress has amended FISA on numerous occasions, each time adding new surveillance tools to the executive's foreign-intelligence toolbox.[7] As a result, FISA as it exists now bears little resemblance to the statute that Congress enacted in 1978.

The Patriot Act amendments at issue in this case are the most recent in the long list of amendments to FISA, and they are also the most significant changes to FISA since the statute's enactment. While most previous amendments have added to the tools available to the government in FISA investigations, the Patriot Act amendments dramatically expand the *class* of investigations in which FISA is available. Previously, FISA's significance was limited to investigations whose primary purpose was foreign intelligence. The Patriot Act amendments – on the Court of Review's theory, at least –

---

[7] For example, the statute was amended in 1995 to allow the government to obtain FISA orders for physical searches as well as electronic surveillance. *See* 50 U.S.C. §§ 1821-29. The statute was amended again in 1998 to allow the government to install "pen registers" and "trap and trace" devices, *see id.* §§ 1841-46, and to allow the government access to certain business records of private individuals and organizations, *see id.* §§ 1861-62. The statute was amended yet again in 1999 to expand the definition of "agent of a foreign power." *See id.* § 1801(b)(2)(D). The Patriot Act made numerous amendments to FISA in addition to those at issue in this case.

extend FISA's significance even to investigations whose primary purpose is law enforcement. If the Court of Review's theory is correct, the government may now use FISA as a law-enforcement tool in a broad category of criminal investigations.

While FISA as originally enacted raised constitutional questions, the extension of FISA to investigations whose purpose is not primarily foreign intelligence raises constitutional concerns of an entirely different magnitude. What began as a relatively narrow and well-defined exception to the Fourth Amendment's ordinary strictures has now become a license for the executive to ignore the Fourth Amendment altogether in a broad class of criminal investigations.[8] This vast expansion in the foreign-intelligence exception has occurred even though, as indicated above, this Court has never sanctioned even the comparatively narrow exception contemplated by FISA as originally enacted.

This Court should accept review in order to make clear that any foreign-intelligence exception cannot constitutionally apply in investigations whose primary purpose is law enforcement.

II. THE COURT OF REVIEW DISREGARDED THE CANON OF CONSTITUTIONAL AVOIDANCE BY REACHING DIFFICULT CONSTITUTIONAL QUESTIONS UNNECESSARILY

Under the canon of constitutional avoidance, when a "statute [is] susceptible of two interpretations, by one of which it would be unconstitutional and by the other valid," a court's "plain duty is to adopt that construction which will

---

[8] A recent proposal would broaden this class even further by removing the "foreign power or agent of a foreign power" requirement in investigations not involving United States persons. *See* s. 113, 108th Cong. (2002).

save the statute from constitutional infirmity." *United States ex rel. Attorney General v. Del. & Hudson Co.*, 213 U.S. 366, 408 (1909). The Court of Review disregarded this canon by adopting the constitutionally problematic theory that FISA is available even when the government's primary purpose is law enforcement.

Through the enactment of Title III and FISA, Congress created two distinct authorization schemes for government surveillance.[9] Title III, enacted in 1968, governs electronic surveillance in criminal investigations. FISA, enacted in 1978, governs electronic surveillance for foreign-intelligence purposes. Criminal investigations relating to national security crimes have always been governed by Title III. Thus, Title III as originally enacted included espionage, sabotage, and treason as predicate offenses. The Senate referred to these as "the offenses that fall within the national security category." S. Rep. 90-1097, at 67 (1968). These national-security crimes remain predicate offenses under Title III today.[10]

Congress's decision to retain the national-security crimes as predicate offenses to Title III makes clear that Congress did not intend to make FISA available in criminal investigations. As discussed above, the standards that govern FISA surveillance are substantially less demanding than those that govern surveillance under Title III. Congress

---

[9] The focus in this discussion is on the differences between FISA's electronic surveillance provisions and those of Title III. However, there are similar differences between FISA's physical search provisions, *see* 50 U.S.C. §§ 1821-29, and those that govern physical searches conducted in the course of ordinary law enforcement investigations, *see* Fed. R. Crim. P. 41.

[10] Section 201 of the Patriot Act added "any criminal violation of section 229 [of title 18] (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism)." 115 Stat. 272, § 201.

cannot have thought that the government would continue to rely on Title III if the less demanding requirements of FISA were also available. The Court of Review inappropriately disregarded a narrow construction of the Patriot Act's amendments in favor of a broader construction that raises difficult constitutional questions.

III. THE COURT OF REVIEW'S DECISION CONFLICTS WITH THIS COURT'S FOURTH AMENDMENT JURISPRUDENCE

The Court of Review's decision contravenes this Court's Fourth Amendment jurisprudence by holding that the government may constitutionally rely on FISA in investigations whose primary purpose is law enforcement. FISA orders are not warrants within the meaning of the Fourth Amendment, and searches conducted on the basis of FISA orders are presumptively unconstitutional. The Court of Review erred in failing to recognize that FISA orders are not warrants in the constitutional sense, and also erred in finding that FISA surveillance is reasonable. First, FISA searches are not based on criminal probable cause and FISA orders do not meet the Fourth Amendment's particularity requirement. Second, FISA targets do not receive notice – even delayed notice – that their privacy has been compromised. Finally, the applications for FISA searches are not subject to meaningful judicial scrutiny.

Even if the statute's procedures are constitutionally adequate with respect to surveillance whose primary purpose is foreign intelligence, the Court of Review erred in finding those procedures constitutional in investigations whose primary purpose is law enforcement. This Court's jurisprudence is clear: surveillance whose primary purpose is law enforcement must be conducted in conformity with the usual requirements of the Fourth Amendment.

A. The Court of Review's Decision Disregards the Fourth Amendment By Endorsing Warrantless and Unreasonable Searches in Criminal Investigations

Although the Court of Review acknowledged that a FISA order "may not be" a warrant within the meaning of the Fourth Amendment, App. 44a, it did not actually decide the issue. The Court of Review erred in failing to recognize that FISA orders are not warrants within the meaning of the Fourth Amendment, and it erred in upholding the reasonableness of FISA searches conducted in investigations whose primary purpose is law enforcement.

FISA orders are not warrants within the meaning of the Fourth Amendment. In order to be constitutionally adequate, a warrant must (i) be issued by a neutral, disinterested magistrate; (ii) must be based on a demonstration of probable cause to believe that "the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and (iii) must particularly describe the things to be seized as well as the place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotation marks omitted). FISA orders do not satisfy two of these three independent requirements.

FISA orders do not require the government to show probable cause that the target is committing, has committed, or is about to commit a particular criminal offense. *See, e.g.*, *Gerstein v. Pugh*, 420 U.S. 103, 113-14 (1975). Rather, the government need only show probable cause to believe that the surveillance target is a foreign power or agent of a foreign power. *See* 50 U.S.C. § 1805(a)(3)(A). The Court of Review understated the differences between FISA's probable-cause requirement and ordinary criminal probable cause. Yet the government itself has frankly acknowledged the significant distance between the two standards. In response to a Freedom of Information Act request filed by

Petitioner ACLU and others on August 21, 2002, the FBI released, among other things, a document from the FBI's National Security Law Unit entitled, "What do I have to do to get a FISA?" It states, in relevant part,

> Probable cause in the FISA context is similar to, but not the same as, probable cause in criminal cases. Where a U.S. person is believed to be an agent of a foreign power, there must be probable cause to believe that he is engaged in certain activities, for or on behalf of a foreign power, which activities involve or may involve a violation of U.S. criminal law. The phrase "involve or may involve" indicates that the showing of [nexus to] criminality does not apply to FISA applications in the same way it does to ordinary criminal cases. *As a result, there is no showing or finding that a crime has been or is being committed, as in the case of a search or seizure for law enforcement purposes.* The activity identified by the government in the FISA context may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, that would suffice. *In addition, and with respect to the nexus to criminality required by the definitions of "agent of a foreign power," the government need not show probable cause as to each and every element of the crime involved or about to be involved.*

"What do I have to do to get a FISA?," at 2 (Document released by FBI in response to August 21 Freedom of Information Act request submitted by ACLU et al.) (emphases added).

With respect to the particularity requirement, *see, e.g., Berger v. New York*, 388 U.S. 41, 55-56 (1967), FISA orders

do not require the government to have reason to believe that the surveillance will yield information about a particular offense. Rather, the government need only certify that the information sought is foreign intelligence information. *See* 50 U.S.C. § 1804(a)(7)(A). Nor do FISA orders require that the government show probable cause to believe that the facilities to be surveilled will be used in connection with a particular offense, or even that they will be used to communicate foreign intelligence information. Instead, the government need only show probable cause to believe that the facilities are being used or likely to be used by the surveillance target. *See* 50 U.S.C. § 1805(a)(3)(B).

Indeed, FISA orders also fail to meet the standards set out under Title III, the statute that governs electronic surveillance in criminal investigations. *See* 18 U.S.C. § 2518(3)(a) (requiring government to show probable cause that target is engaged in criminal activity); *id*. § 2518(3)(b) (requiring government to show probable cause that surveillance will yield information about particular offense); *id*. § 2518(3)(d) (requiring government to show probable cause that facilities to be monitored are being used in connection with particular offense); *id*. § 2518(5) (limiting term of surveillance orders to 30 days). Nor do FISA orders meet the standards set out under Rule 41 of the Federal Rules of Criminal Procedure, the rule that governs physical searches in criminal investigations. *See, e.g.*, Fed. R. Crim. P. 41(d)(1) (requiring criminal probable cause); Fed. R. Crim. P. 41(e)(2)(A) (requiring that warrant be executed "within a specified time not longer than 10 days").

Because FISA orders are not warrants within the meaning of the Fourth Amendment, searches conducted under FISA are presumptively unconstitutional. *See, e.g., Payton v. New York*, 445 U.S. 573, 586 (1980); *Chimel v. California*, 395 U.S. 752, 762-763 (1969). This Court has repeatedly emphasized that the failure of government agents to obtain a warrant before conducting a search is not "an inconvenience

to be somehow weighed against the claims of [government] efficiency." *United States v. United States District Court ("Keith")*, 407 U.S. 297, 315 (1972) (internal quotation marks omitted). Rather, the warrant clause "is an important working part of our machinery of government, operating as a matter of course to check the well-intentioned but mistakenly over-zealous executive officers who are a party of any system of law enforcement." *Id*. at 316 (internal quotation marks omitted).

B. The Court of Review's Decision Disregards the Fourth Amendment By Allowing the Government to Conduct Searches for Law Enforcement Purposes Without Providing Notice

The Fourth Amendment generally requires that the subject of a search be provided notice that the search has taken place. *See Wilson v. Arkansas*, 514 U.S. 927 (1995) (holding that common-law "knock-and-announce" principle informs Fourth Amendment reasonableness inquiry); *Miller v. United States*, 357 U.S. 301, 313 (1958) ("The requirement of prior notice of authority and purpose before forcing entry into a home is deeply rooted in our heritage and should not be given grudging application."). While notice need not necessarily be contemporaneous with the search, *see United States v. Donovan,* 429 U.S. 413, 429 n.19 (1977) (holding that delayed-notice provisions of Title III supply a constitutionally adequate substitute for contemporaneous notice), this Court has never upheld a statute that, like FISA, authorizes the government to search a person's home or intercept his communications without *ever* informing him that his privacy has been compromised.

The non-provision of notice in FISA investigations is particularly problematic because notice is withheld as a categorical rule, and not upon an individualized showing of necessity. *See Richards v. Wisconsin*, 520 U.S. 385, 393-94 (1997) (rejecting categorical exception to knock-and-

announce principle for searches executed in connection with felony drug investigations); *Franks v. Delaware,* 438 U.S. 154, 168-72 (1978) (holding that subject of an allegedly illegal search must be afforded an opportunity to challenge the propriety of the search in a proceeding that is both public and adversarial). Except in the few cases that end in prosecutions,[11] FISA targets never learn that their homes or offices have been searched or that their communications have been intercepted. Most FISA targets have no way of challenging the legality of the surveillance or obtaining any remedy for violations of their constitutional rights.

C. The Court of Review's Decision Disregards the Fourth Amendment By Foreclosing Meaningful Judicial Review of FISA Applications

Even if FISA's substantive requirements are constitutional, and petitioners believe they are not, the low level of scrutiny that the FISA Court applies with respect to those requirements is constitutionally inadequate in the context of investigations whose primary purpose is law enforcement. The government satisfies most of FISA's requirements simply by certifying that the requirements are met. *See* 50 U.S.C. § 1804(a)(7) (enumerating necessary

---

[11] Not even FISA targets who are prosecuted are afforded a meaningful opportunity to challenge the surveillance's legality. When a defendant contests the legality of FISA surveillance, the Attorney General may file an affidavit in the district court stating that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). The district court must then review the surveillance application and order *ex parte* and *in camera*, unless disclosure is "necessary to make an accurate determination of the legality of the surveillance." *Id.* In practice, the Attorney General files such affidavits as a matter of course. *See United States v. Nicholson*, 955 F.Supp. 588, 592 (E.D.Va. 1997) ("[T]his Court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance. To the contrary, every court examining FISA-obtained evidence has conducted its review *in camera* and *ex parte*.").

certifications); *see also* App. 34a ("the government's purpose as set forth in a section 1804(a)(7)(B) certification is 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"); *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984) (noting that government's "primary purpose" certification is "subjected to only minimal scrutiny by the courts"); *id*. ("The FISA judge . . . is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information.").

While certain (but not all) of these certifications must be accompanied by "a statement of the basis for the certification," 50 U.S.C. § 1804(a)(7)(E), the statute makes clear that the FISA Court is not to scrutinize such statements carefully, but rather is to defer to the government's certification unless it is "clearly erroneous on the basis of the statement made under § 1804(a)(7)(E)," *id*. § 1805(a)(5). As the Court of Review acknowledged, "this standard of review is not, of course, comparable to a probable cause finding by the judge." App. 40a (internal quotation marks omitted).

Judicial oversight under Title III is substantially more robust. To obtain a surveillance order under Title III, the government must provide the court with "a full and complete statement of the facts and circumstances relied upon by the applicant[] to justify his belief that an order should be issued." 18 U.S.C. § 2518(1)(b). The court may "require the applicant to furnish additional testimony or documentary evidence in support of the application." *Id*. § 2518(2). The government cannot meet any of the statute's substantive requirements merely by certifying that it has met them. On the contrary, with respect to most of the statute's substantive requirements, the statute requires the court to find probable cause to believe that they are satisfied. *See id.* § 2518(3).

In fact, FISA so limits the FISA Court's review of government surveillance applications that the FISA Court is severely inhibited in fulfilling its Article III obligation to serve as a meaningful check against unconstitutional actions by the executive branch. By requiring the FISA Court to defer to executive certifications, the statute forecloses the FISA Court from determining whether the substantive requirements have in fact been satisfied. The Constitution prohibits Congress from restricting federal courts' authority in this way. *See United States v. Klein*, 80 U.S. (13 Wall.) 128 (1872).

Ironically, the Court of Review suggested that the lower FISA court, in exercising its limited oversight under the statute, "may well have *exceeded* the constitutional bounds that restrict an Article III court." App. 25a (emphasis added); *see also id*. 47a (characterizing the FISA Court's ruling as "quite intrusive"). The accusation is remarkable because the FISA Court has *never* turned down a surveillance application. Indeed, according to the Attorney General's own reports, between 1996 and 2001 the FISA Court approved without modification 5207 of 5209 applications, or 99.96% of the total.[12] At least with respect to searches whose primary purpose is law enforcement, the review contemplated by the statute is constitutionally inadequate.

D. The Court of Review's Decision Conflicts With This Court's "Special Needs" Jurisprudence

The Court of Review upheld the constitutionality of the Patriot Act's amendments in part by reference to this Court's "special needs" cases. Yet the "special needs" doctrine simply has no application to searches whose primary purpose is law enforcement. On the contrary, those cases stand for the proposition that "[a] search unsupported by probable

---

[12] The Attorney General's annual reports to Congress regarding the Foreign Intelligence Surveillance Act are available at < http://www.usdoj.gov/04foia/readingrooms/oipr_records.htm>.

cause can be constitutional . . . when special needs, *beyond the normal need for law enforcement*, make the warrant and probable-cause requirement impracticable." *Vernonia School District 47J v. Acton*, 515 U.S. 646, 653 (1995) (internal quotation marks omitted and emphasis added).

This Court recently reaffirmed this well-settled rule in *Ferguson v. City of Charleston,* 532 U.S. 67 (2001). That case involved a public hospital's policy of testing pregnant patients for drug use and employing the threat of criminal prosecution as a means of coercing patients into substance-abuse treatment. The Court invalidated the policy. "In other special needs cases," the Court wrote, "we . . . tolerated suspension of the Fourth Amendment's warrant or probable cause requirement in part because there was no law enforcement purpose behind the searches in those cases, and there was little, if any, entanglement with law enforcement." *Id*. at 79 n.15; *see also id*. at 88 (Kennedy, J., concurring) In *Ferguson*, however, "the central and indispensable feature of the policy from its inception was the use of law enforcement." *Id*. at 80.

This Court's decision in *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), is to the same effect. *Edmond* involved vehicle checkpoints instituted in an effort to interdict illegal drugs. The government asserted that the drug crimes were a "severe and intractable" problem, and the Court agreed that "traffic in illegal narcotics creates social harms of the first magnitude." *Id*. at 42. Notwithstanding the seriousness of the law-enforcement interest with respect to the particular crimes at issue, however, the Court invalidated the checkpoint policy. "[T]he gravity of the threat alone," Justice O'Connor wrote, "cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose." *Id*. Where the government's "primary purpose [is] to detect evidence of ordinary criminal wrongdoing," *id*. at 38, the Fourth

Amendment forecloses the government from conducting searches except based on probable cause.

The Court of Review acknowledged that the special needs cases apply only where the government's primary purpose is not law enforcement, but it contended that in the present case the relevant purpose is FISA's "programmatic purpose." App. 52a. This Court has made abundantly clear, however, that Fourth Amendment requirements do not turn on a criminal investigation's programmatic or ultimate purpose. In *Ferguson*, for example, the government argued that the ultimate purpose of the hospital's policy was not law enforcement but public health. The Court rejected that argument's relevance, writing:

> The threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose . . . was to ensure the use of those means. In our opinion, the distinction is critical. Because law enforcement involvement always serves some broader social purpose or objective, under respondents' view, virtually any nonconsensual suspicionless search could be immunized under the special needs doctrine by defining the search solely in terms of its ultimate, rather than immediate, purpose.

532 U.S. at 83-84.[13] The Court of Review's decision thus directly conflicts with this Court's special-needs cases.

---

[13] The Court of Review, App. 51a, also relied on the following dictum from *Edmond*: "The Fourth Amendment would almost certainly permit an appropriately tailored road block set up to thwart an imminent terrorist attack of to catch a dangerous criminal who is likely to flee by way of a particular route." *City of Indianapolis v. Edmond*, 531 U.S. at 44. This Court specifically recognized, however, that such exigencies are "far removed" from ordinary criminal investigation. App. 51a. Here, the government makes no showing of exigency. Indeed, FISA surveillance

IV. THE COURT OF REVIEW'S DECISION CONFLICTS WITH THE DECISIONS OF NUMEROUS LOWER FEDERAL COURTS WHICH HAVE HELD THAT ANY FOREIGN-INTELLIGENCE EXCEPTION MUST BE LIMITED TO INVESTIGATIONS WHOSE PRIMARY PURPOSE IS FOREIGN INTELLIGENCE

The Court of Review's ruling rejected the well-settled consensus that any foreign-intelligence exception must be limited to investigations whose primary purpose is foreign intelligence. *See, e.g., United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991), *cert. denied*, 506 U.S. 816 (1992) (stating that FISA may "not be used as an end-run around the Fourth Amendment's prohibition of warrantless searches"); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987), *cert. denied* 486 U.S. 1010 (1988); *United States v. Duggan*, 743 F.2d at 77.

Neither this Court nor any other court until now has ever held that the government can waive the usual Fourth Amendment standards when its purpose is criminal investigation. Indeed, it was accepted even before FISA was enacted – that is, even before there was a statutory basis for the primary-purpose limitation – that any intelligence exception had to be restricted to investigations whose primary purpose was foreign intelligence. Thus in *Keith* the government argued for a domestic-intelligence exception to the warrant requirement by assuring the Court that it would not rely on the exception as a means of evading Fourth Amendment requirements in criminal investigations. *Keith*, 407 U.S. at 318-19. Lower courts that addressed the permissibility of a *foreign*-intelligence exception similarly emphasized that any such exception could not

---

intended to bring a criminal prosecution would make no sense in the face of an imminent terrorist threat.

constitutionally be used in law enforcement investigations. For example, the Fourth Circuit in *Truong* recognized a foreign-intelligence exception to the warrant requirement but limited the exception to cases in which "the surveillance is conducted primarily for foreign intelligence reasons." *See Truong,* 629 F.2d at 915 (internal quotation marks omitted). The court emphasized that this requirement stemmed from the Fourth Amendment:

> [O]nce surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and . . . importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution.

Id. Other pre-FISA cases affirmed the same principle. *See, e.g., United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974) ("Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental."), *cert. denied*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973); *id*. at 427 (Goldberg, J., concurring).

The Court of Review disregarded these cases and disagreed with *Truong's* assumption that "foreign policy concerns recede" when the government's principal intent is to prosecute. App. 46a. It then rejected the primary-purpose limitation entirely, reasoning that the limitation inhibits or even forecloses the government from using criminal prosecution as a tool to protect national security. *See id. 46a-50a*. In fact, the primary-purpose limitation has *never* prevented the government from using criminal prosecution as

a tool to protect national security. Its only effect is to dictate which standards the government must meet in order to engage in surveillance whose profound intrusiveness even the government does not dispute. *See Berger v. New York*, 388 U.S. at 63 ("It is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded"). The government is always entitled to engage in such surveillance if it can meet the requirements of the Fourth Amendment, and the primary-purpose limitation does not compromise this authority. The Court of Review erred in discounting without discussion the other side of the *Truong* court's reasoning – the principle that privacy concerns come to the fore when the government's intent is to prosecute. *See, e.g., Weeks v. United States*, 232 U.S. 383, 393 (1914) (stating that exclusionary rule is necessary because "[i]f letters and documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the Fourth Amendment . . . is of no value").

In summary, the Court of Review's conclusion that FISA searches and surveillance are reasonable when used primarily for criminal investigation finds no support in this Court's or appellate court rulings.

V. THE COURT OF REVIEW'S DECISION JEOPARDIZES FIRST AMENDMENT FREEDOMS BY ELIMINATING FOURTH AMENDMENT SAFEGUARDS

Traditionally, the warrant and probable cause requirements have served as important safeguards of First Amendment interests by preventing the government from intruding into an individual's protected sphere merely because of that individual's exercise of First Amendment rights. Expanding the circumstances in which the government may conduct searches without conforming to

those requirements presents the danger that the government's surveillance power will chill activity that is protected under the First Amendment.

This Court has recognized the importance of the Fourth Amendment in protecting First Amendment rights:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. . . . History abundantly documents the tendency of Government – however benevolent and benign its motives – to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.

Keith, 407 U.S. at 313-14; *see also id*. at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."). The D.C. Circuit made the same point in *Zweibon v. Mitchell,* 516 F.2d. 594 (D.C. Cir. 1975), a case that rejected the constitutionality of a warrantless wiretap of the Jewish Defense League:

> Prior judicial review is important not only to protect the privacy interests of those whose conversations the government seeks to overhear, but also to protect free and robust exercise of the First Amendment rights of speech and association by those who might otherwise be chilled by the fear of unsupervised and unlimited Executive power to institute electronic surveillances.

Id. at 633.

The Court of Review's decision endorses a dramatic expansion of the foreign-intelligence exception, and opens the door to surveillance abuses that seriously threatened our democracy in the past. To protect robust and uninhibited debate by petitioners and all Americans, this Court should accept review and strictly limit surveillance that undermines First Amendment freedoms.

A. CONCLUSION

For the reasons stated above, petitioners urge this Court to grant review in this case.

Respectfully submitted.

ANN BEESON
Counsel of Record
JAMEEL JAFFER
STEVEN R. SHAPIRO
American Civil Liberties Union Foundation

JOSHUA L. DRATEL
JOHN D. CLINE
TOM GOLDSTEIN
National Association of Criminal Defense Lawyers

February 2003

Appendix A

UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

Argued September 9, 2002 Decided November 18, 2002

In re: Sealed Case No. 02-001

Consolidated with 02-002

On Motions for Review of Orders of the United States Foreign Intelligence Surveillance Court
(Nos. 02-662 and 02-968)

Theodore B. Olson, Solicitor General, argued the cause for appellant the United States, with whom *John Ashcroft*, Attorney General, *Larry D. Thompson*, Deputy Attorney General, *David S. Kris*, Associate Deputy Attorney General, *James A. Baker*, Counsel for Intelligence Policy, and *Jonathan L. Marcus*, Attorney Advisor, were on the briefs.

Ann Beeson, *Jameel Jaffer*, *Steven R. Shapiro*, for *amicus curiae* American Civil Liberties Union, with whom *James X. Dempsey* for Center for Democracy and Technology, *Kate Martin* for Center for National Security Studies, *David L. Sobel* for Electronic Privacy Information Center, and *Lee Tien* for Electronic Frontier Foundation, were on the brief.

John D. Cline, *Zachary A. Ives*, and *Joshua Dratel*, for amicus curiae National Association of Criminal Defense Lawyers.

Before: GUY, *Senior Circuit Judge, Presiding*; SILBERMAN and LEAVY, *Senior Circuit Judges*.

Opinion for the Court filed *Per Curiam*.

Per Curiam: This is the first appeal from the Foreign Intelligence Surveillance Court to the Court of Review since the passage of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1862 (West 1991 and Supp. 2002), in 1978. This appeal is brought by the United States from a FISA court surveillance order which imposed certain restrictions on the government. Since the government is the only party to FISA proceedings, we have accepted briefs filed by the American Civil Liberties Union (ACLU)[14] and the National Association of Criminal Defense Lawyers (NACDL) as *amici curiae*.

Not surprisingly this case raises important questions of statutory interpretation, and constitutionality. After a careful review of the briefs filed by the government and *amici*, we conclude that FISA, as amended by the Patriot Act,[15] supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution. We therefore remand for further proceedings in accordance with this opinion.

I.

The court's decision from which the government appeals imposed certain requirements and limitations accompanying an order authorizing electronic surveillance of an "agent of a

[14] Joining the ACLU on its brief are the Center for Democracy and Technology, Center for National Security Studies, Electronic Privacy Information Center, and Electronic Frontier Foundation.

[15] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 155 Stat. 272 (Oct. 26, 2001).

foreign power" as defined in FISA. There is no disagreement between the government and the FISA court as to the propriety of the electronic surveillance; the court found that the government had shown probable cause to believe that the target is an agent of a foreign power and otherwise met the basic requirements of FISA. The government's application for a surveillance order contains detailed information to support its contention that the target, who is a United States person, is aiding, abetting, or conspiring with others in international terrorism. [***approx. 1 page deleted***][16] The FISA court authorized the surveillance, but imposed certain restrictions, which the government contends are neither mandated nor authorized by FISA. Particularly, the court ordered that

> law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.

To ensure the Justice Department followed these strictures the court also fashioned what the government refers to as a

[16] The bracketed information is classified and has been redacted from the public version of the opinion.

"chaperone requirement"; that a unit of the Justice Department, the Office of Intelligence Policy and Review (OIPR) (composed of 31 lawyers and 25 support staff), "be invited" to all meetings between the FBI and the Criminal Division involving consultations for the purpose of coordinating 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." If representatives of OIPR are unable to attend such meetings, "OIPR shall be apprized of the substance of the meetings forthwith in writing so that the Court may be notified at the earliest opportunity."

These restrictions are not original to the order appealed.[17] They are actually set forth in an opinion written by the former Presiding Judge of the FISA court on May 17 of this year. But since that opinion did not accompany an order conditioning an approval of an electronic surveillance application it was not appealed. It is, however, the basic decision before us and it is its rationale that the government challenges. The opinion was issued after an oral argument before all of the then-serving FISA district judges and clearly represents the views of all those judges.[18]

We think it fair to say, however, that the May 17 opinion of the FISA court does not clearly set forth the basis for its decision. It appears to proceed from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law

---

[17] To be precise, there are two surveillance orders on appeal, one renewing the other with identical conditions.

[18] The argument before all of the district judges, some of whose terms have since expired, was referred to as an "en banc" although the statute does not contemplate such a proceeding. In fact, it specifically provides that if one judge declines to approve an application the government may not seek approval from another district judge, but only appeal to the Court of Review. 50 U.S.C. §§ 1803 (a), (b).

enforcement officers in the Executive Branch–indeed, it uses the word "wall" popularized by certain commentators (and journalists) to describe that supposed barrier. Yet the opinion does not support that assumption with any relevant language from the statute.

The "wall" emerges from the court's implicit interpretation of FISA. The court apparently believes 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. But the court neither refers to any FISA language supporting that view, nor does it reference the Patriot Act amendments, which the government contends specifically altered FISA to make clear that an application could be obtained even if criminal prosecution is the primary counter mechanism.

Instead the court relied for its imposition of the disputed restrictions on its statutory authority to approve "minimization procedures" designed to prevent the acquisition, retention, and dissemination within the government of material gathered in an electronic surveillance that is unnecessary to the government's need for foreign intelligence information. 50 U.S.C. § 1801(h).

Jurisdiction

This court has authority "to review the denial of any application" under FISA. *Id.* § 1803(b). The FISA court's order is styled as a grant of the application "as modified." It seems obvious, however, that the FISA court's order actually denied the application to the extent it rejected a significant portion of the government's proposed minimization procedures and imposed restrictions on Department of Justice investigations that the government opposes. Indeed, the FISA court was clear in rejecting a portion of the application.

Under these circumstances, we have jurisdiction to review the FISA court's order; to conclude otherwise would elevate form over substance and deprive the government of judicial review of the minimization procedures imposed by the FISA court. See M*obile Comm. Corp. v. FCC*, 77 F.3d 1399, 1403-04 (D.C. Cir.) (grant of station license subject to condition that is unacceptable to applicant is subject to judicial review under statute that permits such review when application for license is denied), cert. denied, 519 U.S. 823 (1996).

II.

The government makes two main arguments. The first, it must be noted, was not presented to the FISA court; indeed, insofar as we can determine it has never previously been advanced either before a court or Congress.[19] That argument is that the supposed pre-Patriot Act limitation in FISA that restricts the government's intention to use foreign intelligence information in criminal prosecutions is an illusion; it finds no support in either the language of FISA or its legislative history. The government does recognize that several courts of appeals, while upholding the use of FISA surveillances, have opined that FISA may be used only if the government's primary purpose in pursuing foreign intelligence information is not criminal prosecution, but the government argues that those decisions, which did not carefully analyze the statute, were incorrect in their statements, if not incorrect in their holdings.

Alternatively, the government contends that even if the primary purpose test was a legitimate construction of FISA prior to the passage of the Patriot Act, that Act's amendments to FISA eliminate that concept. And as a corollary, the

[19] Since proceedings before the FISA court and the Court of Review are *ex parte*-not adversary-we can entertain an argument supporting the government's position not presented to the lower court.

government insists the FISA court's construction of the minimization procedures is far off the mark both because it is a misconstruction of those provisions per se, as well as an end run around the specific amendments in the Patriot Act designed to deal with the real issue underlying this case. The government, moreover, contends that the FISA court's restrictions, which the court described as minimization procedures, are so intrusive into the operation of the Department of Justice as to exceed the constitutional authority of Article III judges.

The government's brief, and its supplementary brief requested by this court, also set forth its view that the primary purpose test is not required by the Fourth Amendment. The ACLU and NACDL argue, inter alia, the contrary; that the statutes are unconstitutional unless they are construed as prohibiting the government from obtaining approval of an application under FISA if its "primary purpose" is criminal prosecution.

The 1978 FISA

We turn first to the statute as enacted in 1978.[20] It authorizes a judge on the FISA court to grant an application for an order approving 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," 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." 50 U.S.C. § 1805(a)(3). As is

[20] As originally enacted, FISA covered only electronic surveillance. It was amended in 1994 to cover physical searches. Pub. L. No. 103-359, 108 Stat. 3444 (Oct. 14, 1994). Although only electronic surveillance is at issue here, much of our statutory analysis applies to FISA's provisions regarding physical searches, 50 U.S.C. §§ 1821-1829, which mirror to a great extent those regarding electronic surveillance.

apparent, the definitions of agent of a foreign power and foreign intelligence information are crucial to an understanding of the statutory scheme.[21] The latter means

(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.

Id. § 1801(e)(1).[22]

The definition of an agent of a foreign power, if it pertains to a U.S. person (which is the only category relevant to this case), is closely tied to criminal activity. The term includes any person who "knowingly engages in clandestine intelligence gathering activities . . . which activities involve or may involve a violation of the criminal statutes of the

---

[21] Foreign power is defined broadly to include, *inter alia*, "a group engaged in international terrorism or activities in preparation therefore" and "a foreign-based political organization, not substantially composed of United States persons." 50 U.S.C. §§ 1801 (a) (4), (5).

[22] A second definition of foreign intelligence information includes information necessary to "the national defense or the security of the United States," or "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2). This definition generally involves information referred to as "affirmative" or "positive" foreign intelligence information rather than the "protective" or "counterintelligence" information at issue here.

United States," or "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor." *Id.* §§ 1801(b)(2)(A), (C) (emphasis added). International terrorism refers to 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 violation* if committed within the jurisdiction of the United States or any State." *Id.* § 1801(c)(1) (emphasis added). Sabotage means activities that "involve a violation of chapter 105 of [the criminal code], or that would involve such a violation if committed against the United States." *Id.* § 1801(d). For purposes of clarity in this opinion we will refer to the crimes referred to in section 1801(a)-(e) as foreign intelligence crimes.[23]

In light of these definitions, it is quite puzzling that the Justice Department, at some point during the 1980s, 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. To be sure, section 1804, which sets forth the elements of an application for an order, required a national security official in the Executive Branch–typically the Director of the FBI–to certify that "the purpose" of the surveillance is to obtain foreign intelligence information (amended by the Patriot Act to read "a significant purpose"). But as the government now argues, the definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism. Indeed, 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

[23] Under the current version of FISA, the definition of "agent of a foreign power" also includes U.S. persons who enter the United States under a false or fraudulent identity for or on behalf of a foreign power. Our term "foreign intelligence crimes" includes this fraudulent conduct, which will almost always involve a crime.

noted, the definition of an agent of a foreign power–if he or she is a U.S. person–is grounded on criminal conduct.

It does not seem that FISA, at least as originally enacted, even contemplated that the FISA court would inquire into the government's purpose in seeking foreign intelligence information. Section 1805, governing the standards a FISA court judge is to use in determining whether to grant a surveillance order, requires the judge to find that

> 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.

50 U.S.C. § 1805(a)(5).[24] And section 1804(a)(7)(E) requires that the application include "a statement of the basis of 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." That language certainly suggests that, aside from the probable cause, identification of facilities, and minimization procedures the judge is to determine and approve (also set forth in section 1805), the only other issues are whether electronic surveillance is necessary to obtain the information and whether the information sought is actually foreign intelligence

[24] Section 1804(d) simply provides that "[t]he 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."

information–not the government's proposed use of that information.[25]

Nor does the legislative history cast doubt on the obvious reading of the statutory language that foreign intelligence information includes evidence of foreign intelligence crimes. To the contrary, the House Report explained:

> [T]he term "foreign intelligence information," especially as defined in subparagraphs (e)(1)(B) and (e)(1)(C), can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities. With respect to information concerning U.S. persons, foreign intelligence information includes information necessary to protect against clandestine intelligence activities of foreign powers or their agents. Information about a spy's espionage activities obviously is within this definition, and it is *most likely at the same time evidence of criminal activities*.

H.R. REP. NO. 95-1283 (hereinafter "H. REP.") at 49 (1978) (emphasis added).

The government argues persuasively that arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity. The government might wish to surveil the agent for some

---

[25] At oral argument before the FISA judges, the court asked government counsel whether a companion provision of FISA, section 1822(c), that gives the court *jurisdiction* over physical searches "for *the purpose* of obtaining foreign intelligence information," obliged the court to consider the government's "primary purpose." We think that language points in the opposite direction since it would be more than a little strange for Congress to require a court to make a searching inquiry into the investigative background of a FISA application before concluding the court had jurisdiction over the application.

period of time to discover other participants in a conspiracy or to uncover a foreign power's plans, but typically at some point the government would wish to apprehend the agent and it might be that only a prosecution would provide sufficient incentives for the agent to cooperate with the government. Indeed, the threat of prosecution might be sufficient to "turn the agent." It would seem that the Congress actually anticipated the government's argument and explicitly approved it. The House Report said:

> *How this information may be used* "to protect" against clandestine intelligence activities *is not prescribed* by the definition of foreign intelligence information, although, of course, how it is used may be affected by minimization procedures . . . . And no information acquired pursuant to this bill could be used for other than lawful purposes . . . . *Obviously, use of "foreign intelligence information" as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism.* The bill, therefore, explicitly recognizes that information which is evidence of crimes involving [these activities] can be sought, retained, and used pursuant to this bill.

Id. (emphasis added). The Senate Report is on all fours:

> U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of foreign powers. *Intelligence and criminal law enforcement tend to merge in this area*. . . . [S]urveillances conducted under [FISA] 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. 95-701 (hereinafter "S. REP.") at 10-11 (1978) (emphasis added).

Congress was concerned about the government's use of FISA surveillance to obtain information not truly intertwined with the government's efforts to protect against threats from foreign powers. Accordingly, the certification of purpose under section 1804(a)(7)(B) served to

> prevent the practice of targeting, for example, a foreign power for electronic surveillance when the true purpose of the surveillance is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that the sole purpose of such surveillance is to secure "foreign intelligence information," as defined, and not to obtain some other type of information.

H. REP. at 76; see also S. REP. at 51. But Congress did not impose any restrictions on the government's use of the foreign intelligence information to prosecute agents of foreign powers for foreign intelligence crimes. Admittedly, the House, at least in one statement, noted 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 United States persons must be necessary to important national concerns." H. REP. at 36. That, however, was an observation, not a proscription. And the House as well as the Senate made clear that prosecution is one way to combat foreign intelligence crimes. See *id.*; S. REP. at 10- 11.

The origin of what the government refers to as the false dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is not appears to have been a Fourth Circuit case decided in 1980. *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). That case, however, involved an electronic surveillance carried out prior to the passage of FISA and predicated on the President's executive power. In approving the district court's exclusion of evidence obtained through a warrantless surveillance subsequent to the point in time when the government's investigation became "primarily" driven by law enforcement objectives, the court held that the Executive Branch should be excused from securing a warrant only when "the object of the search or the surveillance is a foreign power, its agents or collaborators," and "the surveillance is conducted 'primarily' for foreign intelligence reasons." *Id.* at 915. Targets must "receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution." *Id.* at 916. Although the *Truong* court acknowledged that "almost all foreign intelligence investigations are in part criminal" ones, it rejected the government's assertion that "if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment." *Id.* at 915.

Several circuits have followed *Truong* in applying similar versions of the "primary purpose" test, despite the fact that *Truong* was not a FISA decision. (It was an interpretation of the Constitution, in the context of measuring the boundaries of the President's inherent executive authority, and we discuss *Truong's* constitutional analysis at length in Section III of this opinion.) In one of the first major challenges to a FISA search, *United States v. Megahey*, 553 F. Supp. 1180 (E.D.N.Y. 1982), aff'd sub nom. *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984), the district court acknowledged that while Congress clearly viewed arrest and prosecution as

one of the possible outcomes of a FISA investigation, surveillance under FISA would nevertheless be "appropriate only if foreign intelligence surveillance is the Government's primary purpose." *Id.* at 1189-90. Six months earlier, another judge in the same district had held that the *Truong* analysis did not govern FISA cases, since a FISA order was a warrant that met Fourth Amendment standards. *United States v. Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982). *Falvey*, however, was apparently not appealed and *Megahey* was. The Second Circuit, without reference to *Falvey*, and importantly in the context of affirming the conviction, approved *Megahey's* finding that the surveillance was not "directed towards criminal investigation or the institution of a criminal prosecution." *Duggan*, 743 F.2d at 78 (quoting *Megahey*, 553 F. Supp. at 1190). Implicitly then, the Second Circuit endorsed the *Megahey* dichotomy. Two other circuits, the Fourth and the Eleventh, have similarly approved district court findings that a surveillance was primarily for foreign intelligence purposes without any discussion–or need to discuss–the validity of the dichotomy. See *United States v. Pelton*, 835 F.2d 1067, 1075-76 (4th Cir. 1987), cert. denied, 486 U.S. 1010 (1988); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987), cert. denied, 485 U.S. 937 (1988).

Then, the First Circuit, seeing *Duggan* as following *Truong*, explicitly interpreted FISA's purpose wording in section 1804(a)(7)(B) to mean that "[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance." *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (citations omitted), cert. denied, 506 U.S. 816 (1992). Notably, however, the Ninth Circuit has refused

> to draw too fine a distinction between criminal and intelligence investigations. "International terrorism," by definition, requires the investigation of activities that constitute crimes.

> That the government may later choose to prosecute is irrelevant. . . . FISA is meant to take into account "[t]he differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities . . . ."

United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988) (citations omitted).

Neither *Duggan* nor *Johnson* tied the "primary purpose" test to actual statutory language. In Duggan the court stated that "[t]he requirement that foreign intelligence information be the primary objective of the surveillance is plain," and the district court was correct in "finding that 'the purpose of the surveillance in this case, both initially and throughout, was to secure foreign intelligence information and was not, as [the] defendants assert, directed towards criminal investigation or the institution of a criminal prosecution.'" Duggan, 743 F.2d at 77-78 (quoting *Megahey*, 553 F. Supp. at 1190).[26] Yet the court never explained why it apparently read foreign intelligence information to exclude evidence of crimes–endorsing the district court's implied dichotomy–when the statute's definitions of foreign intelligence and foreign agent are actually cast in terms of criminal conduct. (It will be recalled that the type of foreign intelligence with which we are concerned is really counterintelligence, see supra note 9.) And Johnson did not even focus on the phrase "foreign intelligence information" in its interpretation of the "purpose" language in section 1804(a)(7)(B). *Johnson*, 952 F.2d at 572.

---

[26] Interestingly, the court noted that the FISA judge "is not to second guess the Executive Branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77.

It is almost as if *Duggan*, and particularly *Johnson*, assume that the government seeks foreign intelligence information (counterintelligence) for its own sake–to expand its pool of knowledge–because there is no discussion of how the government would use that information outside criminal prosecutions. That is not to say that the government could have no other use for that information. The government's overriding concern is to stop or frustrate the agent's or the foreign power's activity by any means, but if one considers the actual ways in which the government would foil espionage or terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category. 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 issue with which we are confronted.

In sum, we think that the FISA as passed by Congress in 1978 clearly 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. In order to understand the FISA court's decision, however, it is necessary to trace developments and understandings within the Justice Department post-*Truong* as well as after the passage of the Patriot Act. As we have noted, some time in the 1980s–the exact moment is shrouded in historical mist–the Department applied the *Truong* analysis to an interpretation of the FISA statute. What is clear is that in 1995 the Attorney General adopted "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations."

Apparently to avoid running afoul of the primary purpose test used by some courts, the 1995 Procedures limited

contacts between the FBI and the Criminal Division in cases where FISA surveillance or searches were being conducted by the FBI for foreign intelligence (FI) or foreign counterintelligence (FCI) purposes.[27] The procedures state that "the FBI and Criminal Division should ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either the fact or the appearance of the Criminal Division's *directing* or *controlling* the FI or FCI investigation toward law enforcement objectives." 1995 Procedures at 2, ¶ 6 (emphasis added). Although these procedures provided for significant information sharing and coordination between criminal and FI or FCI investigations, based at least in part on the "directing or controlling" language, they eventually came to be narrowly interpreted within the Department of Justice, and most particularly by OIPR, as requiring OIPR to act as a "wall" to prevent the FBI intelligence officials from communicating with the Criminal Division regarding ongoing FI or FCI investigations. See *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* (AGRT Report), Chapter 20 at 721-34 (May 2000). Thus, the focus became the nature of the underlying investigation, rather than the general purpose of the surveillance. Once prosecution of the target was being considered, the procedures, as interpreted by OIPR in light of the case law, prevented the Criminal Division from providing any meaningful advice to the FBI. *Id.*

The Department's attitude changed somewhat after the May 2000 report by the Attorney General and a July 2001 Report by the General Accounting Office both concluded that the Department's concern over how the FISA court or other

---

[27] We certainly understand the 1995 Justice Department's effort to avoid difficulty with the FISA court, or other courts; and we have no basis to criticize any organization of the Justice Department that an Attorney General desires.

federal courts might interpret the primary purpose test has inhibited necessary coordination between intelligence and law enforcement officials. See *id.* at 721-34;[28] General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited* (July 2001) (GAO-01-780) (GAO Report) at 3. The AGRT Report also concluded, based on the text of FISA and its legislative history, that not only should the purpose of the investigation not be inquired into by the courts, but also that Congress affirmatively anticipated that the underlying investigation might well have a criminal as well as foreign counterintelligence objective. AGRT Report at 737. In response to the AGRT Report, the Attorney General, in January 2000, issued additional, interim procedures designed to address coordination problems identified in that report. In August 2001, the Deputy Attorney General issued a memorandum clarifying Department of Justice policy governing intelligence sharing and establishing additional requirements. (These actions, however, did not replace the 1995 Procedures.) But it does not appear that the Department thought of these internal procedures as "minimization procedures" required under FISA.[29] Nevertheless, the FISA court was aware that the procedures

[28] According to the Report, within the Department the primary proponent of procedures that cordoned off criminal investigators and prosecutors from those officers with counterintelligence responsibilities was the deputy counsel of OIPR. See AGRT Report at 714 & n.949. He was subsequently transferred from that position and made a senior counsel. He left the Department and became the Legal Advisor to the FISA court.

[29] There are other detailed, classified procedures governing the acquisition, retention, and dissemination of foreign intelligence and non-foreign intelligence information that have been submitted to and approved by the FISA court as "minimization procedures." Those classified minimization procedures are not at issue here.

were being followed by the Department and apparently adopted elements of them in certain cases.

The Patriot Act and the FISA Court's Decision

The passage of the Patriot Act altered and to some degree muddied the landscape. In October 2001, Congress amended FISA to change "the purpose" language in 1804(a)(7)(B) to "a significant purpose." It also added a provision allowing "Federal officers who conduct electronic surveillance to acquire foreign intelligence information" to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents. 50 U.S.C. § 1806(k)(1). And such coordination "shall not preclude" the government's certification that a significant purpose of the surveillance is to obtain foreign intelligence information, or the issuance of an order authorizing the surveillance. *Id.* § 1806(k)(2). Although the Patriot Act amendments to FISA expressly sanctioned consultation and coordination between intelligence and law enforcement officials, in response to the first applications filed by OIPR under those amendments, in November 2001, the FISA court for the first time adopted the 1995 Procedures, as augmented by the January 2000 and August 2001 Procedures, as "minimization procedures" to apply in all cases before the court.[30]

The Attorney General interpreted the Patriot Act quite differently. On March 6, 2002, the Attorney General approved new "Intelligence Sharing Procedures" to

[30] In particular, the court adopted Part A of the 1995 Procedures, which covers "Contacts During an FI or FCI Investigation in which FISA Surveillance or Searches are being Conducted." The remainder of the 1995 Procedures addresses contacts in cases where FISA is not at issue.

implement the Act's amendments to FISA. The 2002 Procedures supersede prior procedures and were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials. They eliminated the "direction and control" test and allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance." On March 7, 2002, the government filed a motion with the FISA court, noting that the Department of Justice had adopted the 2002 Procedures and proposing to follow those procedures in all matters before the court. The government also asked the FISA court to vacate its orders adopting the prior procedures as minimization procedures in all cases and imposing special "wall" procedures in certain cases.

Unpersuaded by the Attorney General's interpretation of the Patriot Act, the court ordered that the 2002 Procedures be adopted, *with modifications*, as minimization procedures to apply in all cases. The court emphasized that the definition of minimization procedures had not been amended by the Patriot Act, and reasoned that the 2002 Procedures "cannot be used by the government to amend the Act in ways Congress has not." The court explained:

> Given our experience in FISA surveillances and searches, we find that these provisions in sections II.B and III [of the 2002 Procedures], particularly those which authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are 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*" . . . as mandated in §1801(h) and § 1821(4).

May 17, 2001 Opinion at 22 (emphasis added by the FISA court).[31] The FISA court also adopted a new rule of court procedure, Rule 11, which provides that "[a]ll 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."

Undeterred, the government submitted the application at issue in this appeal on July 19, 2002, and expressly proposed using the 2002 Procedures *without modification*. In an order issued the same day, the FISA judge hearing the application granted an order for surveillance of the target but modified the 2002 Procedures consistent with the court's May 17, 2002 en banc order. It is the July 19, 2002 order that the government appeals, along with an October 17, 2002 order granting, with the same modifications as the July 19 order, the government's application for renewal of the surveillance in this case. Because those orders incorporate the May 17, 2002 order and opinion by reference, however, that order and opinion are before us as well.

* * * *

[31] In describing its experience with FISA searches and surveillance, the FISA court's opinion makes reference to certain applications each of which contained an FBI agent's affidavit that was inaccurate, particularly with respect to assertions regarding the information shared with criminal investigators and prosecutors. Although we do not approve any misrepresentations that may have taken place, our understanding is that those affidavits were submitted during 1997 through early 2001, and therefore any inaccuracies may have been caused in part by the confusion within the Department of Justice over implementation of the 1995 Procedures, as augmented in January 2000. In any event, while the issue of the candor of the FBI agent(s) involved properly remains under investigation by the Department of Justice's Office of Professional Responsibility, the issue whether the wall between the FBI and the Criminal Division required by the FISA court has been maintained is moot in light of this court's opinion.

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.

Under section 1805 of FISA, "the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that . . . the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title." 50 U.S.C. § 1805(a)(4). The statute defines minimization procedures in pertinent part as:

> (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.

Section 1801(h) also contains the following proviso:

> (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. . . .

Id. § 1801(h).

As is evident from the face of section 1801(h), minimization procedures are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. If the data is not foreign intelligence information as defined by the statute, the procedures are to ensure that the government does not use the information to identify the target or third party, unless such identification is necessary to properly understand or assess the foreign intelligence information that is collected. *Id.* § 1801(h)(2). By minimizing *acquisition*, Congress envisioned that, for example, "where a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party" to the communication. H. REP. at 55-56. By minimizing *retention*, Congress intended that "information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed where feasible." H. REP. at 56. Furthermore, "[e]ven with respect to information needed for an approved purpose, *dissemination* should be restricted to those officials with a need for such information." *Id.* (emphasis added).

The minimization procedures allow, however, the retention and dissemination of nonforeign intelligence

information which is evidence of *ordinary crimes* for preventative or prosecutorial purposes. See 50 U.S.C. § 1801(h)(3). Therefore, if through interceptions or searches, evidence of "a serious crime totally unrelated to intelligence matters" is incidentally acquired, the evidence is "*not* . . . required to be destroyed." H. REP. at 62 (emphasis added). As we have explained, under the 1978 Act, "evidence of certain crimes like espionage would itself constitute 'foreign intelligence information,' as defined, because it is necessary to protect against clandestine intelligence activities by foreign powers or their agents." H. REP. at 62; see also *id.* at 49. In light of these purposes of the minimization procedures, there is simply no basis for the FISA court's reliance on section 1801(h) 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.

The FISA court's decision and order not only misinterpreted and misapplied minimization procedures it was entitled to impose, but as the government argues persuasively, the FISA court 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). Subject to statutes dealing with the organization of the Justice Department, however, the Attorney General has the responsibility to determine how to deploy personnel resources. As the Supreme Court said in *Morrison v. Olson* in cautioning the Special Division of the D.C. Circuit to avoid unauthorized administrative guidance of Independent Counsel, "[t]he gradual expansion of the authority of the Special Division might in another context be a bureaucratic success story, but

it would be one that would have serious constitutional ramifications." 487 U.S. 654, 684 (1988).[32]

* * * *

We also think the refusal by the FISA court to consider the legal significance of the Patriot Act's crucial amendments was error. The government, in order to avoid the requirement of meeting the "primary purpose" test, specifically sought an amendment to section 1804(a)(7)(B) which had required a certification "that the purpose of the surveillance is to obtain foreign intelligence information" so as to delete the article "the" before "purpose" and replace it with "a." The government made perfectly clear to Congress why it sought the legislative change. Congress, although accepting the government's explanation for the need for the amendment, adopted language which it perceived as not giving the government quite the degree of modification it wanted. Accordingly, section 1804(a)(7)(B)'s wording became "that *a significant* purpose of the surveillance is to obtain foreign intelligence information" (emphasis added). There is simply no question, however, that Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution.

No committee reports accompanied the Patriot Act but the floor statements make congressional intent quite apparent. The Senate Judiciary Committee Chairman Senator Leahy acknowledged that "[p]rotection against these foreign-

---

[32] In light of *Morrison v. Olson* and *Mistretta v. United States*, 488 U.S. 361 (1989), we do not think there is much left to an argument made by an opponent of FISA in 1978 that the statutory responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process. See *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, 9745, 7308, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess. 221 (1978) (statement of Laurence H. Silberman).

based threats by any lawful means is within the scope of the definition of 'foreign intelligence information,' and the use of FISA to gather evidence for the enforcement of these laws was contemplated in the enactment of FISA." 147 Cong. Rec. S11004 (Oct. 25, 2001). "This bill . . . break[s] down traditional barriers between law enforcement and foreign intelligence. This is not done just to combat international terrorism, but for any criminal investigation that overlaps a broad definition of 'foreign intelligence.'" 147 Cong. Rec. S10992 (Oct. 25, 2001) (statement of Sen. Leahy). And Senator Feinstein, a "strong support[er]," was also explicit. The ultimate objective was to make it

> easier to collect foreign intelligence information under the Foreign Intelligence Surveillance Act, FISA. Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence.
>
> But in today's world things are not so simple. In many cases, surveillance will have two key goals– the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary" purpose of the investigation can be difficult, and will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.
>
> Rather than forcing law enforcement to decide which purpose is primary–law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA.

> The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution. Many of the individuals involved in supporting the September 11 attacks may well fall into both of these categories.

147 Cong. Rec. S10591 (Oct. 11, 2001).

To be sure, some Senate Judiciary Committee members including the Chairman were concerned that the amendment might grant too much authority to the Justice Department–and the FISA court. Senator Leahy indicated that the change to significant purpose was "very problematic" since it would "make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution." 147 Cong. Rec. S10593 (Oct. 11, 2001). Therefore he suggested that "it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of 'foreign intelligence information.'" 147 Cong. Rec. S11004 (Oct. 25, 2001) (emphasis added). But the only dissenting vote against the act was cast by Senator Feingold. *For the Record: Senate Votes*, 59 CONG. QUARTERLY (WKLY.) 39, Oct. 13, 2001, at 2425. Senator Feingold recognized that the change to "significant purpose" meant that the government could obtain a FISA warrant "even if the primary purpose is a criminal investigation," and was concerned that this development would not respect the protections of the Fourth Amendment. 147 Cong. Rec. S11021 (Oct. 25, 2001).

In sum, there can be no doubt as to Congress' intent in amending section 1804(a)(7)(B). Indeed, it went further to

emphasize its purpose in breaking down barriers between criminal law enforcement and intelligence (or counterintelligence) gathering by adding section 1806(k):

> (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 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; or
>
> (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 [1804](a)(7)(B) of this title or the entry of an order under section [1805] of this title.

The FISA court noted this amendment but thought that Congress' approval of consultations was not equivalent to authorizing law enforcement officers to give advice to officers who were conducting electronic surveillance nor did it sanction law enforcement officers "directing or controlling" surveillances. However, dictionary definitions of "consult" include giving advice. See, e.g., OXFORD

ENGLISH DICTIONARY ONLINE (2d ed. 1989). Beyond that, when 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 be taking the lead.

Neither *amicus* brief defends the reasoning of the FISA court. NACDL's brief makes no attempt to interpret FISA or the Patriot Act amendments but rather argues the primary purpose test is constitutionally compelled. The ACLU relies on Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522, to interpret FISA, passed 10 years later. That technique, to put it gently, is hardly an orthodox method of statutory interpretation. FISA was passed to deal specifically with the subject of foreign intelligence surveillance. The ACLU does argue that Congress' intent to preclude law enforcement officials initiating or controlling foreign intelligence investigations is revealed by FISA's exclusion of the Attorney General–a law enforcement official–from the officers who can certify the foreign intelligence purpose of an application under section 1804. The difficulty with that argument is that the Attorney General supervises the Director of the FBI who is both a law enforcement and counterintelligence officer. The Attorney General or the Deputy Attorney General, moreover, must approve all applications no matter who certifies that the information sought is foreign intelligence information. 50 U.S.C. § 1804(a).[33]

The ACLU insists that the significant purpose amendment only "clarified" the law permitting FISA surveillance orders "even if foreign intelligence is not its *exclusive* purpose" (emphasis added). In support of this rather

[33] Furthermore, the Attorney General of Deputy Attorney General must approve the use in a criminal proceeding of information acquired pursuant to FISA. 50 U.S.C. § 1806(b).

strained interpretation, which ignores the legislative history of the Patriot Act, the ACLU relies on a *September 10, 2002* hearing of the Judiciary Committee (the day after the government's oral presentation to this court) at which certain senators made statements–somewhat at odds with their floor statements prior to the passage of the Patriot Act–as to what they had intended the year before. The D.C. Circuit has described such post-enactment legislative statements as "legislative future" rather than legislative history, not entitled to authoritative weight. See *General Instrument Corp. v. FCC*, 213 F.3d 724, 733 (D.C. Cir. 2000).

Accordingly, the Patriot Act amendments clearly disapprove the primary purpose test. And as a matter of straightforward logic, if a FISA application can be granted even if "foreign intelligence" is only a significant–not a primary–purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime. We therefore believe the Patriot Act amply supports the government's alternative argument but, paradoxically, the Patriot Act would seem to conflict with the government's first argument because by using the term "significant purpose," the Act now implies that another purpose is to be distinguished from a foreign intelligence purpose.

The government heroically tries to give the amended section 1804(a)(7)(B) a wholly benign interpretation. It concedes that "the 'significant purpose' amendment recognizes the *existence* of the dichotomy between foreign intelligence and law enforcement," but it contends that "it cannot be said to recognize (or approve) its *legitimacy*." Supp. Br. of U.S. at 25 (emphasis in original). We are not persuaded. The very letter the Justice Department sent to the Judiciary Committee in 2001 defending the constitutionality of the significant purpose language implicitly accepted as legitimate the dichotomy in FISA that the government now claims (and we agree) was false. It said, "it is also clear that

while FISA states that 'the' purpose of a search is for foreign surveillance, that need not be the only purpose. Rather, law enforcement considerations can be taken into account, so long as the surveillance also has a legitimate foreign intelligence purpose." The senatorial statements explaining the significant purpose amendments which we described above are all based on the same understanding of FISA which the Justice Department accepted–at least until this appeal. In short, even though we agree that the original FISA did not contemplate the "false dichotomy," the Patriot Act actually did–which makes it no longer false. The addition of the word "significant" to section 1804(a)(7)(B) 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), as we discussed above, 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.

That leaves us with something of an analytic conundrum. On the one hand, Congress did not amend the definition of foreign intelligence information which, we have explained, includes evidence of foreign intelligence crimes. On the other hand, Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test. Nevertheless, it is our task to do our best to read the statute to honor congressional intent. The better reading, it seems to us, excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution. We therefore reject the government's argument to the contrary. Yet this may not make much practical difference. Because, as the government points out, when it commences an electronic surveillance of a foreign agent,

typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.

The important point is–and here we agree with the government–the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. 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 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.

The government claims that even prosecutions of *non*-foreign intelligence crimes are consistent with a purpose of gaining foreign intelligence information so long as the government's objective is to stop espionage or terrorism by putting an agent of a foreign power in prison. That interpretation transgresses the original FISA. It will be recalled that Congress intended section 1804(a)(7)(B) to prevent the government from targeting a foreign agent when its "true purpose" was to gain non-foreign intelligence information–such as evidence of ordinary crimes or scandals. See supra at p.14. (If the government inadvertently came upon evidence of ordinary crimes, FISA provided for the transmission of that evidence to the proper authority. 50 U.S.C. § 1801(h)(3).) It can be argued, however, that by providing that an application is to be granted if the

government has only a "significant purpose" of gaining foreign intelligence information, the Patriot Act allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime. Yet we think that would be an anomalous reading of the amendment. For we see not the slightest indication that Congress meant to give that power to the Executive Branch. Accordingly, the manifestation of such a purpose, it seems to us, would continue to disqualify an application. That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself. But the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

One final point; we think the government's purpose as set forth in a section 1804(a)(7)(B) certification is 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. 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. This is not a standard whose application the FISA court legitimately reviews by seeking to inquire into which Justice Department officials were instigators of an investigation. All Justice Department officers–including those in the FBI–are under the control of the Attorney General. If he wishes a particular investigation to be run by an officer of any division, that is his prerogative. There is nothing in FISA or the Patriot Act that suggests otherwise. 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.

III.

Having determined that FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is *not* criminal prosecution, we are obliged to consider whether the statute as amended is consistent with the Fourth Amendment. The Fourth Amendment provides:

> 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.

Although the FISA court did not explicitly rely on the Fourth Amendment, it at least suggested that this provision was the animating principle driving its statutory analysis. The FISA court indicated that its disapproval of the Attorney General's 2002 Procedures was based on the need to safeguard the "privacy of Americans in these highly intrusive surveillances and searches," which implies the invocation of the Fourth Amendment. The government, recognizing the Fourth Amendment's shadow effect on the FISA court's opinion, has affirmatively argued that FISA is constitutional. And some of the very senators who fashioned the Patriot Act amendments expected that the federal courts, including presumably the FISA court, would carefully consider that question. Senator Leahy believed that "[n]o matter what

statutory change is made . . . the court may impose a constitutional requirement of 'primary purpose' based on the appellate court decisions upholding FISA against constitutional challenges over the past 20 years." 147 Cong. Rec. S11003 (Oct. 25, 2001). Senator Edwards stated that "the FISA court will still need to be careful to enter FISA orders only when the requirements of the Constitution as well as the statute are satisfied." 147 Cong. Rec. S10589 (Oct. 11, 2001).

We are, therefore, grateful to the ACLU and NACDL for their briefs that vigorously contest the government's argument. Both NACDL (which, as we have noted above, presents only the argument that the statute as amended is unconstitutional) and the ACLU rely on two propositions. The first is not actually argued; it is really an assumption–that a FISA order does not qualify as a warrant within the meaning of the Fourth Amendment. The second is that any government surveillance whose *primary purpose* is criminal prosecution *of whatever kind* is *per se* unreasonable if not based on a warrant.

The FISA court expressed concern that unless FISA were "construed" in the fashion that it did, the government could use a FISA order as an improper substitute for an ordinary criminal warrant under Title III. That concern seems to suggest that the FISA court thought Title III procedures are constitutionally mandated if the government has a prosecutorial objective regarding an agent of a foreign power. But in *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)–in which the Supreme Court explicitly declined to consider foreign intelligence surveillance–the Court indicated that, even with respect to domestic national security intelligence gathering for prosecutorial purposes where a warrant was mandated, Title III procedures were not constitutionally required: "[W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case.

We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'" Nevertheless, in asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns.

Comparison of FISA Procedures with Title III

It is important to note that while many of FISA's requirements for a surveillance order differ from those in Title III, few of those differences have any constitutional relevance. In the context of ordinary crime, beyond requiring searches and seizures to be reasonable, the Supreme Court has interpreted the warrant clause of the Fourth Amendment to require three elements:

> First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe that "the evidence sought will aid in a particular apprehension or conviction" for a particular offense. Finally, "warrants must particularly describe the 'things to be seized,'" as well as the place to be searched.

Dalia v. United States, 441 U.S. 238, 255 (1979) (citations omitted).

With limited exceptions not at issue here, both Title III and FISA require prior judicial scrutiny of an application for an order authorizing electronic surveillance. 50 U.S.C. § 1805; 18 U.S.C. § 2518. And there is no dispute that a FISA judge satisfies the Fourth Amendment's requirement of a "neutral and detached magistrate." See *United States v.*

Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987) (FISA court is a "detached and neutral body"); see also *Keith*, 407 U.S. at 323 (in domestic national security context, suggesting that a request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court).

The statutes differ to some extent in their probable cause showings. Title III allows a court to enter an ex parte order authorizing electronic surveillance if it determines on the basis of the facts submitted in the government's application that "there is probable cause for belief that an individual is committing, has committed, or is about to commit" a specified predicate offense. 18 U.S.C. § 2518(3)(a). FISA by contrast requires a showing of probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3). We have noted, however, that where a U.S. person is involved, an "agent of a foreign power" is defined in terms of criminal activity.[34] Admittedly, the definition of one category of U.S.- person agents of foreign powers–that is, persons engaged in espionage and clandestine intelligence activities for a foreign power–does not necessarily require a showing of an imminent violation of criminal law. See 50 U.S.C. § 1801(b)(2)(A) (defining such activities as those which "involve" or "*may* involve" a violation of criminal statutes of the United States). Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases. See H. REP. at 39-40, 79. And with good reason–these activities present the type of threats contemplated by the Supreme Court in *Keith* when it recognized that the focus of security surveillance "may be less precise than that directed against more conventional types of crime" even in the area of *domestic* threats to

[34] The term "foreign power," which is not directly at issue in this case, is not defined solely in terms of criminal activity. For example, although the term includes a group engaged in international terrorism, which would involve criminal activity, it also includes any foreign government. 50 U.S.C. § 1801(a)(1).

national security. Keith, 407 U.S. *at 322. Congress was aware of Keith's reasoning, and recognized that it applies* a fortiori to foreign threats. See S. REP. at 15. As the House Report notes with respect to clandestine intelligence activities:

> The term "may involve" not only requires less information regarding the crime involved, but also permits electronic surveillance at some point prior to the time when a crime sought to be prevented, as for example, the transfer of classified documents, actually occurs.

H. REP. at 40. Congress allowed this lesser showing for clandestine intelligence activities–but not, notably, for other activities, including terrorism–because it was fully aware that such foreign intelligence crimes may be particularly difficult to detect.[35] At the same time, however, it provided another safeguard not present in Title III–that is, the requirement that there be probable cause to believe the target is acting "for or on behalf of a foreign power." Under the definition of "agent of a foreign power" FISA surveillance could not be authorized

> against an American reporter merely because he gathers information for publication in a newspaper, even if the information was classified by the Government. Nor would it be authorized against a Government employee or former employee who reveals secrets to a reporter or in a book for the purpose of informing the American people. This definition would not authorize surveillance of ethnic Americans who lawfully

[35] For example, a federal agent may witness a "meet" or "drop" where information is being passed but be unable to determine precisely what information is being transmitted and therefore be unable to show that a crime is involved or what specific crime is being committed. See H. REP. at 39-40; see also S. REP. at 23.

> gather political information and perhaps even lawfully share it with the foreign government of their national origin. It obviously would not apply to lawful activities to lobby, influence, or inform Members of Congress or the administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information preparatory to such lawful activities.

H. REP. at 40. Similarly, FISA surveillance would not be authorized against a target engaged in purely domestic terrorism because the government would not be able to show that the target is acting for or on behalf of a foreign power. As should be clear from the foregoing, FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security.

Turning then to the first of the particularity requirements, while Title III requires probable cause to believe that particular communications concerning the specified crime will be obtained through the interception, 18 U.S.C. § 2518(3)(b), FISA instead requires an official to designate the type of foreign intelligence information being sought, and to certify that the information sought is foreign intelligence information. When the target is a U.S. person, the FISA judge reviews the certification for clear error, but this "standard of review is not, of course, comparable to a probable cause finding by the judge." H. REP. at 80. Nevertheless, FISA provides additional protections to ensure that only pertinent information is sought. The certification must be made by a national security officer–typically the FBI Director–and must be approved by the Attorney General or the Attorney General's Deputy. Congress recognized that this certification would "assure[] written accountability within the Executive Branch" and provide "an internal check on Executive Branch arbitrariness." H. REP. at 80. In addition, the court may require the government to submit any further

information it deems necessary to determine whether or not the certification is clearly erroneous. See 50 U.S.C. § 1804(d).

With respect to the second element of particularity, although Title III generally 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), 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. 50 U.S.C. § 1805(a)(3)(B). In cases where the targeted facilities are not leased to, listed in the name of, or used by the individual committing the crime, Title III requires the government to show a nexus between the facilities and communications regarding the criminal offense. The government does not have to show, however, anything about the target of the surveillance; it is enough that "*an individual*"–not necessarily the target–is committing a crime. 18 U.S.C. §§ 2518(3)(a), (d); see *United States v. Kahn*, 415 U.S. 143, 157 (1974) ("when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a wire interception order may, nevertheless, properly issue under [Title III]"). On the other hand, FISA requires probable cause to believe the target is an agent of a foreign power (that is, the individual committing a foreign intelligence crime) who uses or is about to use the targeted facility. Simply put, FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications. See H. REP. at 73 ("the target of a surveillance is the individual or entity or about whom or from whom information is sought").

There are other elements of Title III that at least some circuits have determined are constitutionally significant–that

is, necessity, duration of surveillance, and minimization. See, e.g., *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994). Both statutes have a "necessity" provision, which requires the court to find that the information sought is not available through normal investigative procedures. See 18 U.S.C. § 2518(3)(c); 50 U.S.C. §§ 1804(a)(7)(E)(ii), 1805(a)(5). Although the court's clearly erroneous review under FISA is more limited than under Title III, this greater deference must be viewed in light of FISA's additional requirement that the certification of necessity come from an upper level Executive Branch official. The statutes also have duration provisions; Title III orders may last up to 30 days, 18 U.S.C. § 2518(5), while FISA orders may last up to 90 days for U.S. persons. 50 U.S.C. § 1805(e)(1). This difference is 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. Moreover, 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. And where Title III requires minimization of what is acquired,[36] as we have discussed, for U.S. persons, FISA requires minimization of what is acquired, retained, and disseminated. The FISA court notes, however, that 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 reasonableness of this approach depends on the facts and circumstances of each case. *Scott v. United States*, 436 U.S. 128, 140-43 (1978) (acquisition of virtually all conversations was reasonable under the circumstances). Less minimization in the acquisition stage may well be justified to the extent the intercepted communications are "ambiguous in nature or

[36] Title III requires agents to conduct surveillance "in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." 18 U.S.C. § 2518(5).

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." *Id.* at 140. 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. [*[4-5 lines deleted]*]

Amici particularly focus on the differences between the two statutes concerning notice.[37] Title III requires notice to the target (and, within the discretion of the judge, to other persons whose communications were intercepted) once the surveillance order expires. 18 U.S.C. § 2518(8)(d). FISA does not require notice to a person whose communications were intercepted unless the government "intends to enter into evidence or otherwise use or disclose" such communications in a trial or other enumerated official proceedings. 50 U.S.C. § 1806(c). As the government points out, however, to the extent evidence obtained through a FISA surveillance order is used in a criminal proceeding, notice to the defendant is required. Of course, where such evidence is not ultimately going to be used for law enforcement, Congress observed

[37] *Amici* also emphasize that Title III generally entitles a defendant to obtain the surveillance application and order to challenge to the legality of the surveillance, 18 U.S.C. § 2518(9), while FISA does not normally allow a defendant to obtain the same if the Attorney General states that disclosure or an adversary hearing would harm national security, 50 U.S.C. § 1806(f). Under such circumstances, the judge conducts an in camera and ex parte review to determine whether the electronic surveillance was lawful, whether disclosure or discovery is necessary, and whether to grant a motion to suppress. Id. §§ 1806(f), (g). Clearly, the decision whether to allow a defendant to obtain FISA materials is made by a district judge on a case by case basis, and the issue whether such a decision protects a defendant's constitutional rights in any given case is not before us.

that "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement." S. REP. at 12.

Based on the foregoing, it should be evident that while Title III contains some protections that are not in FISA, in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections.[38] Still, to the extent 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. The government itself does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense. See *Cavanagh*, 807 F.2d at 790 (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); see also Pelton, 835 F.2d at 1075 (joining *Cavanagh* in holding that FISA procedures meet constitutional requirements); *Falvey*, 540 F. Supp. at 1314 (holding that unlike in *Truong*, a congressionally crafted warrant that met Fourth Amendment standards was obtained authorizing the surveillance). We do not decide the issue but note that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment.

Did Truong Articulate the Appropriate Constitutional Standard?

[38] In addition to the protections already discussed, FISA has more extensive reporting requirements than Title III, compare 18 U.S.C. § 2519(2) with 50 U.S.C. § 1808(a)(1), and is subject to close and continuing oversight by Congress as a check against Executive Branch abuses. S. REP. at 11-12. Also, the Patriot Act contains sunset provisions, see Section 224(a) of Patriot Act, Pub. L. 107-56, 115 Stat. 272 (Oct. 26, 2001), thus allowing Congress to revisit the Act's amendments to FISA.

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. Cf. *Keith*, 407 U.S. at 322-23 (in domestic security context, holding that standards different from those in Title III "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the government for intelligence information and the protected rights of our citizens"). To answer that question–whether the Patriot Act's disavowal of the primary purpose test is constitutional–besides comparing the FISA procedures with Title III, it is necessary to consider carefully the underlying rationale of the primary purpose test.

It will be recalled that the case that set forth the primary purpose test as *constitutionally required* was *Truong*. The Fourth Circuit thought that *Keith's* balancing standard implied the adoption of the primary purpose test. We reiterate that *Truong* dealt with a pre-FISA surveillance based on the President's constitutional responsibility to conduct the foreign affairs of the United States. 629 F.2d at 914. Although *Truong* suggested the line it drew was a constitutional minimum that would apply to a FISA surveillance, see *id.* at 914 n.4, it had no occasion to consider the application of the statute carefully. The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.[39] It was incumbent upon the court, therefore, to determine the boundaries of that constitutional authority in the case before it. We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach

[39] Although the plurality opinion in *Zweibon v. Mitchell*, 516 F.2d 594, 633-51 (D.C. Cir. 1975) (en banc), cert. denied, 425 U.S. 944 (1976), suggested the contrary in dicta, it did not decide the issue.

on the President's constitutional power. The question before us is the reverse, 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.

The district court in the *Truong* case had excluded evidence obtained from electronic surveillance after the government's investigation–the court found–had converted from one conducted for foreign intelligence reasons to one conducted primarily as a criminal investigation. (The defendants were convicted based in part on surveillance evidence gathered before that point.) The district judge had focused on the date that the Criminal Division had taken a central role in the investigation. The court of appeals endorsed that approach stating:

> We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, 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 prosecution.

Id. at 915 (emphasis added).

That analysis, in our view, rested on a false premise and the line the court sought to draw was inherently unstable, unrealistic, and confusing. The false premise was the assertion that once the government moves to criminal prosecution, its "foreign policy concerns" recede. As we have discussed in the first part of the opinion, that is simply not true as it relates to counterintelligence. In that field 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. Indeed, the Fourth Circuit itself, rejecting defendant's arguments that it should adopt a "solely foreign intelligence purpose test," acknowledged that "almost all foreign intelligence investigations are in part criminal investigations." *Id.* (It would have been more accurate to refer to counterintelligence investigations.)

The method the court endorsed for determining when an investigation became primarily criminal was based on the organizational structure of the Justice Department. The court determined an investigation became primarily criminal when the Criminal Division played a lead role. This approach has led, over time, to the quite intrusive organizational and personnel tasking the FISA court adopted. Putting aside the impropriety of an Article III court imposing such organizational strictures (which we have already discussed), the line the Truong court adopted–subsequently referred to as a "wall"–was unstable because it generates dangerous confusion and creates perverse organizational incentives. See, e.g., AGRT Report at 723-26.[40] That is so because counterintelligence brings to bear both classic criminal investigation techniques as well as less focused intelligence gathering. Indeed, effective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task. A standard which punishes such cooperation could well be thought dangerous to national security.[41] Moreover, by

---

[40] We are told that the FBI has even thought it necessary because of FISA court rulings to pass off a criminal investigation to another government department when the FBI was conducting a companion counterintelligence inquiry.

[41] The AGRT Report bears this out: "Unfortunately, the practice of excluding the Criminal Division from FCI investigations was not an isolated event confined to the Wen Ho Lee matter. It has been a way of doing business for OIPR, acquiesced in by the FBI, and inexplicably indulged by the Department of Justice. One FBI supervisor has said that it has only been 'lucky' that a case has not yet been hampered by the rigid

focusing on the subjective motivation of those who initiate investigations, the *Truong* standard, as administered by the FISA court, could be thought to discourage desirable initiatives. (It is also at odds with the Supreme Court's Fourth Amendment jurisprudence which regards the subjective motivation of an officer conducting a search or seizure as irrelevant. See, e.g., *Whren v. United States*, 517 U.S. 806 (1996).)

Recent testimony before the Joint Intelligence Committee amply demonstrates that the *Truong* line is a very difficult one to administer. Indeed, it was suggested that the FISA court requirements based on *Truong* may well have contributed, whether correctly understood or not, to the FBI missing opportunities to anticipate the September 11, 2001 attacks.[42] That is not to say that we should be prepared to jettison Fourth Amendment requirements in the interest of national security. Rather, assuming arguendo that FISA orders are not Fourth Amendment warrants, the question

---

interpretation of the rules governing contacts with the Criminal Division. It may be said that in the Wen Ho Lee investigation, luck ran out." Id. at 708 (citation omitted).

[42] An FBI agent recently testified that efforts to conduct a criminal investigation of two of the alleged hijackers were blocked by senior FBI officials–understandably concerned about prior FISA court criticism–who interpreted that court's decisions as precluding a criminal investigator's role. One agent, frustrated at encountering the "wall," wrote to headquarters: "[S]omeday someone will die–and wall or not–the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the National Security Law Unit will stand behind their decisions then, especially since the biggest threat to us now, [Usama Bin Laden], is getting the most 'protection.'" The agent was told in response that headquarters was frustrated with the issue, but that those were the rules, and the National Security Law Unit does not make them up. *The Malaysia Hijacking and September 11th: Joint Hearing Before the Senate and House Select Intelligence Committees* (Sept. 20, 2002) (written statement of New York special agent of the FBI).

becomes, are the searches constitutionally reasonable. And in judging reasonableness, the instability of the *Truong* line is a relevant consideration.

The Fourth Circuit recognized that the Supreme Court had never considered the constitutionality of warrantless government searches for foreign intelligence reasons, but concluded the analytic framework the Supreme Court adopted in *Keith*–in the case of domestic intelligence surveillance–pointed the way to the line the Fourth Circuit drew. The Court in *Keith* had, indeed, balanced the government's interest against individual privacy interests, which is undoubtedly the key to this issue as well; but we think the *Truong* court misconceived the government's interest and, moreover, did not draw a more appropriate distinction that Keith at least suggested. That is the line drawn in the original FISA statute itself between ordinary crimes and foreign intelligence crimes.

It will be recalled that *Keith* carefully avoided the issue of a warrantless foreign intelligence search: "We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." 407 U.S. at 321- 22.[43] But in indicating that a somewhat more relaxed warrant could suffice in the domestic intelligence situation, the court drew a distinction between the crime involved in that case, which posed a threat to national security, and "ordinary crime." *Id.* at 322. It pointed out that "the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes." *Id.*

The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society

---

[43] The Court in a footnote though, cited authority for the view that warrantless surveillance may be constitutional where foreign powers are involved. *Keith*, 407 U.S. at 322 n.20.

from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity. As we discussed in the first section of this opinion, the criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective;[44] indeed, punishment of a terrorist is often a moot point.

Supreme Court's Special Needs Cases

The distinction between ordinary criminal prosecutions and extraordinary situations underlies the Supreme Court's approval of entirely warrantless and even suspicionless searches that are designed to serve the government's "special needs, beyond the normal need for law enforcement." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotation marks omitted)) (random drug-testing of student athletes).[45] Apprehending drunk drivers and securing the border constitute such unique interests beyond ordinary, general law enforcement. *Id.* at 654 (citing *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990), and *United States v. Martinez- Fuerte*, 428 U.S. 543 (1976)).

A recent case, *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), is relied on by both the government and amici. In

---

[44] To be sure, punishment of a U.S. person's espionage for a foreign power does have a deterrent effect on others similarly situated.

[45] The Court has also allowed searches for certain administrative purposes to be undertaken without particularized suspicion of misconduct. *See, e.g., New York v. Burger*, 482 U.S. 691, 702-04 (1987) (warrantless administrative inspection of premises of closely regulated business); *Camara v. Municipal Court*, 387 U.S. 523, 534-39 (1967) (administrative inspection to ensure compliance with city housing code).

that case, the Court held that a highway check point designed to catch drug dealers did not fit within its special needs exception because the government's "primary purpose" was merely "to uncover evidence of ordinary criminal wrongdoing." *Id.* at 41-42. The Court rejected the government's argument that the "severe and intractable nature of the drug problem" was sufficient justification for such a dragnet seizure lacking any individualized suspicion. *Id.* at 42. *Amici* particularly rely on the Court's statement 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." *Id.*

But by "purpose" the Court makes clear it was referring not to a subjective intent, which is not relevant in ordinary Fourth Amendment probable cause analysis, but rather to a programmatic purpose. The Court distinguished the prior check point cases *Martinez-Fuerte* (involving checkpoints less than 100 miles from the Mexican border) and *Sitz* (checkpoints to detect intoxicated motorists) on the ground that the former involved the government's "longstanding concern for the protection of the integrity of the border," *id.* at 38 (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985)), and the latter was "aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways." *Id.* at 39. The Court emphasized that it was decidedly not drawing a distinction between suspicionless seizures with a "non-law-enforcement primary purpose" and those designed for law enforcement. *Id.* at 44 n.1. Rather, the Court distinguished general crime control programs and those that have another particular purpose, such as protection of citizens against special hazards or protection of our borders. The Court specifically acknowledged that an appropriately tailored road block could be used "to thwart an imminent terrorist attack." *Id.* at 44. The nature of the "emergency,"

which is simply another word for threat, takes the matter out of the realm of ordinary crime control.[46]

Conclusion

FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from "ordinary crime control." After the events of September 11, 2001, though, it is hard to imagine greater emergencies facing Americans than those experienced on that date.

We acknowledge, however, that the constitutional question presented by this case–whether Congress's 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 other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning.

---

[46] *Amici* rely on *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), in arguing that the "special needs" cases acknowledge that the Fourth Amendment is particularly concerned with intrusions whose primary purpose is to gather evidence of crime. In that case, the Court struck down a non-consensual policy of testing obstetrics patients for drug use. The Court stated that "[w]hile the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence *for law enforcement purposes* in order to reach that goal." Id. at 82-83 (emphasis in original; footnotes omitted). In distinguishing the "special needs" cases, the Court noted that "[i]t is especially difficult to argue that the program here was designed simply to save lives," in light of evidence that the sort of program at issue actually discouraged women from seeking prenatal care. Id. at 844 n.23. Thus, *Ferguson* does not involve a situation in which law enforcement is directly connected to the prevention of a special harm.

Although the Court in *City of Indianapolis* cautioned that the threat to society is not dispositive in determining whether a search or seizure is reasonable, it certainly remains a crucial factor. Our case may well involve the most serious threat our country faces. Even 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. We, therefore, believe firmly, applying the balancing test drawn from *Keith*, that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

Accordingly, we reverse the FISA court's orders in this case to the extent they imposed conditions on the grant of the government's applications, vacate the FISA court's Rule 11, and remand with instructions to grant the applications as submitted and proceed henceforth in accordance with this opinion.

Appendix B

FILED
KAREN E. SUTTON, CLERK
MAY 17 2002
U.S. Foreign Intelligence
Surveillance Court

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE ALL MATTERS SUBMITTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

Docket Numbers: Multiple

MEMORANDUM OPINION
(AS CORRECTED AND AMENDED)

I

The Department of Justice has moved this 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. The Court has considered the Government's motion, the revised intelligence sharing procedures, and the supporting memorandum of law as required by the Foreign Intelligence Surveillance Act (hereafter the FISA or the Act) at 50 U.S.C. §1805(a)(4) and §1824(a)(4) (hereafter omitting citations to 50 U.S.C.) to determine whether the proposed minimization procedures submitted with the Government's motion comport

with the definition of minimization procedures under §1801 (h) and §1921(4) of the Act. The Government's motion will be GRANTED, EXCEPT THAT THE PROCEDURES MUST BE MODIFIED IN PART.

The Court's analysis and findings are as follows:

JURISDICTION. Section 1803 of the FISA which established this Court provides that the Court "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 Act." The comparable provision added when the FISA was amended to include physical searches appears in §1822(c) entitled "Jurisdiction of Foreign Intelligence Surveillance Court," and says

> The Foreign Intelligence Surveillance Court shall have jurisdiction to hear applications for and grant orders approving a physical search for the purpose of obtaining foreign intelligence information anywhere in the United States under the procedures set forth in this subchapter. (emphasis added)

Examination of the text of the statute leaves little doubt that the collection of foreign intelligence information is the raison d'etre for the FISA. Starting with its title, foreign intelligence information is the core of the Act.

- foreign intelligence information is defined in §1801(e);
- minimization procedures to protect the privacy rights of Americans, defined in §1801(h), and §1821(4), must be reasonably designed and consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

- section 1802(b) which authorizes the Government to file applications for electronic surveillance with this Court, empowers the judges of this Court to grant orders "approving electronic surveillance of a foreign power or agent of a foreign power for the purpose of obtaining foreign intelligence information." (emphasis added);
- applications for electronic surveillance and physical search must contain a certification from a senior Executive Branch official (normally the FBI Director in U.S. person cases) that "the information sought is foreign intelligence information," that "a significant purpose of the surveillance is to obtain foreign intelligence information," that "such [foreign intelligence] information cannot reasonably be obtained by normal investigative techniques," and "designates the type of foreign intelligence information being sought." (§1804(a)(7)) Comparable requirements apply in applications for physical searches. (§1923(a)(7)).
- Applications for physical searches must contain a statement of the facts and circumstances relied on by the FBI affiant to justify his or her belief that the premises or property to be searched contains foreign intelligence information and a statement of the nature of the foreign intelligence information being sought. (§1823(a)(4)(B) and §1823(a)(6).

Additionally, the two Presidential Executive orders empowering the Attorney General to approve the filing of applications for electronic surveillances and physical searches, and granting the FBI Director and other senior executives the power to make the certifications required under the Act, specify "the purpose of obtaining foreign intelligence information." (emphasis added) E.O. 12139, May 23, 1979, and E.O. 12949, February 9, 1995). Clearly this

Court's jurisdiction is limited to granting orders for electronic surveillances and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the Act.[47]

SCOPE. Our findings regarding minimization apply only to communications of or concerning U.S. persons as defined in §1801(i) of the act: U.S. citizens and permanent resident aliens whether or not they are the named targets in the electronic surveillances and physical searches. Conversely, this opinion does not apply to communications of foreign powers defined in §1801(a), nor to non-U.S. persons.

METHODOLOGY. The analysis and findings in this opinion are based on traditional statutory construction of the FISA's provisions. The question before the Court involves straightforward application of the FISA as it pertains to minimization procedures, and raises no constitutional questions that need be decided. Discretion to evaluate proposed minimization procedures has been vested in the Court by the Congress expressly in the Act, (§1805(a)(4) and §1824(a)(4)). The Court's determinations are grounded in the

[47] On April 17, 2002 the Government filed a supplemental memorandum of law in support of its March 7, 2002 motion. The supplemental memorandum misapprehends the issue that is before the Court. That issue is whether the FISA authorizes electronic surveillances and physical searches primarily for law enforcement purposes so long as the Government also has "a significant" foreign intelligence purpose. The Court is not persuaded by the supplemental memorandum, and its decision is not based an the issue of its jurisdiction but on the interpretation of minimization procedures.

plain language of the FISA, and where applicable, in its legislative history. The statute requires the Court to make the necessary findings, to issue orders "as requested or modified," for electronic surveillances and physical searches, as well as to "assess compliance" with minimization procedures for information concerning U.S. persons. (§1805 and §1824 of the Act).

CONSIDERATION OF THE ISSUE. Prior to May of 1979, when the FISA became operational, it was not uncommon for courts to defer to the expertise of the Executive Branch in matters of foreign intelligence collection. Since May 1979, this Court has often recognized the expertise of the government in foreign intelligence collection and counterintelligence investigations of espionage and international terrorism, and accorded great weight to the government's interpretation of FISA's standards. However, this Court, or on appeal the Foreign Intelligence Surveillance Court of Review having jurisdiction "to review the denial of any application," is the arbiter of the FISA's terms and requirements. (§1803(b)) The present seven members of the Court have reviewed and approved several thousand FISA applications, including many hundreds of surveillances and searches of U.S. persons. The members bring their specialized knowledge to the issue at hand, mindful of the FISA's preeminent role in preserving our national security, not only in the present national emergency, but for the long term as a constitutional democracy under the rule of law.

II

We turn now to the government's proposed minimization procedures which are to be followed in all electronic surveillances and physical searches past, present, and future. In addition to the Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power that are filed with the Court, which we continue to approve, the government has submitted new supplementary minimization procedures

adopted by the Attorney General and promulgated in the form of a memorandum addressed to the Director of the FBI and other senior Justice Department executives and dated March 6, 2002. (hereafter the Attorney General's memorandum or the 2002 procedures). The Attorney General's memorandum is divided into three sections entitled:

"I. INTRODUCTION AND STATEMENT Of GENERAL PRINCIPLES,"[48]

"II. INTELLIGENCE SHARING PROCEDURES CONCERNING THE CRIMINAL DIVISION," AND "III. INTELLIGENCE SHARING PROCEDURES CONCERNING A USAO."

The focus of this decision is sections II and III which set out supplementary procedures affecting the acquisition, retention, and dissemination of information obtained through electronic surveillances and physical searches of U.S. persons to be approved as part of the government's applications and incorporated in the orders of this Court.

Our duty regarding approval of these minimization procedures is inscribed in the Act, as is the standard we must follow in our decision making. Where Congress has enacted a statute like the FISA, and defined its terms, we are bound to follow those definitions. We cannot add to, subtract from, or modify the words used by Congress, but must apply the

---

[48] The Attorney General's memorandum of March 6, 2002 asserts its interpretation of the recent amendments to the FISA to mean that the Act can now "be used primarily for a law enforcement purpose, so long as a significant foreign intelligence purpose remains." The government supports this argument with a lengthy memorandum of law which we have considered. However, the Court has decided this matter by applying the FISA's standards for minimization procedures defined in §1801(h) and §1821(4) of the Act, and does not reach the question of whether the FISA may be used primarily for law enforcement purposes. We leave this question for another day.

FISA's provisions with fidelity to their plain meaning and in conformity with the overall statutory scheme. The FISA is a statute of unique character, intended to authorize electronic surveillances and physical searches of foreign powers and their agents, including U.S. Persons. "Further, as a statute addressed entirely to 'specialists,' it must as Mr. Justice Frankfurter observed, 'be read by judges with the minds of *** specialists'."[49]

The Attorney General's new minimization procedures are designed to regulate acquisition, retention, and dissemination of information involving the FISA (i.e., disseminating information, consulting, and providing advice) between FBI counterintelligence and counterterrorism officials on the one hand, and FBI criminal investigators, trial attorneys in the Justice Department's Criminal Division, and U.S. Attorney's Offices on the other hand. These new minimization procedures supersede similar procedures issued by the Attorney General in July 1995 (hereafter the 1995 procedures) which were augmented in January 2000 and then in August 2001 by the current Deputy Attorney General. The Court has relied on the 1995 procedures, which have been followed by the FBI and the Justice Department in all electronic surveillance and physical searches of U.S. persons since their promulgation in July 1995. In November 2001, the court formally adopted the 1995 procedures, as augmented, as minimization procedures defined in §1801(h) and §1821(4), and has incorporated them in all applicable orders and warrants granted since then.

The 2002 procedures have been submitted to the Court pursuant to §1804(a)(5) and §1823(a)(5) to supplement the Standard Minimization Procedures for U.S. Person Agents of Foreign Powers. Both sets of procedures are to be applied in past and future electronic surveillances and physical searches

---

[49] Cheng Fan Kwok v. Immigration and Naturalization Service, 392 U.S. 206, S.Ct. 1970 (1968).

subject to the approval of this Court. Pursuant to §1805(a) and §1824(a) the Court has carefully considered the 2002 intelligence sharing procedures. The Court finds that these procedures 1) have been adopted by the Attorney General, 2) are designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons, and 3) are, therefore, minimization procedures as defined in §1801(h) and §1821(4).

The standard we apply in these findings is mandated in §1805(a)(4) and §1824(a)(4), which state that "the proposed minimization procedures meet the definition of minimization procedures under §101(h), [§1801(h) and §1821(4)] of the Act." 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).

Thus in approving minimization procedures the Court is to ensure that the intrusiveness of foreign intelligence surveillances and searches on the privacy of U.S. persons is "consistent" with the need of the United States to collect foreign intelligence information from foreign powers and their agents.

Our deliberations begin with an examination of the first part of §1801(h) and §1821(4) involving the acquisition, retention and dissemination of U.S. person information. Most of the rules and procedures for minimization are set forth in the Standard Minimization Procedures which will continue to be applied along with the 2002 procedures, and permit exceptionally thorough acquisition and collection through a broad army of contemporaneous electronic surveillance techniques. Thus, in many U.S. person electronic surveillances the FBI will be authorized to conduct, simultaneously, telephone, microphone, call phone, e-mail and computer surveillance of the U.S. person target's home, workplace and vehicles. Similar breadth is accorded the FBI in physical searches of the target's residence, office, vehicles, computer, safe deposit box and U.S. mails where supported by probable cause. The breadth of acquisition is premised an the fact that clandestine intelligence activities and activities in preparation for international terrorism are undertaken with considerable discretion and support from sophisticated intelligence services of nation states and well-financed groups engaged in international terrorism.

The intrusiveness of the FBI's electronic surveillances and sophisticated searches and seizures is sanctioned by the following practices and provisions in the FISA:

- a foreign intelligence standard of probable cause instead of the more traditional criminal standard of probable cause;
- having to show only that the place or facility to be surveilled or searched is being used or about to be used without the need of showing that it is being used in furtherance of the espionage or terrorist activities;
- surveillances and searches are conducted surreptitiously without notice to the target unless they are prosecuted;

- surveillances and now searches arc authorized for 90 days, and may continue for as long as one year or more in certain cases;
- large amounts of information are collected by automatic recording to be minimized after the fact;
- most information intercepted or seized has a dual character as both foreign intelligence information and evidence of crime (e.g., the identity of a spy's handler, his/her communication signals and deaddrop locations; the fact that a terrorist is taking flying lessons, or purchasing explosive chemicals) differentiated primarily by the persons using the information;[50]
- when facing criminal prosecution, a target cannot obtain discovery of the FISA applications and affidavits supporting the Court's orders in order to challenge them because the FISA mandates in camera, ex parte review by the district court "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security." §1806(f))and §1825(g)

It is self evident that the technical and surreptitious means available for acquisition of information by electronic surveillances and physical searches, coupled with the scope and duration of such intrusions and other practices under the FISA, give the government a powerful engine for the

[50] Sections §1801(h)(3) and §1821(4)(C) require that the minimization procedures must allow retention and dissemination of evidence of a crime which has been, is being, or is about to be committed. Such crimes are not related to the target's intelligence or terrorist activities, and the information would have to be discarded otherwise because it is not necessary to produce foreign intelligence information. Such retention and dissemination is not relevant to the issues considered in this opinion. Foreign Intelligence Surveillance Act of 1978, H.R. 7308, 95th Congress, 2nd Session, Report 95-1283, Pt. 1, p.62.

collection of foreign intelligence information targeting U.S. persons.

Retention under the standard minimization procedures is also heavily weighted toward the government's need for foreign intelligence information. Virtually all information seized, whether by electronic surveillance or physical search, is minimized hours, days, or weeks after collection. The principal steps in the minimization process are the same for electronic surveillances and physical searches:

- information is reduced to an intelligible form: if recorded it is transcribed, if in a foreign language it is translated, if in electronic or computer storage it is accessed and printed, if in code it is decrypted and if on film or similar media it is developed and printed;
- once the information is understandable, a reviewing official, usually an FBI case agent, makes an informed judgment as to whether the information seized is or might be foreign intelligence information related to clandestine intelligence activities or international terrorism;
- if the information is determined to be, or might be, foreign intelligence, it is logged into the FBI's records and filed in a variety of storage systems from which it can be retrieved for analysis, for counterintelligence investigations or operations, or for use at criminal trial;
- if found not to be foreign intelligence information, it must be minimized, which can be done in a variety of ways depending upon the format of the information: if recorded the information would not be indexed, and thus become non-retrievable, if in hard copy from facsimile intercept or computer print-out it should be discarded, if on re-recordable media it could be

> erased, or if too bulky or too sensitive, it might be destroyed.

These same principles of minimization are applied to all information collected, whether by electronic surveillance or physical search. The most critical step in retention is the analysis in which an informed judgment is made as to whether or not the communications or other data seized is foreign intelligence information. To guide FBI personnel in this determination the Standard Minimization Procedures for U.S. Person Agent of a Foreign Power in Section 3(a)(4) Acquisition/Interception/Monitoring and Logging provide that "communications of or concerning United States persons that could not be foreign intelligence information or are not evidence of a crime . . . may not be logged or summarized." (emphasis added). Minimization is required only if the information "could not be" foreign intelligence. Thus, it is obvious that the standard for retention of FISA-acquired information is weighted heavily in favor of the government.

This brings us to the third and perhaps most complex part of minimization practice, the dissemination and use of FISA-acquired information. Recognizing the broad sweep of acquisition allowed under FISA's definition of electronic surveillance (and, subsequently, physical searches), coupled with the low threshold for retention in the "could not be foreign intelligence" standard, Congress has provided guidance for the Court in the FISA's legislative history:

> On the other hand, given this degree of latitude the committee believes it is imperative that with respect to information concerning U.S. persons which is retained as necessary for counterintelligence or counter terrorism purposes, rigorous and strict controls be placed on the retrieval of such identifiable information and its dissemination or use for purposes other than

counterintelligence or counter terrorism. (emphasis added)[51]

The judge has the discretionary power to modify the order sought, such as with regard to the period of authorization . . . or the minimization procedures to be followed. (emphasis added)[52] The Committee contemplates that the court would give these procedures most careful consideration. If it is not of the opinion that they will be effective, the procedures should be modified. (emphasis added)[53]

Between 1979 when the FISA became operational and 1995, the government relied on the standard minimization procedures described herein to regulate all electronic surveillance. In 1995, following amendment of the FISA to permit physical searches, comparable minimization procedures were adopted for foreign intelligence searches. On July 19, 1995, the Attorney General issued Procedures for Contracts Between the FBI and Criminal Division Concerning FI and Foreign Counterintelligence Investigations, which in part A regulated "Contacts During an FI or FCI Investigation in Which FISA Surveillance or Searches are Being Conducted" between FBI personnel and trial attorneys of the Department's Criminal Division. The Court was duly informed of these procedures and has considered them an integral part of the minimization process although they were not formally submitted to the Court under §1804 (a)(5) or §1823(a)(5). In January, 2000 the Attorney General augmented the 1995 procedures to permit more information sharing from FISA cases with the Criminal Division, and the current Deputy Attorney General expanded the procedures in August 2001. Taken together, the 1995

---

[51] Id. at 59.
[52] Id at 78.
[53] Id. at 80.

Procedures, as augmented, permit substantial consultation and coordination as follows:

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

b. The 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, and the Criminal Division, about intelligence cases, including those in which FISA is or may be used;

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.

The Court came to rely on these supplementary procedures, and approved their broad information sharing and coordination with the Criminal Division in thousands of applications. In addition, because of the FISA's requirement (since amended) that the FBI Director certify that "the purpose" of each surveillance and search was to collect foreign intelligence information, the Court was routinely apprised of consultations and discussions between the FBI, the Criminal Division, and U.S. Attorney's offices in cases where there were overlapping intelligence and criminal investigations or interests. This process increased dramatically in numerous FISA applications concerning the September 11th attack on the World Trade Center and the Pentagon.

In order to preserve both the appearance and the fact that FISA surveillances and searches were not being used sub rosa for criminal investigations, the Court routinely approved the use of information screening "walls" proposed by the government in its applications. Under the normal "wall" procedures, where there were separate intelligence and criminal investigations, or a single counter-espionage investigation with overlapping intelligence and criminal interests, FBI criminal investigators and Department prosecutors were not allowed to review all of the raw FISA intercepts or seized materials lest they become defacto partners in the FISA surveillances and searches. Instead, a screening mechanism, or person, usually the chief legal

counsel in a FBI field office, or an assistant U.S. attorney not involved in the overlapping criminal investigation, would review all of the raw intercepts and seized materials and pass on only that information which might be relevant evidence. In unusual cases such as where attorney-client intercepts occurred, Justice Department lawyers in OIPR acted as the "wall." In significant cases, involving major complex investigations such as the bombings of the U.S. Embassies in Africa, and the millennium investigations, where criminal investigations of FISA targets were being conducted concurrently, and prosecution was likely, this Court became the "wall" so that FISA information could not be disseminated to criminal prosecutors without the Court's approval. In some cases where this Court was the "wall," the procedures seemed to have functioned as provided in the Court's orders; however, in an alarming number of instances, there have been troubling results.

Beginning in March 2000, the government notified the Court that them had been disseminations of FISA information to criminal squads in the FBI's New York field office, and to the U.S. Attorney's Office for the Southern District of Now York, without the required authorization of the Court as the"wall" in four or five FISA cases. Subsequently, the government filed a notice with the Court about its unauthorized disseminations.

In September 2000, the government came forward to confess error in some 75 FISA applications related to major terrorist attacks directed agaiinst the United States. The errors related to misstatements and omissions of material facts. including:

a. an erroneous statement in the FBI Director's FISA certification that the target of the FISA was not under criminal investigation;

b. erroneous statements in the FISA affidavits of FBI agents concealing the separation of the overlapping

intelligence and criminal investigations, and the unauthorized sharing of FISA information with FBI criminal investigators and assistant U.S. attorneys;

c. omissions of material facts from FBI FISA affidavits relating to a prior relationship between the FBI and a FISA target, and the interview of a FISA target by an assistant U.S. attorney.

In November of 2000, the Court held a special meeting to consider the troubling number of inaccurate FBI affidavits in so many FISA applications. After receiving a more detailed explanation from the Department of Justice about what went wrong, but not why, the Court decided not to accept inaccurate affidavits from FBI agents whether or not intentionally false. One FBI agent was barred from appearing before the Court as a FISA affiant. The Court decided to await the results of the investigation by the Justice Department's Office of Professional Responsibility before taking further action.

In March of 2001, the government reported similar misstatements in another series of FISA applications in which there was supposedly a "wall" between separate intelligence and criminal squads in FBI field offices to screen FISA intercepts, when in fact all of the FBI agents were on the same squad and all of the screening was done by the one supervisor overseeing both investigations.

To come to grips with this problem, in April of 2001, the FBI promulgated detailed procedures governing the submission of requests to conduct FISA surveillances and searches, and to review draft affidavits in FISA applications, to ensure their accuracy. These procedures are currently in use and require careful review of draft affidavits by the FBI agents in the field offices who are conducting the FISA case investigations, as well as the supervising agents at FBI headquarters who appear before the Court and swear to the affidavits.

In virtually every instance, the government's misstatements and omissions in FISA applications and violations of the Court's orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors. These incidents have been under investigation by the FBI's and the Justice Department's Offices of Professional Responsibility for more than one year to determine how the violations occurred in the field offices, and how the misinformation found its way into the FISA applications and remained uncorrected for more than one year despite procedures to verify the accuracy of FISA pleadings. As of this date, no report has been published, and how these misrepresentations occurred remains unexplained to the Court.

As a consequence of the violations of its orders, the Court has taken some supervisory actions to assess compliance with the "wall" procedures. First, until September 15, 2001, it required all Justice Department personnel who received certain FISA information to certify that they understood that under "wall" procedures FISA information was not to be shared with criminal prosecutors without the Court's approval. Since then, the Court has authorized criminal division trial attorneys to review all FBI international terrorism case files, including FISA case files and required reports from FBI personnel and Criminal Division attorneys describing their discussions of the FISA cases. The government's motion that the Court rescind all "wall" procedures in all international terrorism surveillances and searches now pending before the Court, or that has been before the Court at anytime in the past, was deferred by the Court until now at the suggestion of the government, pending resolution of this matter.

Given this history in FISA information sharing, the Court now turns to the revised 2002 minimization procedures. We recite this history to make clear that the Court has long approved, under controlled circumstances, the sharing of

FISA information with criminal prosecutors as well as consultations between intelligence and criminal investigations where FISA surveillances and searches are being conducted. However, the proposed 2002 minimization procedures eliminate the bright line in the 1995 procedures prohibiting direction and control by prosecutors on which the Court has relied to moderate the broad acquisition retention, and dissemination of FISA information in overlapping intelligence and criminal investigations. Paragraph A.6 of the 1995 procedures provided in part:

> Additionally, the FBI and the Criminal Division should ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling the FI or FCI investigation toward law enforcement objectives. (emphasis added)

As we conclude the first part of our statutory task, we have determined that the extensive acquisition of information concerning U.S. persons through secretive surveillances and searches authorized under FISA, coupled with broad powers of retention and information sharing with criminal prosecutors, weigh heavily on one side of the scale which we must balance to ensure that the proposed minimization procedures are consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. (§1805(a)(4) and §1824(a)(4))

III

The 2002 minimization rules set out in sections II and III, "Intelligence Sharing Procedures Concerning the Criminal Division" and "Intelligence Sharing Procedures Concerning a USAO," continue the existing practice approved by this Court of in-depth dissemination of FISA infomation to Criminal Division trial attorneys and U.S. Attorney's Offices (hereafter criminal prosecutors). These new procedures apply

in two kinds of counterintelligence cases in which FISA is the only effective tool available to both counterintelligence and criminal investigators:

1) those cases in which separate intelligence and criminal investigations of the same U.S. person FISA target are conducted by different FBI agents (overlapping investigations), usually involving international terrorism, and in which separation can easily be maintained, and

2) those cases in which one investigation having a U.S. person FISA target is conducted by a team of FBI agents which has both intelligence and criminal interests (overlapping interests) usually involving espionage and similar crimes in which separation is impractical.

In both kinds of counterintelligence investigations where FISA is being used, the proposed 2002 minimization procedures authorize 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 as now expressly provided in §1806(k)(1) and §1825(k)(1), These consultations propose to include:

II. A. "Disseminating Information," which gives criminal prosecutors access to "all information developed" in FBI counterintelligence investigations, including FISA acquired information, as well as annual and other reports, and presumably ad hoc reporting of significant events (e.g., incriminating FISA intercepts or seizures) to criminal prosecutors.

II. B. "Providing Advice," where criminal prosecutors are authorized 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." Recommendations may include advice about criminal investigation and prosecution as well as the strategy and goals for investigations, the law enforcement and intelligence methods to be used in investigations, and the interaction between intelligence and law enforcement components of investigations.

Last, but most relevant to this Court's finding, criminal prosecutors are empowered to advise FBI intelligence officials concerning "the initiation, operation, continuation, or expansion of FISA searches and surveillance." (emphasis added) This provision is 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."

In section III, "Intelligence Sharing Procedures Concerning a USAO," U.S. attorneys are empowered to "engage in consultations to the same extent as the Criminal Division under parts II. A and II. B of these procedures," in cases involving international terrorism.

A fair reading of those provisions leaves only one conclusion -- under sections II and III of the 2002 minimization procedures, criminal prosecutors are to have a significant role directing FISA surveillances and searches from start to finish in counterintelligence cases having overlapping intelligence and criminal investigations or interests, guiding them to criminal prosecution. The government makes no secret of this policy, asserting its interpretation of the Act's new amendments which "allows FISA to be used primarily for a law enforcement purpose."

Given our experience in FISA surveillances and searches, we find that these provisions in sections II.B and III, particularly those which authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are

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) as mandated in §1801(h)and §1821(4). The 2002 procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillances and Rule 41 searches. This may be because the government is unable to meet the substantive requirements of these law enforcement tools, or because their administrative burdens are too onerous. In either case, the FISA's definition of minimization procedures has not changed, and these procedures cannot be used by the government to amend the Act in ways Congress has not. We also find the provisions in section II.B and III. wanting because the prohibition in the 1995 procedures of criminal prosecutors "directing or controlling" FISA cases has been revoked by the proposed 2002 procedures. The government's memorandum of law expends considerable effort justifying deletion of that bright line, but the Court is not persuaded.

The Court has long accepted and approved minimization procedures authorizing in-depth information sharing and coordination with criminal prosecutors as described in detail above. In the Court's view, the plain meaning of consultations and coordination now specifically authorized in the Act is based on the need to adjust or bring into alignment two different but complementary interests -- intelligence gathering and law enforcement. In FISA cases this presupposes separate intelligence and criminal investigations, or a single investigation with intertwined interests, which need to be brought into harmony to avoid dysfunction and frustration of either interest. 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. The proposed 2002

minimization procedures require the Court to balance the government's use of FISA surveillances and searches against the government's need to obtain and use evidence for criminal prosecution, determining the "need of the United States to obtain, produce, and disseminate foreign intelligence information" as mandated by §1801(h) and §1821(4).

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, including:

- a foreign intelligence standard instead of a criminal standard of probable cause;
- use of the most advanced and highly intrusive techniques for intelligence gathering; and
- surveillances and searches for extensive periods of time;

based on a standard that the U.S. person is only using or about to use the places to be surveilled and 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.

THEREFORE, because

- the procedures implemented by the Attorney General govern the minimization of electronic surveillances and searches of U.S. persons;
- such intelligence and criminal investigations both target the same U.S. person;
- the information collected through FISA surveillances and searches is both foreign intelligence information and evidence of crime, depending upon who is using it;
- there are pervasive and invasive techniques for electronic surveillances and physical searches authorized under the FISA;
- surveillances and searches may be authorized for extensive periods of time;
- notice of surveillances and searches is not given to the targets unless they prosecuted;
- the provisions in FISA constrain discovery and adversary hearings and require ex parte, in camera review of FISA surveillances and searches at criminal trial;
- the FISA, as opposed to Title III and Rule 41 searches, is the only tool available in these overlapping intelligence and criminal investigations;
- there are extensive provisions in the minimization procedures for dissemination of FISA intercepts and seizures to criminal prosecutors and for consultation

and coordination with intelligence officials using the FISA;

- criminal prosecutors would, under the proposed procedures, no longer be prohibited from "directing or controlling" counterintelligence investigations involving use of the FISA toward law enforcement objectives; and
- criminal prosecutors would, under the proposed procedures, be empowered to direct the use of FISA surveillances and searches toward law enforcement objectives by advising FBI intelligence officials on the initiation, operation, continuation and expansion of FISA authority from this Court,

The Court FINDS that parts of section II.B of the minimization procedures submitted with the Government's motion are NOT reasonably designed, in light of their purpose and technique, "consistent with the need of the United States to obtain, produce, or disseminate foreign intelligence information" as defined in §1801(h) and §1821(4) of the Act.

THEREFORE, pursuant to this Court's authority under §1805(a) and §1824(a) to issue ex parte orders for electronic surveillances and physical searches "as requested or as modified," the Court herewith grants the Governments motion BUT MODIFIES the pertinent provisions of sections II.B. of the proposed minimization procedures as follows:

The second and third paragraphs of section II.B shall be deleted, and the following paragraphs substituted in place thereof:

"The FBI, the Criminal Division, and OIPR may consult with each other 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. Such

consultations and coordination may address, among other things, exchanging information already acquired, identifying categories of information needed and being sought, preventing either investigation or interest from obstructing or hindering the other, compromise of either investigation, and long term objectives and overall strategy of both investigations in order to ensure that the overlapping intelligence and criminal interests of the United States are both achieved. Such consultations and coordination may be conducted directly between the components, however, OIPR shall be invited to all such consultations, and if they are unable to attend, OIPR shall be apprised of the substance of the consultations forthwith in writing so that the Court may be notified at the earliest opportunity."

"Notwithstanding the foregoing, law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives."

These modifications are intended to bring the minimization procedures into accord with the language used in the FISA, and reinstate the bright line used in the 1995 procedures, on which the Court has relied. The purpose of minimization procedures as defined in the Act, is not to amend the statute, but to protect the privacy of Americans in these highly intrusive surveillances and searches, "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

A separate order shall issue this date.

All seven judges of the Court concur in the Corrected and Amended Memorandum Opinion.

ROYCE C. LAMBERTH
Presiding Judge

DATE: 5-17-02 6:40 p.m.

FILED
KAREN E. SUTTON, CLERK
MAY 17 2002
U.S. Foreign Intelligence
Surveillance Court

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE ALL MATTERS SUBMITTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

Docket Numbers: Multiple

ORDER
(AS AMENDED)

Motion having been made by the United States of America, by James A. Baker, Counsel for Intelligence Policy, United States Department of Justice, for the Court to approve proposed minimization procedures entitled Intelligence Sharing Procedures for Foreign Intelligence and Foreign

Counterintelligence Investigations Conducted by the FBI, to be used in electronic surveillances and physical searches authorized by this Court, as well as a supporting memorandum of law, and a supplemental memorandum, which filing was approved by the Attorney General of the United States, and full consideration having been given to the matters set forth therein, the Court finds:

1. The President has authorized the Attorney General of the United States to approve applications for electronic surveillance and physical search for foreign intelligence purposes. 50 U.S.C. §1805(a)(1) and §1824(a)(1);

2. The motion has been made by a Federal officer and approved by the Attorney General, 50 U.S.C. §1805(a)(2) and §1824(a)(2);

3. The proposed minimization procedures entitled Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI as modified herein, meet the definition of minimization procedures under §1801(h) and §1821(4)of the Act, 50 U.S.C. §1805(a)(4) and §1824(a)(4).

WHEREFORE IT IS ORDERED,

A. The aforementioned minimization procedures are herewith modified, pursuant to this Court's authority under 50 U.S.C. §1805(a) and (c) and 50 U.S.C.§1824(a) and (c), to delete the second, third, and fourth paragraphs from Section I of the proposed minimization procedures. A revised statement of "General Principles" that is not inconsistent with the Court's opinion may be included in the Attorney General's memorandum.

B. The aforementioned minimization procedures are further modified, pursuant to this Court's authority under 50 U.S.C. §1805(a) and (c) and 50 U.S.C. §1824(a) and (c), to delete the second and third paragraphs from Section II.B and substitute the following paragraphs in place thereof:

"The FBI, the Criminal Division, and OIPR may consult with each other 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. Such consultations and coordination may address, among other things, exchanging in information already acquired; identifying categories of information needed and being sought; preventing either investigation or interest from obstructing or hindering the other; compromise of either investigation: and long term objectives and overall strategy of both investigations in order to ensure that the overlapping intelligence and criminal interests of the United States are both achieved. Such consultations and coordination may be conducted directly between the components; however, OIPR shall be invited to all such consultations, and if they are unable to attend, OIPR shall be apprized of the substance or the meetings forthwith in writing so that the Court may be notified at the earliest opportunity."

"Notwithstanding the foregoing, law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives."

C. Use of the aforementioned minimization procedures as modified, in a11 <u>future</u> electronic surveillance and physical searches shall be subject to the approval of the Court in each electronic surveillance and physical search where their use is

proposed by the Government pursuant to 50 U.S.C. §1804(a)(5)) and §1823(a)(5).

WHEREFORE, IT IS FURTHER ORDERED, pursuant to the authority conferred on this Court by the Foreign Intelligence Surveillance Act, that the motion of the United States to use the aforementioned minimization procedures as modified, in all electronic surveillances and physical searches already approved by the Court, as described in the Government's motion is GRANTED AS MODIFIED herein.

A separate Memorandum Opinion bas been filed this date. The motion of the United States has been considered by all of the judges of this Court, all of whom concur in the Memorandum Opinion and in the Order. The Court has also adopted a new administrative rule to monitor compliance with this Order as follows:

Rule 11. Criminal Investigations in FISA Cases

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.

All seven judges of the Court concur in this Amended Order.

ROYCE C. LAMBERTH
Presiding Judge,
United States Foreign Intelligence
Surveillance Court

Signed 5-17-02 6:40 p.m. E.S.T.

FILED
KAREN E. SUTTON, CLERK
MAY 17 2002
U.S. Foreign Intelligence
Surveillance Court

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE ALL MATTERS SUBMITTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

Docket Numbers: Multiple

ORDER

Motion having been made by the United States of America, by James A. Baker, Counsel for Intelligence Policy, United States Department of Justice, for the Court to clarify its order of April 22, 2002 in the above captioned matter, and full consideration having been given to the matters set forth therein, the motion to clarify is granted and the Court's order and memorandum opinion of April 22, 2002 in this matter are amended as follows:

1. The language of the Court's order and memorandum opinion of April 22, 2002 are amended to include the following substitute sentence in the second paragraph of the modified minimization procedures to read: "Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives."

2. The government also asks that the Court clarify whether its use of the term "law enforcement officials" in the substitute minimization language adopted by the Court "applies to FBI agents as well as to prosecutors." The Court's own opinion states as follows:

The Attorney General's new minimization procedures are designed to regulate the acquisition, retention and dissemination of information involving the FISA (i.e., disseminating information, consulting, and providing advice) between FBI counterintelligence and counter-terrorism officials on the one hand, and FBI criminal investigators, trial attorneys in the Justice Department's Criminal Division, and U.S. Attorney's Offices on the other hand. (emphasis added) (Opinion, 6-7).

The Court uses, and intended to use, the term "law enforcement officials" in conjunction with the source and context from which it originated, i.e., the recent amendment to the FISA in which Congress expressly authorized consultations and coordination between federal officers who conduct electronic surveillances and physical searches to acquire foreign intelligence information and "Federal law enforcement officers." (50 U.S.C. §1806(k) and §1825(k). The new minimization procedures apply to the minimization

process in FISA electronic surveillances and physical searches, and to those involved in the process -- including both FBI agents and criminal prosecutors.

Contrary to the assumption made in the government's motion, all of the judges of this Court concurred in both the opinion and order of April 22, 2002.

ROYCE C. LAMBERTH
Presiding Judge
United States Foreign Intelligence
Surveillance Court

Date: 5-17-02 6:40 p.m.

CONCURRING IN THE ORDER:

Honorable William H. Stafford, Jr.
Judge, United States Foreign
Intelligence Surveillance Court

Honorable Stanley S. Brotman
Judge, United States Foreign
Intelligence Surveillance Court

Honorable Harold A. Baker
Judge, United States Foreign
Intelligence Surveillance Court

Honorable Michael J. Davis
Judge, United States Foreign
Intelligence Surveillance Court

Honorable Claude M. Hilton
Judge, United States foreign
Intelligence Surveillance Court

Honorable Nathaniel M. Gorton
Judge, United States Foreign
Intelligence Surveillance Court

Appendix C

Excerpts from the Foreign Intelligence Surveillance Act

§ 1801. Definitions

As used in this subchapter:

(a) "Foreign power" means—

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

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

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

(b) "Agent of a foreign power" means—

(1) any person other than a United States person, who--

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power;

(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).

(c) "International terrorism" means 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.

(d) "Sabotage" means activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

• • •

(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.

(i) "United States person" means 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.

§ 1804. Applications for court orders

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include—

(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—

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

(B) that a significant 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;

(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 than 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.

§ 1805. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

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

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

(3) 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.

(b) Probable cause

In determining whether or not probable cause exists for purposes of an order under subsection (a)(3), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

§ 1806. Use of information

(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.

• • •

(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 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.

§ 1823. Application for order

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving a physical search under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this subchapter. Each application shall 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 target 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);

(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.

§ 1824. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1823 of this title, the judge shall enter an ex parte order as requested or as modified approving the physical search if the judge finds 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 upon 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;

(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.

(b) Probable cause

In determining whether or not probable cause exists for purposes of an order under subsection (a)(3), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) Specifications and directions of orders

An order approving a physical search under this section shall—

(1) 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 or 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 physical searches are approved; and

(2) 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 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 Central Intelligence 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

(E) that the Federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained, or disseminated

(1) An order issued 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 1801(a) of this title, 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 targeted against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title may be for the

period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter 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 chapter for a physical search targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power, as defined in section 1801(a)(4) of this title, that is not a United States person, or against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title, 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.

(3) At or before the end of the period of time for which a physical search is approved by an order or an extension, or at any time after a physical search is carried out, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

§ 1825. Use of information

(d) Notification by United States

Whenever the United States 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 a physical search

pursuant to the authority of this subchapter, the United States shall, prior to the trial, hearing, or the 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 United States intends to so disclose or so use such information.

• • •

(f) Motion to suppress

(1) Any person against whom evidence obtained or derived from a physical search 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 search on the grounds that--

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

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

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

Whenever a court or other authority is notified pursuant to subsection (d) or (e) of this section, or whenever a motion is made pursuant to subsection (f) 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 a physical search authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this subchapter, 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 provision of law, if the Attorney General files an affidavit under oath that disclosure or any 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 physical search as may be necessary to determine whether the physical search 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 physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

(h) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (g) of this section determines that the physical search 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 the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court

determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.