No. 02-001

IN THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

IN RE

ON APPEAL FROM
THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

BRIEF FOR THE UNITED STATES

JOHN ASHCROFT
Attorney General

LARRY D. THOMPSON
Deputy Attorney General

THEODORE B. OLSON
Solicitor General

DAVID S. KRIS
Associate Deputy Attorney General

JAMES A. BAKER
Counsel for Intelligence Policy

JONATHAN L. MARCUS
Attorney Advisor
Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
(202) 514-2882

TABLE OF CONTENTS (U)

TABLE OF AUTHORITIES (U)

CASES: Page

STATUTES and RULES:

MISCELLANEOUS:

IN THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

No. 02-001

IN RE

ON APPEAL FROM
THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

BRIEF FOR THE UNITED STATES

JURISDICTION (U)

This is an appeal by the United States from the partial denial of an application for orders authorizing electronic surveillance under the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1862 (FISA). The Foreign Intelligence Surveillance Court (FISC) (Baker, J.), which had jurisdiction under 50 U.S.C. §§ 1803(a) and 1822(c), entered its judgment, and provided a written statement of reasons for its decision, on July 19, 2002. In accord with 50 U.S.C. § 1803(a) and Rule 6 of the Rules of the FISC, the United States moved for transmittal of the record, under seal, to this Court on July 24, 2002. This Court's jurisdiction rests on 50 U.S.C. § 1803(b). (U)

Although the FISC's order is not styled as a "denial," but rather as a grant of the FISA application as "as modified," it qualifies as a "denial" for purposes of establishing this Court's jurisdiction. July 2002 Order at 9. As detailed below, the government's application proposed that the electronic surveillance be authorized on certain terms, and the FISC's order rejected those terms and imposed restrictions on the government's investigation. Thus, the government's application was denied in part. See, *e.g.*, *Mobile Communications Corp. of Am.* v. *FCC*, 77 F.3d 1399, 1403-1404 (D.C. Cir. 1996) (grant of station license subject to condition that is unacceptable to applicant is denial of license subject to judicial review under statute that permits such review when applications for license are denied; otherwise the FCC could "foreclose judicial review of a de facto denial by couching its decision as an approval subject to some intolerable condition").[1] (U)

---

[1] To the extent any doubt remains as to this Court's jurisdiction, we ask the Court to rely on the All Writs Act, 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." 28 U.S.C. § 1651(a). Where, as here, a lower court issues a decision denying effect to key provisions of a recently enacted federal statute, mandamus is appropriate. See, *e.g.*, *In re Sealed Case*, 151 F.3d 1059, 1063 (D.C. Cir. 1998) (per curiam) (granting mandamus where right to it is "clear and indisputable" and "no other adequate means to attain the relief exist") (internal quotation marks omitted). (U)

QUESTION PRESENTED (U)

Whether the FISC erred in denying in relevant part an application for orders authorizing electronic surveillance where a "significant purpose" of the surveillance is to obtain foreign intelligence information, 50 U.S.C. § 1804(a)(7)(B), and intelligence officers conducting the electronic surveillance intend to "consult with Federal law enforcement officers to coordinate efforts to investigate [and] protect against * * * international terrorism," 50 U.S.C. § 1806(k). (U)

STATEMENT (U)

I. STATUTORY FRAMEWORK (U)

The Foreign Intelligence Surveillance Act of 1978 (FISA) governs electronic surveillance and physical searches of foreign powers and their agents inside the United States. The statute establishes two special courts: The FISC, which is comprised of 11 district court judges appointed by the Chief Justice, and this Court, which is comprised of three district court or court of appeals judges appointed by the Chief Justice.[2] 50 U.S.C. §§ 1803(a) and (b). The FISC has jurisdiction to grant or deny

---

[2] As enacted in 1978, FISA provided for a FISC comprised of seven district court judges. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), raised the number of judges from seven to 11, of whom no fewer than three must reside within 20 miles of the District of Columbia. (U)

applications for orders authorizing electronic surveillance and physical searches under the procedures set forth in FISA, and this Court has jurisdiction to review the denial of any application made under FISA. *Ibid.*; 50 U.S.C. § 1822(b)-(d).[3] (U)

Applications for court orders authorizing searches or surveillance under FISA are made to the FISC under oath by a federal officer with the approval of the Attorney General, the Acting Attorney General, or the Deputy Attorney General. 50 U.S.C. §§ 1801(g), 1804, 1823. The application must identify or describe the target of the search or surveillance, and establish that the target is either a "foreign power" or an "agent of a foreign power." 50 U.S.C. §§ 1804(a)(3), 1804(a)(4)(A), 1823(a)(3), 1823(a)(4)(A). A "foreign power" is defined to include, among other things, a "foreign government or any component thereof," and a "group engaged in international terrorism." 50 U.S.C. §§ 1801(a)(1), (4). The statute defines

---

[3] As enacted in 1978, FISA permitted applications for and orders authorizing electronic surveillance, but did not refer to physical searches. 50 U.S.C. §§ 1801-1811. In 1994, the statute was amended to permit applications for and orders authorizing physical searches. Pub. L. No. 103-359, 108 Stat. 3423, 3443 (Oct. 14, 1994); 50 U.S.C. §§ 1821-1829. The procedures governing FISA physical searches are similar to those governing FISA electronic surveillance. Although this case does not involve a physical search, we cite both the electronic surveillance and parallel physical search provisions of FISA in this brief. (U)

"agent of a foreign power" to include any person who "knowingly engages in * * * international terrorism * * * for or on behalf of a foreign power," and any person "other than a United States person" - i.e., someone other than a U.S. citizen or permanent resident alien - who is a "member" of a group engaged in international terrorism. 50 U.S.C. §§ 1801(b)(1)(A), (b)(2)(C), (i). "International terrorism" is defined by FISA to require activities that (1) involve violent or dangerous acts that violate U.S. law (or would do so if committed here); (2) appear to be intended to "intimidate or coerce" a civilian population, to "influence" government policy through "intimidation or coercion," or to "affect the conduct of government by assassination or kidnapping"; and (3) either "occur totally outside the United States, or transcend national boundaries" in various ways. 50 U.S.C. § 1801(c). (U)

Each FISA application must include a certification from a high-ranking Executive Branch official, such as the Director of the FBI, that the official "deems the information sought [by the search or surveillance] to be foreign intelligence information," and that "a significant purpose" of the search or surveillance is to obtain "foreign intelligence information."[4] 50 U.S.C.

---

[4] As originally enacted in 1978, FISA required a certification that "the purpose" of the search or surveillance

§§ 1804(a)(7)(A)-(B), 1823(a)(7)(A)-(B). FISA defines the term "foreign intelligence information" to include information necessary to "protect" the United States from espionage and international terrorism committed by foreign powers or their agents. 50 U.S.C. § 1801(e)(1). Each FISA application must also propose "minimization procedures" for the conduct of the search or surveillance. 50 U.S.C. §§ 1804(a)(5), 1823(a)(5), 1801(h), 1821(4). (U)

An individual judge of the FISC reviews each FISA application following its submission. 50 U.S.C. §§ 1805, 1824. To approve an application, the judge must find that it establishes "probable cause" to believe that the target of the search or surveillance is a foreign power or an agent of a foreign power. *Ibid.* The judge must also find that the proposed minimization procedures are "reasonably designed * * * 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." *Ibid.*; 50 U.S.C. §§ 1801(h), 1821(4).

---

was to obtain foreign intelligence information. The standard was changed to "a significant purpose" in the USA Patriot Act. See Argument II.B, *infra*. (U)

Finally, where the target of the search or surveillance is a "United States person" - a U.S. citizen or permanent resident alien - the judge must find that the Executive Branch's certification that a significant purpose of the search or surveillance is to obtain foreign intelligence information is not "clearly erroneous." 50 U.S.C. §§ 1805, 1824; H.R. Rep. No. 95-1283, Part I, 95th Cong., 2d Sess. (1978), at 80-81 [hereinafter House Report]. (U)

If the judge grants the FISA application, he signs an order identifying or describing the target and the facilities or places to be searched or surveilled, and directing that minimization procedures be followed, among other things. 50 U.S.C. §§ 1805(c), 1824(c). If the FISC judge denies a FISA application, he must "provide immediately for the record a written statement of each reason for [the] decision." 50 U.S.C. §§ 1803(a), 1822(c). Once an individual judge has denied an application, no other FISC judge may consider it; this Court is the only forum in which the FISC judge's decision may be reviewed. *Ibid.* There is no provision in FISA for a notice of appeal from the denial of an application; instead, "on motion of the United States, the record shall be transmitted, under seal, to" this Court. *Ibid.*; see FISC Rule 6. Thereafter, this Court may either affirm or reverse the FISC judge's decision; if this

Court "determines that the application was properly denied," then it too must "provide for the record a written statement of each reason for its decision." 50 U.S.C. §§ 1803(b), 1822(d). The Supreme Court has jurisdiction to review this Court's decision by writ of certiorari. *Ibid.* (U)

II. THE FISA APPLICATION AND THE FISC'S ORDER IN THIS CASE (U)

A. The Foreign Counterintelligence Investigation. (U)

B. The Criminal Investigation. (U)

C. Coordination Between the Counterintelligence and Criminal Investigations. (U)

The FISA application in this case stated that, upon approval of the FISC, the government would follow the coordination standards set forth in Intelligence Sharing Procedures adopted by the Attorney General on March 6, 2002. App. 1:2.[5] As detailed below, the Attorney General adopted those Procedures to implement the USA Patriot Act, which changed the standards governing coordination between intelligence and law enforcement officials under FISA. The new Procedures were submitted to the FISC on

[5] "App." refers to the Appendix filed with the FISA Application in this case, and is followed by a tab number, and where applicable, a document number, and/or a page number. (U)

March 7, 2002, and were rejected in part and rewritten in part by the FISC in an order and opinion issued on May 17, 2002. App. 6. In the current case, the FISC likewise rejected the government's request to follow the March 2002 Procedures and granted the FISA application on condition that the government obey the FISC's May 2002 order. See July 2002 Order 6-7. The following paragraphs describe the main provisions of the March 2002 Procedures, the FISC's May 2002 order modifying the Procedures, and the FISC's May 2002 opinion explaining the reasons for its order. (U)

1. The March 2002 Procedures. The Department's March 2002 Intelligence Sharing Procedures are designed to ensure that foreign intelligence (FI) and foreign counterintelligence (FCI) investigations "are conducted lawfully, particularly in light of requirements imposed by [FISA]," and to "promote the effective coordination and performance of the [Department's] criminal and counterintelligence functions." App. 1:2 at 1. They identify two important amendments to FISA made by the USA Patriot Act that authorize more effective coordination between intelligence and law enforcement officials. First, the Procedures explain, while prior law provided that "FISA could be used only for the 'primary purpose' of obtaining 'foreign intelligence information,'" the USA Patriot Act "allows FISA to be used for 'a significant purpose,' rather than the primary purpose, of obtaining foreign

intelligence information." *Id.* at 2 (quoting 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)). Thus, the Procedures explain, the Patriot Act "allows FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains" (emphasis in original). *Ibid.* (U)

Second, the Patriot Act "expressly authorizes intelligence officers who are using FISA to 'consult' with federal law enforcement officers to 'coordinate efforts to investigate or protect against' foreign threats to national security," including international terrorism. App. 1:2 at 2 (quoting 50 U.S.C. §§ 1806(k), 1825(k)). Under this authority, the Procedures explain, intelligence and law enforcement officers may exchange a "full range of information and advice" concerning their efforts to protect against international terrorism (and the other specified threats). *Ibid.* The Procedures further explain that robust coordination is permitted because the Patriot Act provides expressly that such coordination "'shall not' preclude the government's certification of a significant foreign intelligence purpose or the issuance of a FISA warrant" by the FISC. *Ibid.* (quoting 50 U.S.C. §§ 1806(k), 1825(k)). (U)

In keeping with that understanding of the USA Patriot Act, the Procedures generally permit the total exchange of information and advice between intelligence and law enforcement officials,

emphasizing that "[t]he overriding need to protect the national security from foreign threats compels a full and free exchange of information and ideas." App. 1:2 at 2. Part II.A of the Procedures, which governs information-sharing, provides that prosecutors "shall have access to all information developed in full field FI and FCI investigations" that are conducted by the FBI, including investigations in which FISA is being used, "except as limited by orders issued by the [FISC], controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases." *Id.* at 2-3. The FBI's principal obligation is to keep prosecutors "apprised of all information" from such investigations "that is necessary to the ability of the United States to investigate and protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities." *Id.* at 3. To implement these requirements, prosecutors are granted access to FBI files and memoranda. *Ibid.*[6] (U)

---

[6] These provisions, and the advice-giving provisions described in the next paragraph of the text, apply to the Department's Criminal Division and to a United States Attorney's Office in any case involving international terrorism. In espionage cases, the U.S. Attorneys receive information from and provide advice to the FBI as authorized by the Criminal Division. See March 2002 Procedures, Parts II and III. (U)

Part II.B of the Procedures, which governs advice-giving, allows prosecutors to provide advice to the FBI about the conduct of an FI or FCI investigation, including advice about the use of FISA. App. 1:2 at 4. It directs the FBI, the Office of Intelligence Policy and Review (OIPR), which represents the Department before the FISC, and prosecutors to meet regularly, and as needed, to conduct consultations. *Ibid.* The Procedures explicitly permit consultations directly between prosecutors and the FBI, without OIPR present. *Ibid.* The Procedures describe the range of permitted consultations as follows:

> Consultations may include the exchange of advice and recommendations on all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities, including protection against the foregoing through criminal investigation and prosecution, subject to the limits set forth above. Relevant issues include, but are not limited to, the strategy and goals for the investigation; the law enforcement and intelligence methods to be used in conducting the investigation; the interaction between intelligence and law enforcement components as part of the investigation; and the initiation, operation, continuation, or expansion of FISA searches or surveillance.

Ibid. (emphasis added). The Procedures explain that "[s]uch consultations are necessary to the ability of the United States to coordinate efforts to investigate and protect against foreign threats to national security as set forth in 50 U.S.C. 1806(k), 1825(k)." *Ibid.* (U)

2. The FISC's May 2002 Order. In its May 2002 order, the FISC accepted some aspects of the Department's March 2002 Procedures and rejected others. The FISC accepted in full the information-sharing provisions of the Procedures, Part II.A. See App. 6:2 at 2; App. 6:3 at 25. Thus, the FISC approved the Department's standards generally allowing wholesale dissemination of information from FI and FCI investigations to law enforcement officials, subject to specific limits imposed in particular cases. (U)

However, the FISC rejected much of Part II.B of the Procedures, which allows law enforcement officials to give advice to intelligence officials. Instead of allowing consultation and coordination on "all issues" necessary to protect the United States from foreign threats to national security, the FISC held that prosecutors and intelligence agents may consult on the following matters, "among other things":

> [1] exchanging information already acquired; [2] identifying categories of information needed and being sought; [3] preventing either [the law enforcement or counterintelligence] investigation or interest from obstructing or hindering the other; [4] [preventing the] compromise of either investigation; and [5] [formulating] 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.

App. 6:2 at 2-3. (U)

Notwithstanding that authorization to provide advice, however, the FISC imposed three limits on advice-giving. First, it held that law enforcement officials may "not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances," and warned law enforcement officials not to "direct or control the use of FISA procedures to enhance criminal prosecution." App. 6:2 at 3. Thus, for example, law enforcement officials may not nominate targets for FISA searches or surveillance. Nor may they recommend that an existing FISA search or surveillance be conducted in a particular way or seek particular information. (U)

Second, the FISC instructed the FBI and prosecutors to "ensure that advice designed to preserve the option of a criminal prosecution does not inadvertently result in [prosecutors'] directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives." App. 6:2 at 3. The FISC's approval of advice designed to "preserve" the option of a criminal prosecution, and its ban on advice amounting to prosecutorial "direction or control" of an investigation, led the government to file a motion for clarification. App. 5. The motion inquired whether the FISC intended to permit advice designed to "enhance," rather than merely to "preserve," a

criminal prosecution, a distinction addressed at length in a major report on FISA that was the subject of extended discussions between the FISC and the government. See IV *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation*, Chapter 20, at 721-734 (May 2000) (hereinafter AGRT Report); App. 2:2 at 7-8, 22-23. The motion asked the FISC either to delete the reference to "preserv[ing]" advice or to explain in more detail the scope of any ban on "enhancing" advice. The FISC did neither. Compare App. 4:1 at 3 with App. 6:1 at 1-2, and App. 6:2 at 3.[7] (U)

Third and finally, the FISC imposed a "chaperone" requirement, holding that prosecutors may not consult with intelligence agents unless they first invite OIPR to participate in the consultation, and that OIPR must participate unless it is "unable" to do so. If OIPR does not participate, the FISC held, it "shall be apprised of the substance of the meetings forthwith in writing so that the [FISC] may be notified at the earliest opportunity." App. 6:2 at 3. The FISC also adopted a new rule to the same effect: "All FISA applications shall include

---

[7] The language quoted in the text is from the FISC's May 2002 order. App. 6:2. The motion for clarification (App. 5) was filed in response to nearly identical language in an order issued on April 22, 2002. App. 4:1. The May 2002 order was issued in response to the motion for clarification. See App. 6:1, 2. (U)

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." FISC Rule 11. (U)

3. The FISC's May 2002 Opinion. The FISC explained the reasons for its order in a lengthy opinion. At the outset, the FISC identified "the issue that is before this Court" as "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." App. 6:3 at 4 n.1 (emphasis in original). However, the FISC expressly declined to address that issue, explaining that it would "not reach the question of whether the FISA may be used primarily for law enforcement purposes." *Id.* at 6 n.2. Instead, the FISC held that "[t]he question before the Court involves straightforward application of the FISA as it pertains to minimization procedures," and explained that it had "decided this matter by applying the FISA's standards for minimization procedures defined in § 1801(h) and § 1821(4) of the Act." *Id.*

at 4, 6 n.2. Thus, the Court did not significantly address or interpret the USA Patriot Act.[8] (U)

The FISC explained that it was relying on minimization standards because "the FISA's definition of minimization procedures has not changed, and [the March 2002 Procedures] cannot be used by the government to amend the Act in ways Congress has not." App. 6:3 at 22. The FISC explained its conclusions as follows:

> Given our experience in FISA surveillances and searches, we find that these provisions in sections II.B and III [of the Department's March 2002 Procedures], particularly those which authorize criminal prosecutors to advise FBI intelligence agents on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are designed to enhance the acquisition, retention and dissemination of

---

[8] The FISC's only significant reliance on the USA Patriot Act was to make the new procedures more restrictive than procedures that governed prior to the Act. Prior intelligence sharing procedures governed consultations between intelligence agents and prosecutors, but not consultations between intelligence agents and law enforcement agents. See App. 7. The FISC's order, however, applies at least in part to law enforcement agents because it uses the term "law enforcement officials" rather than "prosecutors." In response to a motion for clarification (App. 5), the FISC explained that "[t]he Court uses, and intended to use, the term 'law enforcement officials'" in its opinion and order "in conjunction with the source and context from which it originated, i.e., the recent amendments to the FISA." App. 6:1 at 2 (referring to 50 U.S.C. §§ 1806(k), 1825(k)). The FISC stated that "[t]he 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." *Ibid.* (U)

> 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 [FISA's minimization provisions, 50 U.S.C.] § 1801(h) and § 1821(4).

Ibid. (emphasis added by the FISC); see also *id.* at 23, 25. Thus, the FISC concluded that the Department's March 2002 Procedures violated FISA's minimization standards because they authorized searches and surveillance "for law enforcement purposes" rather than "foreign intelligence purposes." Yet the FISC never explained the textual or other basis for this dichotomy between foreign intelligence and law enforcement, and it expressly declined even to consider whether FISA itself authorizes searches or surveillance primarily for a law enforcement purpose. (U)

SUMMARY OF ARGUMENT (U)

1. The FISC's order in this case, and its May 2002 opinion and order, which substantially reject the Department's March 2002 Intelligence Sharing Procedures, rest on a fundamental misapplication of FISA and the USA Patriot Act. The most striking aspect of the FISC's decision is its express refusal even to consider the meaning of the USA Patriot Act. App. 6:3 at 6 n.2. By relying solely on FISA's "minimization" provisions for its rulings, the FISC effectively held that the USA Patriot Act

made no change in the Department's authority to coordinate between intelligence and law enforcement officials. Indeed, the FISC explained that it was modifying the Department's March 2002 Procedures to "reinstate the bright line used in [the Department's] 1995 procedures, on which the Court has relied." *Id.* at 27. That holding was plainly wrong: The USA Patriot Act provides expressly for increased coordination and was clearly intended to alter the standards that previously governed such coordination. (U)

The FISC's decision cannot be sustained as an application of FISA's minimization standards. Those standards require the government to follow procedures in conducting a search or surveillance that are "reasonably designed" to "minimize" the acquisition of nonpublic information concerning unconsenting U.S. persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1), 1821(4)(A). Minimization procedures are designed to limit the acquisition, retention, and dissemination of information that is not otherwise subject to collection under FISA. They may not be used to prevent the government from seeking information that FISA clearly permits it to obtain, or from engaging in consultations that FISA clearly permits it to conduct. Accordingly, the FISC erred in relying on minimization

as an independent check on the government's purpose for using FISA and coordination between intelligence and law enforcement officials. (U)

2. The 1978 version of FISA provides, and the USA Patriot Act's recent amendments to the statute confirm, that it may be used to support law enforcement efforts to protect national security from foreign threats. In its original form, FISA authorized electronic surveillance for "the purpose" of obtaining "foreign intelligence information," which was (and is) defined to include information necessary to "protect against" specified foreign threats to national security, such as espionage and international terrorism. 50 U.S.C. § 1801(e)(1). However, the statute has never prescribed the kinds of efforts, law enforcement or otherwise, that may be used to achieve that protection, other than to require that they be lawful. 50 U.S.C. §§ 1806(a), 1825(a). Indeed, FISA's original legislative history recognized that prosecution of spies and terrorists was one legitimate way to protect national security, and that FISA could be used for the purpose of obtaining evidence for such a prosecution. Thus, a prosecution designed to protect national security from foreign threats was not merely an incidental byproduct of electronic surveillance under FISA; it could be the reason for conducting the surveillance. (U)

Despite the plain language and legislative history of the 1978 version of FISA, the FISC and other courts generally have not interpreted it to permit electronic surveillance (or physical searches) primarily to obtain evidence for a prosecution. These decisions pay insufficient heed to the language of FISA. If this Court agrees with those cases, however, FISA may still be used primarily to obtain evidence for a prosecution as long as the statute is also being used for a significant non-law enforcement foreign intelligence purpose. A purpose may be "significant" regardless of the existence or importance of any other purpose. (U)

Under either approach, the FISC erred in denying the FISA application in this case, and in modifying the Department's March 2002 Intelligence Sharing Procedures. If FISA may be used for the purpose of obtaining evidence for a prosecution specifically designed to protect national security, then consultations conducted in furtherance of such a prosecution are obviously permissible. Indeed, such consultations are affirmative evidence of a purpose to obtain foreign intelligence information. In any event, however, such consultations could not render a non-law enforcement purpose "insignificant." That is because the significance of a purpose to obtain foreign intelligence information is not affected by the existence or strength of a

purpose to obtain evidence for law enforcement, even if the law enforcement purpose provides the primary motive for using FISA. (U)

3. FISA and the USA Patriot Act, as interpreted herein, are constitutional. Under the Supreme Court's decision in *United States* v. *United States District Court (Keith)*, 407 U.S. 297 (1972), it is the nature of the threat, not the nature of the government's response to that threat, which determines the constitutionality of FISA searches and surveillance. Thus, there is no constitutional basis for distinguishing between law enforcement efforts and other means of protecting this country against foreign spies and terrorists. Where the government's purpose is to protect national security, its choice among otherwise lawful methods for achieving the protection does not implicate the Fourth Amendment. (U)

If this Court rejects that argument, FISA may still be used primarily to collect evidence as long as the government has a "significant" non-law enforcement purpose for conducting the search or surveillance. Prior to FISA, every court of appeals to consider the issue upheld unilateral Executive Branch surveillance where the government's "primary purpose" was to obtain foreign intelligence. Given the extensive protections in FISA, including the requirements for judicial review and approval

of applications before searches or surveillance may occur, and regular congressional oversight, the change from "primary" to "significant" purpose does not make a FISA search or surveillance unreasonable. (U)

ARGUMENT (U)

I. THE FISC ERRED IN USING "MINIMIZATION" PROVISIONS TO LIMIT THE PURPOSE OF FISA SEARCHES AND SURVEILLANCE AND CONSULTATIONS BETWEEN INTELLIGENCE AND LAW ENFORCEMENT OFFICIALS (U)

Contrary to the FISC's conclusion, minimization procedures do not provide an independent basis for limiting the purpose of FISA searches or surveillance, or consultations between intelligence and law enforcement officials. Under FISA, "minimization procedures" are defined to be

> 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 [or 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.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A). These standards do not contemplate limits on the acquisition of information that is otherwise subject to collection under the statute. Rather, like their counterparts in Title III, they are designed to minimize the acquisition of information that is not otherwise subject to collection under the statute. See *Scott* v. *United States*, 436

U.S. 128 (1978) (interpreting minimization standards of Title III, 18 U.S.C. § 2510(5)). As the House Report underlying FISA explains, "[b]y minimizing acquisition, the committee envisions, for example, that in a given case, where A is the target of a wiretap, after determining that A's wife is not engaged with him in clandestine intelligence activities, the interception of her calls on the tapped phone, to which A is not a party, probably ought to be discontinued as soon as it is realized that she rather than A was the party." House Report 55; see S. Rep. No. 95-701, 95th Cong., 2d Sess. (1978), at 37-38 [hereinafter Senate Intelligence Report]. Thus, minimization governs the implementation of surveillance to ensure that acquisition (and retention and dissemination) of information is not overbroad in relation to the surveillance's authorized purpose and scope; but minimization has nothing whatsoever to do with defining the authorized purpose and scope of a surveillance.[9] (U)

---

[9] The FISC's May 17 opinion may be read to suggest that we agreed with its authority to regulate the purpose of searches and surveillance, and consultations between intelligence and law enforcement officials, under the rubric of minimization. See, *e.g.*, App. 6:3 at 8. That is clearly not the case. See App. 1:3 at 30 n.7. The FISC acknowledged our objection to its reliance on minimization at the July 19, 2002 hearing on the FISA application in this case. (A transcript of the July 19 hearing has not yet been prepared.) Although the FISC's May 2002 Order suggests that the FISC intends to regulate intelligence investigations whether or not FISA is being used, we do not believe that the FISC intends to regulate intelligence investigations prior to the use of FISA. (U)

Indeed, FISA's minimization standards are more generous than those in Title III, because they require minimization only "consistent with" the government's "need to obtain, produce, and disseminate foreign intelligence information." See House Report 56 ("given the nature of the intelligence gathering, minimizing acquisition should not be as strict as under" Title III). Thus, the government is required to take minimization steps only to the extent that those steps do not interfere with its basic entitlement under FISA to acquire, retain, and disseminate foreign intelligence information. Cf. *Scott*, 436 U.S. at 140 ("there are surely cases, such as the one at bar, where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable."). (U)

Even if minimization could be used to limit the purpose of FISA searches and surveillance, or to restrict coordination between intelligence and law enforcement officials, the FISC still erred. As discussed in Argument II, *infra*, FISA contains specific provisions that govern the "purpose" of searches and surveillance and the "coordinat[ion]" between intelligence and law enforcement officials. Thus, even if minimization could be used to regulate purpose or coordination, it clearly cannot do so in a way that conflicts with FISA's purpose and coordination provisions themselves. The statute must be read as a whole.

See, *e.g.*, *United States* v. *Morton*, 467 U.S. 822, 828 (1984). Thus, the meaning of FISA's purpose and coordination provisions, as originally enacted and as modified by the USA Patriot Act, was unavoidably before the FISC, as it is now before this Court. (U)

II. CONSULTATIONS TO COORDINATE LAW ENFORCEMENT AND INTELLIGENCE EFFORTS TO PROTECT NATIONAL SECURITY FROM FOREIGN THREATS CANNOT JUSTIFY DENIAL OF A FISA APPLICATION (U)

A. FISA May Be Used Primarily, or Exclusively, to Obtain Evidence for a Prosecution Designed to Protect the United States Against Foreign Spies and Terrorists. (U)

1. Since its enactment in 1978, FISA has authorized searches or surveillance where the primary or a significant "purpose of the [search or surveillance] is to obtain foreign intelligence information." 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B). Thus, distinguishing one purpose from another under FISA depends initially on the meaning of the term "foreign intelligence information." The statute defines that term to include

> 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.

50 U.S.C. § 1801(e)(1). (U)

Under this definition, information is foreign intelligence information only if it is relevant or necessary to help the United States protect against certain specified threats, including attack, sabotage, terrorism, and espionage committed by foreign powers or their agents. Thus, information concerning purely domestic threats to the United States - *e.g.*, information concerning Timothy McVeigh's plan to bomb the Oklahoma City Federal Building - is not foreign intelligence information. Correspondingly, information concerning foreign activities that do not threaten national security - *e.g.*, an international fraud scheme - is also not foreign intelligence information. However, information about an al Qaeda conspiracy to bomb New York is foreign intelligence information because it concerns international terrorism committed by a foreign power and is needed to protect against that threat. See 50 U.S.C. § 1801(a)-(c); House Report at 47-50.[10] (U)

---

[10] A second definition of "foreign intelligence information," in 50 U.S.C. § 1801(e)(2), includes information relevant or necessary to "the national defense of the United States" or "the conduct of the foreign affairs of the United States." This definition, which generally involves information referred to as "affirmative" or "positive" foreign intelligence

Although "foreign intelligence information" must be relevant or necessary to "protect" against the specified threats, the statutory definition does not limit how the government may use the information to achieve that protection. In other words, the definition does not discriminate between protection through diplomatic, economic, military, or law enforcement efforts, other than to require that those efforts be "lawful." 50 U.S.C. §§ 1806(a), 1825(a).[11] Thus, for example, where information is relevant or necessary to recruit a foreign spy or terrorist as a double agent, that information is "foreign intelligence information" if the recruitment effort will "protect against" espionage or terrorism. Similarly, where information is relevant or necessary to prosecute a foreign spy or terrorist, that

---

rather than "protective" foreign intelligence or "counterintelligence" information, is not at issue in this case, and is rarely the object of surveillances in which purpose issues arise, because affirmative intelligence information is usually not evidence of a crime. See Senate Intelligence Report at 11 & n.4. (U)

[11] The statute provides that no "information acquired pursuant to" a search or surveillance may be "disclosed for law enforcement purposes" or "used in a criminal proceeding" absent the Attorney General's permission. 50 U.S.C. §§ 1806(b), 1825(c). This provision is designed to ensure that an aggrieved party receives notice that he was subject to FISA searches or surveillance so that he may seek suppression of evidence obtained or derived from FISA before it is used in a "trial" or other proceeding. 50 U.S.C. §§ 1806(c) and (e), 1825(d) and (f). See House Report 88-90. (U)

information is also "foreign intelligence information" if the prosecution will "protect against" espionage or terrorism. (U)

Prosecution is often a most effective means of protecting national security. For example, the recent prosecution of Ahmed Ressam, who was charged with attempting to destroy Los Angeles International Airport, protected the United States by incapacitating Ressam himself from committing further attacks, and by deterring others who might have contemplated similar action. Moreover, as a result of his conviction and sentence, Ressam agreed to cooperate with the government and provided information about the training that he received at an al Qaeda camp overseas. That kind of prosecution thus protects the United States directly, by neutralizing a threat, and indirectly, by generating additional foreign intelligence information. The same is true of the recent prosecution of Robert Hanssen: By far the best source of intelligence on Hanssen's espionage activities is Hanssen himself; and the government gained access to Hanssen only as a result of his capture, prosecution, and plea agreement. (U)

In sum, information is "foreign intelligence information" if it is relevant or necessary to the ability of the United States to protect against threats posed by foreign spies and terrorists. Such protection may be achieved in several ways, including by prosecuting the spy or terrorist. Information therefore may be

"foreign intelligence information" solely by virtue of its importance to such a prosecution. Where the government conducts a search or surveillance for the purpose of obtaining information for use in such a prosecution, it satisfies FISA's standards. (U)

2. The USA Patriot Act confirms this understanding of FISA by incorporating the definition of "foreign intelligence information" into new provisions of the statute that authorize consultations and coordination between federal law enforcement officers and intelligence officers who conduct FISA searches or surveillance. 50 U.S.C. §§ 1806(k), 1825(k). The Patriot Act's "coordination" amendment to FISA provides:

> (1) Federal officers who conduct [electronic surveillance or physical searches] 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;
>
> (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 [50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)] or the entry of an order under [50 U.S.C. §§ 1805 and 1824].

50 U.S.C. §§ 1806(k), 1825(k) (emphasis added). (U)

This amendment authorizes "consult[ation]" and "coordinat[ion]" between intelligence and law enforcement officers. It defines the scope of authorized coordination by incorporating verbatim the foreign threats to national security that are specified in the definition of "foreign intelligence information" - attack, sabotage, terrorism, and espionage committed by foreign powers or their agents. Compare 50 U.S.C. §§ 1806(k)(1)(A)-(C) and 1825(k)(1)(A)-(C), with 50 U.S.C. § 1801(e)(1)(A)-(C). The amendment authorizes consultations to coordinate the government's various "efforts to investigate or protect" against such threats. Thus, consultations concerning purely domestic threats to national security (Timothy McVeigh), or foreign activities that do not threaten national security (international fraud schemes), are not within the scope of the coordination amendment. Consultations concerning an al Qaeda conspiracy to bomb New York, however, are within the scope of the provision, for the same reason that information concerning such a conspiracy is "foreign intelligence information." (U)

By allowing intelligence and law enforcement officials to "coordinate efforts to investigate or protect" against the specified threats, the amendment recognizes that law enforcement investigations and efforts, as well as intelligence investigations and efforts, can "protect" against those threats.

It therefore reaffirms the original meaning of "foreign intelligence information" to include information that will "protect" the United States against espionage and terrorism through both intelligence and law enforcement efforts. (U)

In keeping with that idea, the amendment also provides that authorized coordination "shall not preclude" the certification or finding of a purpose to obtain foreign intelligence information. By definition, coordination authorized by the amendment must be in furtherance of a purpose to investigate or protect against the threats specified in the definition of "foreign intelligence information" - *e.g.*, an al Qaeda conspiracy to bomb New York. Such coordination cannot "preclude" a purpose to obtain foreign intelligence information because it is affirmative evidence of such a purpose. (U)

3. The legislative history of FISA confirms what its plain language provides. When it enacted FISA in 1978, Congress understood that prosecution may be used to protect national security against foreign threats, and that FISA may be used to obtain evidence for such a prosecution. Indeed, the House Report underlying the original statute provides explicitly that FISA may be used for the purpose of obtaining information and evidence to support such a prosecution. In a lengthy paragraph, the House

Committee directly addressed the precise questions that are presented in this appeal:

> Finally, the term "foreign intelligence information," especially as defined in [50 U.S.C. §§ 1801(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. 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, *see* [50 U.S.C. § 1801(h)]. And no information acquired pursuant to this bill could be used for other than lawful purposes, *see* [50 U.S.C. § 1806(a)]. 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 clandestine intelligence activities, sabotage, and international terrorism can be sought, retained, and used pursuant to this bill.

House Report at 49 (emphasis added). (U)

The first underlined passage above makes clear that FISA does not discriminate between law enforcement and non-law enforcement protective methods. It is enough that the government intends to "protect" national security from foreign threats, and that the information sought is "necessary" to achieve that

protection.[12] In other words, as the House Report elsewhere explains, "evidence of certain crimes like espionage [and terrorism] would itself constitute 'foreign intelligence information,' as defined, because it is necessary to protect against clandestine intelligence activity [and international terrorism] by foreign powers or their agents." House Report at 62. (U)

The second underlined passage above makes the same point even more clearly: By explaining that prosecution is one way to protect national security, and by stating that "evidence" of espionage or terrorism offenses may be "sought" as well as retained and used pursuant to FISA, the Report shows that FISA may be used for the purpose of obtaining such evidence, with the intent that it be offered in a prosecution designed to protect national security from foreign threats. Thus, prosecution of spies and terrorists is not merely an incidental byproduct of a FISA search or surveillance. Rather, obtaining evidence for such a prosecution may be the purpose of the surveillance. See Senate Intelligence Report at 10-11 & n.4.[13] (U)

---

[12] By "necessary," Congress meant "important and required," or fulfilling a "significant need," not that the information be absolutely essential. See House Report 47. (U)

[13] There are some apparently contrary indications in the legislative history. For example, the House Report "recognize[d]

Indeed, while the 1978 legislative history correctly predicts that "prosecution is rarely the objective or the result" of FISA surveillance, and that its "primary purpose * * * is not likely to be the gathering of criminal evidence," House Report 24 n.20, 89 (emphasis added), the legislative history recognizes that FISA allows for that possibility. Indeed, Congress understood that while some FISA surveillance would merely "result in the incidental acquisition of information about crimes," other FISA surveillance "[b]y contrast" would actively "seek[] information needed to detect or anticipate the commission of

---

full well that the surveillance[s] under [FISA] are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it comes to United States persons must be necessary to important national security concerns." House Report at 36; see *id.* at 60; S. Rep. No. 95-604, 95th Cong., 2d Sess. (1978), at 39, 55 [hereinafter Senate Judiciary Report]; Senate Intelligence Report at 41-42, 62. However, read in context, those passages do not undermine the idea that FISA may used to obtain evidence for a prosecution designed to protect national security. For example, after stating that FISA may not be used to gather evidence, but only to protect "important national security concerns," the House Report goes on to explain that "[c]ombating the espionage and covert actions of other nations in this country is an extremely important national concern," and that "[p]rosecution is one way * * * to combat such activities." House Report 36. (U)

The Senate Report underlying the 1994 amendments to FISA, which enacted the statute's provisions authorizing physical searches, does not address the issue. See S. Rep. No. 103-296, 103d Cong., 2d Sess. (1994), at 33-34. (U)

crimes." Senate Intelligence Report at 11 & n.4. The Senate Intelligence Report explains:

> Electronic surveillance for foreign counterintelligence and counterterrorism purposes requires different standards and procedures. 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.

Id. at 10-11 (emphasis added, footnote omitted). This statement reflects that FCI investigations, and the use of FISA within those investigations, may be "designed" for a law enforcement purpose. As the Report further explains, surveillance "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." *Id.* at 11. That statement reflects a recognition that prosecution is one of many legitimate "protective" efforts that FISA may be used to support. Accordingly, insofar as the "purpose" of FISA surveillance is concerned, prosecution is no different than traditional counterintelligence efforts like "'[d]oubling' an agent or feeding him false or useless information," or "[m]onitoring him to discover other spies, their tradecraft and equipment." House Report at 36-37. (U)

Senator Leahy referred to this legislative history to make precisely the same point in describing the USA Patriot Act's "coordination" amendment:

> I proposed and the Administration agreed to an additional provision in Section 505 that clarifies the boundaries for consultation and coordination between officials who conduct FISA search and surveillance and Federal law enforcement officials including prosecutors. Such consultation and coordination is authorized for the enforcement of laws that protect against international terrorism, clandestine intelligence activities of foreign agents, and other grave foreign threats to the nation. Protection against these foreign-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. The Justice Department's opinion cites relevant legislative history from the Senate Intelligence Committee's report in 1978, and there is comparable language in the House report.

147 Cong. Rec. S10990-02, at S11004 (October 25, 2001) (emphasis added). This statement makes clear that the drafter of the coordination amendment, who was the Chairman of the Senate Judiciary Committee and one of the principal negotiators of the USA Patriot Act, see *id.* at S11054, understood that FISA may be used to obtain evidence for a prosecution designed to protect national security, and indeed that it had always permitted such use. (U)

4. The text and legislative history of FISA's minimization provisions further confirm that "foreign intelligence

information" includes information sought for use in the prosecution of a foreign spy or terrorist. As noted above (Argument I, *supra*), those provisions require reasonable efforts to minimize the acquisition and retention, and prohibit the dissemination, of nonpublic information concerning U.S. persons consistent with the government's need to "obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1), 1821(4)(A). The minimization provisions also provide, "notwithstanding" the rules governing foreign intelligence information, for retention and dissemination (but not acquisition) of "evidence of a crime" for "law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(C). Thus, FISA has two key minimization provisions: One governing "foreign intelligence" and the other governing "evidence of a crime." (U)

However, as the FISC acknowledged, and as the statute's legislative history makes clear, FISA's "crimes" minimization provision applies only to crimes that do <u>not</u> pose a foreign threat to national security - i.e., what the FISC referred to as crimes that are "not related to the target's intelligence or terrorist activities." App. 6:3 at 10 n.4. Thus, for example, the "crimes" provision would apply if electronic surveillance of a spy revealed that the spy had killed his wife, and would permit intelligence officials to disseminate information about the

murder to law enforcement officials for use in a homicide prosecution. See House Report 62 (referring to "a serious crime totally unrelated to intelligence matters"). But the "crimes" provision does not apply to evidence of crimes that do pose a threat to national security - i.e., it does not permit the dissemination to prosecutors of information concerning Ahmed Ressam's terrorism offenses or Robert Hanssen's espionage. House Report 62; App. 6:3 at 10 n.4. (U)

Of course, evidence of crimes that threaten national security is disseminated to prosecutors - not under the "crimes" minimization provision, but under the "foreign intelligence" minimization provision. The FISC appeared to recognize this point in approving Part II.A of the Department's March 2002 Intelligence Sharing Procedures. See App. 6:2. In any event, Congress clearly appreciated the point when it enacted FISA in 1978. As the House Report put the matter in explaining why the "crimes" minimization provision does not apply to evidence of espionage and terrorism offenses:

> As noted above, *see* [50 U.S.C. § 1801(e)(1)], evidence of certain crimes like espionage would itself constitute "foreign intelligence information," as defined, because it is necessary to protect against clandestine intelligence activity by foreign powers or their agents. Similarly, much information concerning international terrorism would likewise constitute evidence of crimes and also be "foreign intelligence information," as defined. This paragraph [the "crimes"

> minimization provision] does not relate to information, even though it constitutes evidence of a crime, which is also needed by the United States in order to obtain, produce or disseminate foreign intelligence information.

House Report at 62. (U)

Apart from confirming that "foreign intelligence information" includes evidence of espionage and terrorism offenses, the minimization provisions also confirm that FISA may be used for the purpose of obtaining such evidence. Unlike the "crimes" provision, which authorizes retention and dissemination of evidence incidentally obtained through FISA, the "foreign intelligence" provision also authorizes acquisition of information. Compare 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A), with 50 U.S.C. §§ 1801(h)(3) and 1821(4)(C). Accordingly, the government may not conduct surveillance (exclusively) to acquire evidence of a domestic homicide. It may, however, conduct FISA surveillance to acquire evidence of espionage or international terrorism, because such evidence is foreign intelligence information, and because its use by prosecutors is consistent with the foreign intelligence "need[s]" of the United States. (U)

Indeed, the conclusion is the same whether phrased in the language of minimization or the language of purpose: FISA may not be used to "acquire," or for the (exclusive) "purpose" of

obtaining, evidence for the prosecution of a domestic homicide, because such information is not "foreign intelligence information." But FISA may be used to "acquire," or for the "purpose" of obtaining, evidence for the prosecution of a foreign spy or terrorist, because such information is "foreign intelligence information."[14] (U)

5. Despite the plain language and legislative history of the statute, before the passage of the USA Patriot Act the courts did not endorse the use of FISA to obtain evidence for a prosecution designed to protect national security. Instead of distinguishing, as FISA's text and legislative history do, between protective and non-protective efforts and purposes, they distinguished between law enforcement and non-law enforcement efforts and purposes. These courts treated a law enforcement purpose as automatically precluding a protective purpose, as if the two terms are mutually exclusive. In other words, they treated "foreign intelligence information" as if it does not

---

[14] The FISC erred in concluding that information is "foreign intelligence information" only insofar as it is used by intelligence officials for a non-law enforcement purpose. See App. 6:3 at 25. As noted above, FISA allows dissemination of foreign intelligence information only to the extent that there is a foreign intelligence "need" to do so. Thus, prosecutors may receive such information only because it is foreign intelligence information as disseminated to and used by them - i.e., only because they have an independent foreign intelligence need for the information. (U)

include evidence sought for use in the prosecution of a spy or international terrorist. They held that the "primary purpose" of a FISA search or surveillance must be to obtain "foreign intelligence information" as so defined - i.e., that the primary purpose must be a non-law enforcement purpose. See *United States* v. *Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980) (case applying the "primary purpose" test under pre-FISA standards); *United States* v. *Duggan*, 743 F.2d 59, 78 (2d Cir. 1984); *United States* v. *Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987); *United States* v. *Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States* v. *Johnson*, 952 F.2d 565, 572 (1st Cir. 1992). (U)

Insofar as they reject the idea that FISA may be used to collect evidence for law enforcement efforts to protect against foreign spies and terrorists, we believe that these cases were wrongly decided. However, none of the cases expressly rejected the idea that evidence needed for such a prosecution is "foreign intelligence information." Indeed, none of the cases even discussed the government's purpose for prosecuting, and from all that appears the government never advanced the idea that prosecution may be used to protect national security, or that FISA may be used to obtain evidence for such a prosecution. For example, Attorney General Griffin Bell, who testified at the

suppression hearing in *Truong*, described prosecution only as an "incidental" byproduct of a non-criminal counterintelligence investigation: "Let me say that every one of these counterintelligence investigations involved, nearly all of them that I have seen, involves crime in an incidental way. You never know when you might turn up with something you might want to prosecute." 629 F.2d at 916 n.5. Thus, while these decisions clearly distinguish between "law enforcement" and "foreign intelligence" purposes, they do not squarely address the distinction between law enforcement efforts designed to protect against foreign espionage and terrorism and other law enforcement efforts. (U)

One court of appeals appears to have taken a different approach, albeit in dictum. In *United States* v. *Sarkissian*, 841 F.2d 959 (9th Cir. 1988), the government used FISA wiretap evidence to obtain convictions for offenses arising from an international terrorist plot. Relying on the "primary purpose" test, the defendants challenged the admissibility of the FISA evidence. The court of appeals did not decide whether "the test is one of purpose or primary purpose," because it concluded that both tests were satisfied. *Id.* at 964. The court explained: "We refuse to draw too fine a distinction between criminal and intelligence investigations. 'International terrorism,' by

definition, requires the investigation of activities that constitute crimes." *Id.* at 965. (U)

The court in *Sarkissian* went on to observe that "FISA is meant to take into account [t]he differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations," and stated that "[a]t no point was this case an ordinary criminal investigation." 841 F.2d at 965 (internal quotation omitted). It then cited and described several other cases in which FISA surveillance had been upheld, apparently to illustrate the point that none of them involved "ordinary" investigations: a "conspiracy to manufacture machine guns and silencers for 'Omega-7,' an anti-Castro group"; an "IRA attempt to buy parts for bombs and surface-to-air missiles"; an "Armenian terrorist plot to assassinate [a] Turkish diplomat"; and a case involving "IRA arms smuggling." *Ibid.* (U)

Thus, *Sarkissian* appears to recognize that the important distinction under FISA is not between law-enforcement efforts and non-law enforcement efforts, but between efforts to protect national security from foreign threats (including law enforcement efforts to do so) and other efforts (*e.g.*, efforts to protect against domestic terrorists or international fraud schemes). FISA may not be used primarily to obtain evidence for what *Sarkissian* called "ordinary" prosecutions, but it may be used

primarily (or exclusively) to obtain evidence for prosecutions designed to protect national security from foreign threats. (U)

B. FISA May Be Used Primarily to Obtain Evidence for a Prosecution if the Government Also Has a Significant Non-Law Enforcement Foreign Intelligence Purpose. (U)

At a bare minimum, the difficulty of clearly distinguishing the line between law enforcement purposes and protective national security purposes strongly supports allowing the use of FISA primarily for the purpose of obtaining evidence for a prosecution as long as the government also has a "significant" non-law enforcement purpose for obtaining foreign intelligence information. Moreover, because a purpose to obtain foreign intelligence information may be "significant" regardless of the existence or strength of a purpose to obtain evidence for a prosecution, consultations between intelligence and law enforcement personnel cannot preclude the government's certification of purpose or the FISC's issuance of an authorization order. (U)

1. Until the USA Patriot Act, FISA required that "the purpose" of a search or surveillance be to obtain foreign intelligence information. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (amended). However, the federal courts, including the FISC, generally read "the purpose" to mean "primary purpose." See, *e.g.*, *Duggan*, 743 F.2d at 78. Under the "primary purpose"

regime, courts reviewed consultations between intelligence and law enforcement officials in an investigation to determine whether the government's primary purpose for the investigation, and for the FISA search or surveillance conducted within the investigation, was to obtain information for law enforcement. The more consultations that occurred, the more likely courts were to find an improper law enforcement purpose. (U)

For example, the court of appeals in *Truong* determined the government's primary purpose by examining the consultations between intelligence agents (who were conducting the surveillance) and prosecutors (who eventually brought the charges against Truong). The court of appeals agreed with the district court's decision to suppress evidence obtained from electronic surveillance after consultations and coordination had shifted the government's "primary purpose" to prosecution (629 F.2d at 916):

> In this case, the district court concluded that on July 20, 1977, the investigation of Truong had become primarily a criminal investigation. Although the Criminal Division of the Justice Department had been aware of the investigation from its inception, until summer the Criminal Division had not taken a central role in the investigation. On July 19 and July 20, however, several memoranda circulated between the Justice Department and the various intelligence and national security agencies indicating that the government had begun to assemble a criminal prosecution. On the facts of this case, the district court's finding that July 20 was the critical date when the investigation became primarily a criminal investigation was clearly correct. (U)

As explained below, the USA Patriot Act eliminated the "primary purpose" standard by enacting a "significant purpose" standard, and thereby also eliminated *Truong*'s approach to weighing intelligence and law enforcement purposes to determine which is "primary." Nonetheless, as part of its May 2002 order, the FISC adopted a new Rule 11 that is entirely in keeping with *Truong* and is at odds with the USA Patriot Act. It provides: "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." As the discussion below makes clear, Rule 11 cannot be reconciled with the USA Patriot Act. This Court should therefore direct the FISC to rescind the rule. See, *e.g.*, *Carlisle* v. *United States*, 517 U.S. 416, 426-427 (1996); *Bank of Nova Scotia* v. *United States*, 487 U.S. 250, 254-255 (1988). (U)

2. The "significant purpose" test differs from the "primary purpose" test. A purpose is "significant" when it has or is "likely to have influence or effect," or when it is "important." *Meriam-Webster's Collegiate Dictionary* 1091 (10th ed. 1998). Thus, as long as the desire to obtain foreign intelligence information has "influence or effect" on the decision to use FISA, it satisfies the "significant purpose" test. In practice,

it may be easier to recognize a significant purpose by considering its opposite: A purpose is "significant" when it is not "insignificant" - i.e., when it is not trivial, incidental, or pretextual. Cf. *United States* v. *Brito*, 136 F.3d 397, 407 (5th Cir. 1998); *United States* v. *Roberts*, 913 F.2d 211, 220 (5th Cir. 1990). (U)

By requiring only a "significant" purpose to obtain foreign intelligence information, Congress allowed for other purposes, including a purpose to obtain evidence for use in a prosecution, to be the "primary" reason for conducting a search or surveillance. Cf. *United States v. Soto-Silva*, 129 F.3d 340, 347 (5th Cir. 1997) (finding that defendant who maintained house for "primary purpose" of taking care of her mother also maintained house for "significant purpose" of distributing marijuana). Members of Congress who voted for and against the USA Patriot Act discussed and understood that the "significant purpose" amendment would allow the government to use FISA primarily to collect evidence for use in a criminal prosecution. See 147 Cong. Rec. S11021 (Oct. 25, 2001) (statement of Senator Feingold); see also *id.* at S11025 (statement of Senator Wellstone); *id.* at S10593 (Oct. 11, 2001) (statements of Senators Leahy and Cantwell); see also *id.* at S10591 (Oct. 11. 2001) (statement of Senator Feinstein). (U)

The "significant purpose" standard also differs from the "primary purpose" standard because it eliminates the need for courts routinely to compare and weigh competing purposes for using FISA. Unlike "primary," the adjective "significant" is not an inherently relative or comparative term. A purpose may be "significant," in the sense of having "influence or effect," regardless of whether there are other purposes present. Thus, to determine whether a "significant" purpose for using FISA is to obtain foreign intelligence information, courts need not examine the extent of any purpose to obtain evidence for a prosecution. (U)

The legislative history of the USA Patriot Act confirms that Congress intended to eliminate the need to compare purposes. In explaining why the "significant purpose" amendment was enacted, the House Report underlying H.R. 2975 explained:

> Presently, a FISA certification request can only be used where foreign intelligence gathering is the sole or primary purpose of the investigation as interpreted by the courts. This requires law enforcement to evaluate constantly the relative weight of criminal and intelligence purposes when seeking to open a FISA investigation and thereafter as it proceeds.

H.R. Rep. 107-236(l), 107th Cong., 1st Sess., at 60 (Oct. 11, 2001). Thus, the significant purpose amendment was enacted to

relieve the government from the obligation to weigh competing intelligence and law enforcement purposes. (U)

Because the "significant purpose" test does not require comparison of intelligence and law enforcement purposes, it also does not require routine review of consultations between intelligence and law enforcement officials. As in *Truong*, such consultations may be relevant to establish that a law enforcement purpose is "primary," but they are very unlikely to establish that an explained and certified purpose to obtain foreign intelligence information is not "significant." The certification typically is made by the Director of the FBI, and is approved by the Attorney General. Whatever transpires in consultations between line attorneys or agents conducting particular investigations, these high-ranking officials determine the government's actual purpose for using FISA. (U)

That is particularly true where, as here, the consultations fall under the rubric of the USA Patriot Act's "coordination" amendment. Even if the coordination amendment is not read to reaffirm the theory that FISA may be used to obtain evidence for a prosecution designed to protect national security, as argued above, it nonetheless provides explicitly that law enforcement and intelligence officials "may consult" with one another to coordinate efforts to protect against espionage and terrorism,

among other matters. It also provides that such consultations "shall not preclude the certification" of a significant foreign intelligence purpose "or the entry of an order" authorizing a FISA search or surveillance. At a minimum, therefore, the coordination amendment reinforces the conclusion that where the FISA application demonstrates a significant foreign intelligence purpose, authorized consultations and coordination between intelligence and law enforcement officials cannot undermine that purpose. (U)

Indeed, where law enforcement officials seek evidence to prosecute a spy or terrorist, intelligence officials will always (or almost always) have at least a significant purpose to obtain the same information. As the FISC acknowledged in its opinion,

> most information intercepted or seized has a dual character as both foreign intelligence information and evidence of a 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.

App. 6:3 at 10; see *id.* at 25 ("the information collected through FISA surveillances and searches is both foreign intelligence information and evidence of crime, depending on who is using it"); see also House Report 49, 62. Thus, even where consultations with law enforcement officials influence the

purpose or scope of a FISA search or surveillance, the information sought will still be "foreign intelligence information," and a significant purpose will still be to obtain such information for use in non-law enforcement efforts to protect the United States. (U)

To be sure, there may be cases in which review of consultations is appropriate even under the "significant purpose" standard. For example, where the FISA application on its face (or other information before the FISC) strongly suggests an intentionally false certification of purpose, the safe harbor would not preclude judicial review of the consultations that may have occurred among the officials involved. Cf. *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks* v. *Delaware*, 438 U.S. 154 (1978)). Absent such a strong suggestion, however, routine judicial review of consultations between intelligence and law enforcement officials, as required by the FISC's new Rule 11, is inappropriate. Cf. *United States* v. *Armstrong*, 517 U.S. 456, 465-466 (1996) (court may not order discovery in support of selective prosecution claim absent a threshold showing that the government has acted with both discriminatory effect and "a discriminatory purpose"). (U)

C. The FISC Erred in Denying in Part the FISA Application in This Case. (U)

Whether this Court accepts the argument that FISA may be used to obtain evidence for a prosecution designed to protect national security, as set forth in Part II.A, or the alternative argument that it may be used to obtain evidence for a prosecution if the government also has a significant non-law enforcement purpose, as set forth in Part II.B, the FISC clearly erred in limiting consultations between intelligence and law enforcement officials in this case. As the FISA application makes clear, the government is pursuing a traditional intelligence investigation and other intelligence efforts against the target in order to protect against international terrorism, and it is also pursuing a criminal investigation and other law enforcement efforts against him for the same protective purpose. The consultations envisioned in this case are all intended to coordinate these intelligence and law enforcement efforts to investigate and protect against international terrorism. Thus, by definition, they tend to reveal a purpose to protect national security, whether through traditional intelligence efforts or through law enforcement efforts. If this Court accepts the contention that information sought for a prosecution to protect national security is foreign intelligence information, then these consultations

would demonstrate that the FISA surveillance is designed to obtain such information. They would be affirmative evidence of a foreign intelligence purpose. (U)

Alternatively, if this Court rejects that argument, the consultations still could not undermine the significance of a non-law enforcement foreign intelligence purpose. The application explains and certifies that a significant purpose of the surveillance is to monitor the target's terrorist network in this case. There is no basis whatsoever for questioning that assertion on this record. The fact that the government also intends to prosecute in no way detracts from the significance of the non-law enforcement purpose. (U)

The government's efforts to investigate and protect against international terrorism in this case would be aided substantially by adherence to the March 2002 Procedures. At present, the government is conducting two parallel and largely overlapping investigations of the same person, but is compelled to use two separate law enforcement agencies in two separate Departments of the government. That is obviously an inefficient approach. Yet, as the FISA application explains, it is required to ensure that the government does not lose its ability to use FISA in the intelligence investigation. (U)

Although the use of two separate law enforcement agencies to investigate the same target is not a common method of insuring the availability of FISA - other methods include using separate squads of FBI agents with the FISC or another entity serving as the "wall" to regulate consultations between the squads - the difficulty it illustrates is by no means uncommon. Reports from the Executive and Legislative Branches of government alike have found that the "primary purpose" test as applied by the FISC has inhibited necessary coordination between intelligence and law enforcement officials. See IV AGRT Report, Chapter 20, at 721-734; General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited* (July 2001) (GAO-01-780) (hereinafter GAO Report). As the GAO report summarized matters (GAO Report at page 3):

> Coordination between the FBI and the Criminal Division has been limited in those foreign counterintelligence cases where criminal activity is indicated and [FISA] surveillance and searches have been, or may be, employed. A key factor inhibiting this coordination is the concern over how the Foreign Intelligence Surveillance Court or another federal court might rule on the primary purpose of the surveillance or search in light of such coordination.

These findings, although disturbing, should not be surprising: No large organization can achieve a complex mission unless its related parts are allowed to work together. (U)

Two of the FISC's requirements have particularly stifled coordination in this case. First, there is the FISC's warning that prosecutors may not advise intelligence officials in a way that results in "direction or control" of the intelligence investigation. This has chilled the substance of consultations between intelligence and law enforcement officials. Second, there is the rule that prosecutors may not even meet or discuss the case with intelligence agents without first inviting OIPR to participate, and the related requirement that OIPR cannot allow the meeting to occur without its participation unless it is "unable" to do so. This "chaperone" requirement has made it difficult for any consultations to occur at all. The next paragraphs discuss these limitations as they apply in this case. (U)

1. The Ban on "Direction or Control". (U)

As we argued in the FISC in support of the March 2002 Procedures, the "direction or control" test has no textual support in FISA or any published decision interpreting the statute. App. 1:3 at 26-30. More importantly, as a practical matter, the FISC has often equated "direction or control" with the giving of any advice designed to "enhance," rather than merely to "preserve," the possibility of prosecution. See, *e.g.*,

App. 5 at 2-6; AGRT Report at 727-734. As we argued in the FISC (App. 1:3 at 27):

> providing advice, including advice designed to enhance the possibility of a criminal prosecution, cannot be equated with "direction or control." For example, prosecutors may suggest an investigative strategy, propose the use of investigative techniques other than FISA (*e.g.*, consensual monitoring), and advise on interview tactics, all without taking over the investigation as a whole or the FISA activity conducted within it.

In its May 2002 opinion, the FISC stated simply that it was "not persuaded" by these arguments. App. 6:3 at 23. When we pointed out the apparent inconsistency between the FISC's description of the advice that prosecutors may give and its continued reliance on the distinction between "preserving" and "enhancing" advice (App. 5 at 2-6), the FISC reaffirmed its reliance on the distinction (App. 6:1 at 1-2). (U)

2. The Chaperone Requirement. (U)

In sum, the FISC has misinterpreted FISA, and has done so in a way that inhibits necessary coordination. The USA Patriot Act, which the FISC effectively ignored, expressly authorizes coordination between intelligence and law enforcement officials. The Act reflects Congress' recognition that the country and its people can no longer afford a fragmented, blinkered, compartmentalized response to international terrorism and espionage. The FISC has refused to give effect to the Act and the changes it made. This Court should not allow that refusal to stand. (U)

III. AS AMENDED BY THE USA PATRIOT ACT, FISA IS CONSTITUTIONAL (U)

A. FISA May Be Used Primarily, or Exclusively, to Obtain Evidence for a Prosecution Designed to Protect the United States Against Foreign Spies and Terrorists. (U)

1. When Congress enacted FISA in 1978, it understood the constitutional significance of authorizing surveillance for the purpose of obtaining evidence to be used against foreign spies and terrorists. The Senate Intelligence Committee's Report on FISA gave the constitutional question "close scrutiny" because the Committee recognized that FISA "departs from ordinary criminal law enforcement procedures in several ways." Senate Intelligence Report at 11.[15] The Committee concluded, however, that those departures were "'reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens,' as required by the Supreme Court's leading decision in this field, *United States* v. *United*

---

[15] Similarly, Members of Congress understood that the USA Patriot Act could raise constitutional questions, and intended for the courts to resolve the meaning of the statute as written. See 147 Cong. Rec. S10547-01, at S10589 (Oct. 11, 2001) (statement of Senator Edwards); *id.* at S10593 (statement of Senator Cantwell). As Senator Leahy put the matter, the USA Patriot Act "adopts 'significant purpose,' and 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.'" *Id.* at S11004 (Oct. 25, 2001). (U)

States District Court (Keith), 407 U.S. 297, 323 (1972)." *Id.* at 14. (U)

Today, as in 1978, the *Keith* case remains the leading decision of the Supreme Court in this area. In *Keith*, the Court addressed the "delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval." 407 U.S. at 299. The defendants in *Keith* were domestic terrorists, and the Court therefore did not address "the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* at 308. Nor did *Keith* involve "any question or doubt as to the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest" under Title III. *Ibid.* Thus, *Keith* addressed the validity of warrantless electronic surveillance for the purpose of protecting against domestic threats to national security (*e.g.*, Timothy McVeigh).[16] (U)

The Court in *Keith* held that a warrant is required for domestic security surveillance, but that more flexible standards

---

[16] In *Keith* itself, the prosecution stemmed from "the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan." 407 U.S. at 299. (U)

could apply to the issuance of such a warrant. The Court explained the reasons for its conclusion (407 U.S. at 322):

> We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

In light of these "potential distinctions between Title III criminal surveillances and those involving the domestic security," the Court suggested that "Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III." *Ibid.* (U)

Keith's emphasis on the need for flexibility applies with even greater force to surveillance (or searches) directed at foreign threats to national security. As the Senate Intelligence Committee Report on FISA explained, quoting from *Keith*, "[f]ar more than in domestic security matters, foreign counterintelligence investigations are 'long range' and involve 'the interrelation of various sources and types of information.'"

Senate Intelligence Report at 16. Surveillance directed at foreign threats also requires deferential standards of judicial review because it involves an area in which the President, as "Commander-in-Chief and as the Nation's organ for foreign affairs," *Chicago & Southern Air Lines v. Waterman*, 333 U.S. 103, 109 (1948), exercises "very delicate, plenary and exclusive power," *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936), and in which judicial intervention "is rarely proper." *Haig v. Agee*, 453 U.S. 280, 293 (1981).[17] (U)

These concerns, which justify the use of FISA's different standards, do not recede merely because the government intends to protect national security through law enforcement rather than non-law enforcement efforts. On the contrary, *Keith* makes clear that it is the nature of the threat, not the nature of the government's response to the threat, that determines the constitutionality of national security surveillance. Whether the government intends to prosecute a foreign spy or recruit him as a double agent (or use the threat of the former to accomplish the latter), the investigation will often be long range, involve the

---

[17] Both before and after *Keith*, every federal court of appeals squarely to consider the question held that the government may conduct warrantless foreign intelligence surveillance. See, *e.g.*, *Truong*, *supra*. The constitutionality of FISA has also been upheld by every court to consider the issue. See, *e.g.*, *Duggan*, *supra*. (U)

interrelation of various sources and types of information, and present unusual difficulties because of the special training and support available to foreign enemies of this country. As the Senate Intelligence Committee's Report explained, quoting from a 1955 study on espionage:

> The problems of crime detection in combating espionage are not ordinary ones. Espionage is a crime which succeeds only by secrecy. Moreover, spies work not for themselves or private organized crime "syndicates," but as agents of national states. Their activities are therefore likely to be carefully planned, highly organized, and carried on by techniques skillfully designed to prevent detection.

Senate Intelligence Report 13 (quoting Fund for the Republic, *Digest of the Public Record of Communism in the United States* 29 (New York 1955)). As the country learned on September 11, the same is true of many international terrorist groups. (U)

Nothing in *Keith* suggests that the availability of more relaxed constitutional standards for a search or surveillance depends on the absence of a law enforcement purpose. On the contrary, the contrast drawn by the Court between domestic security surveillance and surveillance of "ordinary crime" or "more conventional types of crime" shows that the Court understood that domestic security surveillance focuses on crime, albeit crime of an unusual sort. See also 407 U.S. at 308, 310 (contrasting surveillance of "crimes unrelated to the national

security interest," which are governed by Title III, with surveillance "of those who plot unlawful acts against the Government"). The Court's statement that the "emphasis" of security surveillance is "often" on "prevention" is factually accurate, but also allows for the possibility of an emphasis on prosecution, at least where the prosecution will protect against a "future crisis or emergency." As the Senate Intelligence Report put it, FISA surveillance "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." Senate Intelligence Report at 11; see also House Report at 24 n.20, 89. (U)

2. The foregoing analysis is consistent with more recent Supreme Court decisions addressing searches conducted for "special needs." In *City of Indianapolis* v. *Edmond*, 531 U.S. 32 (2000), the Court struck down suspicionless highway checkpoints designed to apprehend drug dealers, holding that the government's "general crime control ends" in fighting drug trafficking are not a "special need" justifying lower Fourth Amendment standards. *Id.* at 40, 43. The Court made clear, however, that there are "special" law-enforcement needs that may justify more relaxed standards. (U)

For example, the Court in *Edmond* reviewed and approved prior decisions upholding special needs seizures conducted for the purposes of capturing illegal immigrants and stopping intoxicated motorists, despite the fact that "[s]ecuring the border and apprehending drunk drivers are, of course, law enforcement activities, and law enforcement officers employ arrests and criminal prosecutions in pursuit of these goals." 531 U.S. at 42 (citing *Michigan Dept. of State Police* v. *Sitz*, 496 U.S. 444 (1990), and *United States* v. *Martinez-Fuerte*, 428 U.S. 543 (1976)). Indeed, in response to criticism from the dissent, the Court made the point more explicitly:

> THE CHIEF JUSTICE's dissent erroneously characterizes our opinion as resting on the application of a "non-law-enforcement primary purpose test." Our opinion nowhere describes the purposes of the *Sitz* and *Martinez-Fuerte* checkpoints as being "not primarily related to criminal law enforcement." Rather, our judgment turns on the fact that the primary purpose of the Indianapolis checkpoints is to advance <u>the general interest in crime control</u>.

Id. at 44 n.1 (emphasis added). Thus, while the "general interest in crime control" does not justify a departure from ordinary Fourth Amendment standards, a "special" interest concerning a particular type of crime may do so. As explained above, crimes such as espionage and international terrorism,

which represent foreign threats to national security, are "special" in the constitutional sense.[18] (U)

B. FISA May Be Used Primarily to Obtain Evidence for a Prosecution if the Government Also Has a Significant Non-Law Enforcement Foreign Intelligence Purpose. (U)

In light of the foregoing argument, it is crystal clear that the Constitution permits FISA to be used where a "significant purpose" of the search or surveillance is to protect national security from foreign threats through non-law enforcement efforts. The Department explained the constitutionality of the "significant purpose" test for FISA in a letter sent to Congress in support of the USA Patriot Act. The letter is included as an attachment to the Memorandum of Law at App. 1:3, and is summarized below. (U)

Relying on *Keith* and other decisions of the Supreme Court, the Department's letter maintains that "the primary purpose test is more demanding than that called for by the Fourth Amendment's reasonableness requirement." Letter 13. It explains that

---

[18] In *Ferguson* v. *City of Charleston*, 121 S. Ct. 1281 (2001), the Supreme Court struck down a non-consensual drug testing policy that applied to pregnant women seeking medical care at a State hospital. It relied on the fact that the "primary purpose of the [drug testing] program[] was to use the threat of arrest and prosecution in order to force women into treatment" for cocaine abuse. *Id.* at 1292. But the Court did not disapprove *Edmond*, or retreat from the statement in *Edmond* that there may be "special law enforcement needs" that justify more relaxed Fourth Amendment standards. (U)

"because the executive can more fully assess the requirements of national security than can the courts, and because the President has a constitutional duty to protect the national security, the courts should not deny him the authority to conduct intelligence searches even when the national security purpose is secondary to criminal prosecution." *Ibid.* Thus, although most courts have adopted the primary purpose test "to police the line between legitimate foreign intelligence searches and pure domestic law enforcement operations," the letter concludes that the test is too strict in part because "the concerns of government with respect to foreign policy will often overlap with those of law enforcement." Letter 11, 12. (U)

The letter closes by observing that "[e]ven at the time of [FISA's] passage in 1978," there was a "growing realization that 'intelligence and criminal law enforcement tend to merge in [the] area' of foreign counterintelligence and counterterrorism." Letter 14 (quoting Senate Intelligence Report at 11). The letter opines that that merger has continued to the point where "the fine distinction between foreign intelligence gathering and domestic law enforcement has broken down" (*ibid.*):

> Terrorists, supported by foreign powers or interests, had lived in the United States for substantial periods of time, received training within the country, and killed thousands of civilians by hijacking civilian airliners. The [September 11] attack, while

> coordinated from abroad, was carried out from within the United States itself and violated numerous domestic criminal laws. Thus, the nature of the national security threat, while still involving foreign control and requiring foreign counterintelligence, also has a significant domestic component, which may involve domestic law enforcement.

Based on these developments, the letter concludes that "Fourth Amendment doctrine, based as it is ultimately upon reasonableness, will have to take into account that national security threats in the future cannot be so easily cordoned off from domestic criminal investigation." *Ibid.* (U)

Finally, there is one additional reason why the letter's conclusion is not in tension with the result in decisions such as *Truong*, which adopted the "primary purpose" test for warrantless surveillance conducted prior to the enactment of FISA. 629 F.2d at 914 n.4. Even if *Truong* was correctly decided, and the Constitution requires a "primary" intelligence purpose for unilateral Executive Branch surveillance, a "significant" intelligence purpose for FISA surveillance conducted with the prior approval of an Article III court would be reasonable and therefore constitutional under the Fourth Amendment. The reasonableness standard depends on all of the protections for privacy afforded as part of a search or surveillance. Assuming that restrictions on the government's purpose for conducting a

search do serve to protect privacy,[19] reductions in those purpose-related protections are reasonable given the added protections afforded by FISA. (U)

[19] The assumption that restrictions on the purpose of FISA searches or surveillance protect privacy is open to question in light of the fact that intelligence and law enforcement officials seek the same information. Cf. *Chagnon* v. *Bell*, 642 F.2d 1248, 1262 n.25 (D.C. Cir. 1980) ("Official surveillance, whether its purpose be criminal investigation or intelligence gathering, risks infringement of constitutional interests"). (U)

CONCLUSION (U)

It is respectfully submitted that the judgment of the FISC in this case, including its adoption of the opinion and order of May 17, 2002, and its new Rule 11, should be vacated, and the case remanded with directions to the FISC to grant the FISA application as submitted. (U)

JOHN ASHCROFT
Attorney General

LARRY D. THOMPSON
Deputy Attorney General

THEODORE B. OLSON
Solicitor General

DAVID S. KRIS
Associate Deputy Attorney General

JAMES A. BAKER
Counsel for Intelligence Policy

JONATHAN L. MARCUS
Attorney Advisor
Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
(202) 514-2882

Dated: August 21, 2002