

No. 02-001

IN THE UNITED STATES FOREIGN INTELLIGENCE
SURVEILLANCE COURT OF REVIEW

IN RE APPEAL FROM JULY 19, 2002 OPINION
OF THE UNITED STATES FOREIGN INTELLIGENCE
SURVEILLANCE COURT

BRIEF ON BEHALF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES
UNION, CENTER FOR DEMOCRACY AND TECHNOLOGY, CENTER
FOR NATIONAL SECURITY STUDIES, ELECTRONIC PRIVACY
INFORMATION CENTER, ELECTRONIC FRONTIER FOUNDATION,
AND OPEN SOCIETY INSTITUTE
IN SUPPORT OF AFFIRMANCE

ANN BEESON
JAMEEL JAFFER
STEVEN R. SHAPIRO
American Civil Liberties Union
125 Broad Street
New York, NY 10004
Telephone: (212) 549-2601
Facsimile: (212) 549-2651

JAMES X. DEMPSEY
Center for Democracy and Technology
1634 Eye Street, NW, Suite 1100
Washington, DC 20006

Additional Counsel Listed Inside Cover

September 19, 2002

KATE MARTIN
Center for National Security Studies
1120 19th Street, NW, 8th Floor
Washington, DC 20036

DAVID L. SOBEL
Electronic Privacy Information Center
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009

LEE TIEN
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Counsel for *Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

I. STATEMENT OF THE CASE 1

 A. The FISA Court’s May 17 Order and Opinion 2

II. FISA DOES NOT AUTHORIZE LAW ENFORCEMENT OFFICIALS TO CONTROL SURVEILLANCE FOR CRIMINAL INVESTIGATIONS 6

 A. The structure of the surveillance statutes reflects a constitutionally based distinction between intelligence gathering and law enforcement 6

 1. Electronic surveillance poses extraordinary privacy risks, which Congress has addressed through Title III’s rigorous requirements 7

 2. Title III has always regulated electronic surveillance in law enforcement investigations undertaken to protect the national security. 8

 3. FISA governs surveillance for foreign intelligence purposes, and not surveillance to gather evidence of criminal conduct... 10

 4. The procedures of Title III and FISA are substantially different, and FISA was not intended to be an alternative to Title III in criminal cases affecting the national security 12

 B. The Patriot Act confirmed and clarified the boundaries between the foreign intelligence and law enforcement spheres..... 15

 1. The Patriot Act’s significant purpose amendment clarified that foreign intelligence need not be the exclusive purpose of surveillance conducted under FISA’s authority 15

2.	The Patriot Act’s “significant purpose” amendment must be read in conjunction with the Patriot Act’s coordination amendment	19
3.	The FISC order contains a set of objective rules that implement the Patriot Act by preventing law enforcement officials from initiating or controlling and directing FISA surveillances.....	22
III. FISA IS UNCONSTITUTIONAL TO THE EXTENT IT AUTHORIZES SURVEILLANCE WHOSE PRIMARY OR EXCLUSIVE PURPOSE IS TO OBTAIN EVIDENCE FOR A CRIMINAL PROSECUTION.....		
	A. Ordinary Fourth Amendment requirements apply to all searches having law enforcement as their primary or exclusive purpose	26
	B. The Supreme Court’s “special needs” cases confirm that the Fourth Amendment’s ordinary requirements apply to all searches whose primary or exclusive purpose is criminal investigation	31
	C. The government’s theory would suspend ordinary Fourth Amendment requirements not only in espionage and terrorism investigations but in any investigation related to national security	36
IV. ANY EXPANSION IN FISA SURVEILLANCE AUTHORITY WOULD IMPLICATE NUMEROUS OTHER CONSTITUTIONAL INTERESTS		
	A. Allowing FISA to be invoked in criminal investigations would raise Fourth Amendment and Due Process concerns because FISA fails to require notice and denies individuals any meaningful opportunity to challenge illegal surveillance	40
	B. Any extension of FISA would chill protected speech and therefore raise serious First Amendment concerns	44
CONCLUSION.....		45

TABLE OF AUTHORITIES

CASES:

Abel v. United States, 362 U.S. 217 (1960)..... 35

Bartnicki v. Vopper, 532 U.S. 514 (2001)..... 45

Berger v. New York, 388 U.S. 41 (1967)..... 7

City of Indianapolis v. Edmond, 531 U.S. 32 (2000) 32, 33

Detroit Free Press v. Ashcroft, No. 02-1437, 2002 WL 1972919, at *1 (6th Cir. Aug. 26, 2002)..... 39

Ferguson v. City of Charleston, 532 U.S. 67 (2001)..... 31, 34

Franks v. Delaware, 438 U.S. 154 (1978)..... 42

Fuentes v. Shevin, 407 U.S. 67 (1972) 40

Griffin v. Wisconsin, 483 U.S. 868 (1987) 31

Grosjean v. Am. Press Co., 297 U.S. 233 (1936)..... 39

Harris v. United States, 122 S.Ct. 2406 (2002)..... 23

Katz v. United States, 389 U.S. 347 (1967)..... 7

Richards v. Wisconsin, 520 U.S. 385 (1997)..... 40

Skinner v. Railway Labor Executives’ Assn., 489 U.S. 602 (1989) 31

Treasury Employees v. Von Raab, 489 U.S. 656 (1989)..... 31

United States ex rel. Attorney General v. Delaware & Hudson Co., 213 U.S. 366 (1909) 23

United States v. Brown, 484 F.2d 418 (5th Cir. 1973) 24, 30

United States v. Butenko, 494 F.2d 593 (3d Cir.)..... 30

<i>United States v. Cavanagh</i> , 807 F.2d 787 (9 th Cir. 1987)	12
<i>United States v. Duggan</i> , 743 F.2d 59 (2d Cir. 1984)	26, 42
<i>United States v. Johnson</i> , 952 F.2d 565 (1 st Cir. 1991)	27
<i>United States v. Nicholson</i> , 955 F.Supp. 588 (E.D.Va. 1997).....	42
<i>United States v. Pelton</i> , 835 F.2d 1067 (4 th Cir. 1987).....	12, 27
<i>United States v. Robel</i> , 389 U.S. 258 (1967).....	2
<i>United States v. Truong Dinh Hung</i> , 629 F.2d 908 (4 th Cir. 1980)	29
<i>United States v. United States Dist. Court (“Keith”)</i> , 407 U.S. 297 (1972). 8, 27, 28, 44	
<i>Vernonia School District 47J v. Acton</i> , 515 U.S. at 653	31
<i>Wilson v. Arkansas</i> , 514 U.S. 927 (1995).....	40
<i>Zweibon v. Mitchell</i> , 516 F.2d 594 (D.C. Cir.1975).....	passim
STATUTES:	
18 U.S.C. § 2510 <i>et seq.</i>	1, 8
18 U.S.C. § 2511(3).....	10, 15
18 U.S.C. § 2516(o).....	9
18 U.S.C. § 2518(3)(a).....	8,13
18 U.S.C. § 2518(3)(d)	13
18 U.S.C. § 2518(5).....	13
18 U.S.C. § 2518(8).....	13, 40
18 U.S.C. § 2518(8)(d)	13

18 U.S.C. § 2518(9).....	13
18 U.S.C. § 3013a(b)	40
18 USC § 2511(3)	10
50 U.S.C. § 1801 <i>et seq.</i>	1
50 U.S.C. § 1801(b)(2)(A).....	13
50 U.S.C. § 1804(a)(7)(B)	16
50 U.S.C. § 1805(a)(3)(A).....	13
50 U.S.C. § 1805(a)(3)(B)	14
50 U.S.C. § 1805(e)	14
50 U.S.C. § 1806(c)	41
50 U.S.C. § 1806(e)	42
50 U.S.C. § 1806(f).....	14, 42
50 U.S.C. §§ 1821-29	12
50 U.S.C. §1806(k).....	20
Pub. L. 90-351, tit. III, 82 Stat. 211 (1968).....	passim
Pub. L. 101-298, sec. 3(b), 104 Stat. 203 (1989).....	9
Pub. L. 104-132, sec. 434, 110 Stat. 1274 (1996)	9
Pub. L. 99-508, 100 Stat. 1851, 1855-56 (1986).....	9
Pub. L. No. 107-56, 115 Stat. 272 (2001)	passim
S. Rep. 90-1097, at 67 (1968).....	7, 8

MISCELLANEOUS:

*The USA PATRIOT Act In Practice: Shedding Light on the FISA Process:
Hearing Before United States Senate Committee on the Judiciary, 107th
Cong. (Sept. 10, 2002)..... 11, 19, 38, 43*

I. STATEMENT OF THE CASE

This case of first impression raises the question whether federal law enforcement officials can use the Foreign Intelligence Surveillance Act of 1978 (“FISA”), 50 U.S.C. § 1801 *et seq.*, to initiate, control or direct surveillances for criminal investigation. In the court below, the government sought a judicial ruling that FISA can be used where the primary or even exclusive purpose of surveillance is to gather evidence of criminal conduct. Appropriately, the Foreign Intelligence Surveillance Court (“FISC”) rejected the government’s attempt to invoke FISA for electronic surveillance that for over thirty years has been governed by an entirely different statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), 18 U.S.C. § 2510 *et seq.*, which applies to wiretaps in criminal investigations. As the FISC noted, the government’s construction of FISA would allow an end-run around ordinary Fourth Amendment requirements. Neither the text of FISA as amended by the USA PATRIOT Act (“Patriot Act”), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), nor twenty years of judicial interpretation supports this result. While FISA now allows coordination, consultation and information sharing between intelligence and law enforcement officials, it does not authorize surveillance whose primary or exclusive purpose is law enforcement. Indeed, expanding the scope of secret

surveillance under FISA would violate the Fourth Amendment and the Due Process guarantees of the Fifth Amendment, and would jeopardize the First Amendment right to engage in lawful public dissent. Though amici readily acknowledge the need to protect the nation in the current crisis, “[i]t would indeed be ironic if, in the name of national defense, we would sanction the subversion of . . . those liberties . . . which make[] the defense of the Nation worthwhile.” *United States v. Robel*, 389 U.S. 258, 264 (1967).¹

A. The FISA Court’s May 17 Order and Opinion

This case arises from the government’s attempt to disturb the careful balance wrought by Congress and the courts between individual privacy rights and executive power to obtain foreign intelligence.² The government relies on the Patriot Act, which amended FISA after the September 11, 2001 attacks. Prior to the amendments, the government could obtain a FISA surveillance order only upon a certification that “the purpose” of the surveillance was to gather foreign intelligence. The Patriot Act amended this language to require a certification that “a significant purpose” of the surveillance is to gather foreign intelligence. The government argues that this subtle change in language (1) provides it with authority to use FISA

¹ Amici’s interests in this appeal are described in the attached Motion for Leave to File Amici Curiae Brief in Support Of Affirmance.

² This brief focuses principally on electronic surveillance. Importantly, however, the same arguments that amici raise with respect to electronic surveillance apply to physical searches as well, as the FISC’s May 17 Opinion recognizes.

orders primarily – or even exclusively – for law enforcement purposes and (2) permits law enforcement officials to initiate, direct and control FISA surveillances to bolster criminal investigations that otherwise would be subject to Title III.

The current controversy arose in March of this year, when the government asked the Foreign Intelligence Surveillance Court to adopt a set of procedures for all FISA cases, past, present and future. Although styled as “Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI,” the March 2002 procedures in fact sought to implement the Attorney General’s expansive new interpretation of FISA. Under the proposed procedures, FISA surveillance could be initiated, directed, and controlled by law enforcement officials. In effect, the government sought to institutionalize an end-run around the Fourth Amendment’s ordinary requirements – an end-run that would be available to it in any criminal investigation related to national security.

The FISC correctly rejected the government’s audacious reinterpretation of FISA.³ *See In Re All Matters Submitted to the Foreign*

³ The government did not appeal the FISC’s May 17 decision. In July, the government submitted an apparently unrelated FISA application. While the FISC (Baker, J.) granted the July application, the FISC denied the government’s request that the July application be subject to the unmodified March 2002 procedures, instead ruling that the surveillance order would be subject to the March 2002 procedures as

Intelligence Surveillance Court, Memorandum Opinion, May 17, 2002 (hereinafter, “May 17 Opinion”), at 4. Citing the “troubling” history of recent government failures clearly to describe the law enforcement aspects of FISA cases, *id.* at 16, the FISC specifically rejected the section of the proposed procedures that would have allowed law enforcement officials to initiate or control FISA searches, *see id.* at 26-27. The FISC modified that portion of the proposed procedures to substitute two paragraphs concerning consultations between law enforcement officials and intelligence agents. *See id.* In accordance with FISA and the Fourth Amendment, the two substitute paragraphs adopted by the FISC establish objective rules intended to permit coordination and consultation but also to prevent the government from using FISA primarily for law enforcement purposes. The FISC fully approved the government’s proposed procedures that allow the FBI to disseminate to law enforcement officers all information collected in intelligence investigations. *See id.* at 26.

The FISC correctly recognized that the Patriot Act’s promotion of coordination and information-sharing were not meant to – and constitutionally could not – obviate the distinction between surveillance for law enforcement and intelligence purposes. As the FISC concluded, given

modified by the FISC’s May 17 Opinion. (The FISC apparently issued an opinion related to the July application that has not been published.) The government now appeals from the FISC’s July decision.

the relaxed standards for secret surveillance under FISA, authorization for FISA orders must be based on an assessment of the government's purpose and cannot extend to surveillance controlled by law enforcement officials for law enforcement purposes.

This case does not present the issue whether information collected in FISA surveillances and searches can be used in criminal cases. Nor does it present the issue whether law enforcement officials and intelligence officers can coordinate their efforts in situations where they have overlapping interests in the same target. In the Patriot Act, Congress made changes to FISA and Title III that support essentially unlimited sharing of information between intelligence and law enforcement officers. But those amendments assumed and preserved the distinction between surveillance authorization for criminal investigations and intelligence investigations.

The FISC based its decision on the minimization procedures and its ruling can be affirmed under that reasoning alone. As amici explain in detail below, the FISC's ruling is also consistent with FISA's new "significant purpose" language, considered in the context of other Patriot Act changes and the entire statutory scheme for surveillance authorization under Title III and FISA. *See* Section II, *infra*. However if this Court declines to affirm on statutory grounds, the Court must conclude that the significant purpose

amendment rendered FISA unconstitutional. As explained below, the Constitution prohibits FISA surveillance where the government's primary purpose is criminal investigation. *See* Sections III and IV, *infra*.

II. FISA DOES NOT AUTHORIZE LAW ENFORCEMENT OFFICIALS TO CONTROL SURVEILLANCE FOR CRIMINAL INVESTIGATIONS

A. The structure of the surveillance statutes reflects a constitutionally based distinction between intelligence gathering and law enforcement

To support its push for expanded surveillance powers under FISA, the government advances in its brief a two-part argument – that law enforcement is a foreign intelligence function within the definition of FISA and that intelligence collection under FISA can be initiated, directed, and controlled by law enforcement officials. Neither argument is supported by the text or history of FISA, Title III, or the Patriot Act. As explained more fully below, this history establishes three principles important to the present dispute: (1) criminal investigation and foreign intelligence gathering are subject to different constitutional and statutory requirements; (2) surveillance whose primary purpose is criminal investigation, including criminal investigation for national security purposes, has always been governed by Title III; (3) to deter abuse, any departure from normal Fourth Amendment requirements for foreign intelligence gathering must be carefully limited.

1. Electronic surveillance poses extraordinary privacy risks, which Congress has addressed through Title III's rigorous requirements

Since the seminal case of *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court has recognized that electronic surveillance constitutes a search subject to the privacy protections inherent in the Fourth Amendment, *see id.* at 353. Indeed, because of the broad and general scope of electronic surveillance, the Court has stated that “[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices.” *Berger v. New York*, 388 U.S. 41, 63 (1967). The privacy threat inherent in electronic surveillance is especially pernicious because of the high likelihood that innocent communications will be intercepted.

The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope – without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations.

Id. at 65 (Douglas, J., concurring).

Responding to the Supreme Court's holding in *Katz*, and to widespread reports of abusive government surveillance, *see* S. Rep. 90-1097, at 67 (1968) (noting “the widespread use and abuse of electronic surveillance techniques”), Congress passed Title III in 1968 to implement uniform procedures to govern electronic surveillance in criminal

investigations. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, tit. III, 82 Stat. 211, adding 18 U.S.C. § 2510 *et seq.* Title III imposes stringent requirements on electronic surveillance conducted in criminal investigations. One of these requirements, reflecting Fourth Amendment structures, is that law enforcement agents may not conduct such surveillance except on a judge’s finding of probable cause that a serious crime has been or is about to be committed. *See* 18 U.S.C. § 2518(3)(a) (1994). In passing Title III, Congress clearly sought to “safeguard the privacy of innocent persons” while simultaneously promoting more effective control of crime. *See* Pub. L. No. 90-351, tit. III, 82 Stat. 211 (legislative findings); *see also United States v. United States Dist. Court (“Keith”)*, 407 U.S. 297, 302 (1972).

2. Title III has always regulated electronic surveillance in law enforcement investigations undertaken to protect the national security.

From the beginning, Title III procedures have governed criminal investigations for national security purposes. In 1968, espionage, sabotage and treason came at the top of the list of predicate crimes to which the Title III procedures applied. The Senate referred to these as “the offenses that fall within the national security category.” S. Rep. 90-1097, at 67 (1968). Over time, as terrorism emerged as a greater concern, Congress added terrorism

offenses to the list of Title III predicate crimes, so that now essentially all terrorism crimes are covered by Title III. In the Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1851, 1855-56, Congress added to Title III a number of terrorism-related provisions, including section 1203 (relating to hostage taking), section 32 (relating to the destruction of aircraft), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), parts of section 1472 of title 49 (referring to aircraft piracy), and the section in chapter 65 relating to destruction of an energy facility. In the Biological Weapons Anti-Terrorism Act of 1989, Congress added section 175 of title 18 (relating to biological weapons) as a Title III predicate. *See* Pub. L. 101-298, sec. 3(b), 104 Stat. 203. In the Antiterrorism and Effective Death Penalty Act of 1996, Congress added to Title III the visa and passport fraud provisions. *See* Pub. L. 104-132, sec. 434, 110 Stat. 1274, adding 18 U.S.C. § 2516(o).

This process continued in the Patriot Act, which added seven additional terrorism crimes as predicate offenses under Title III. Section 201 of the Patriot added the following to the list of terrorism offenses as predicate crimes under Title III:

(q) any criminal violation of section 229 [of title 18] (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism);

115 Stat. 278. Congress, even as it amended FISA in the Patriot Act, intended Title III to govern the collection of evidence for prosecuting terrorism offenses threatening national security.

3. FISA governs surveillance for foreign intelligence purposes, and not surveillance to gather evidence of criminal conduct

Congress recognized when it adopted Title III that foreign intelligence collection was distinct from law enforcement. Thus, when Congress enacted Title III, it left untouched the President's claimed authority to gather foreign intelligence information related to national security.⁴ This other, exempted sphere of foreign intelligence clearly was not meant to govern criminal investigations undertaken to protect national security: Having just created procedures for collecting evidence to prosecute crimes against the national security, Congress would not have said in the same statute that it did not limit the powers of the President to collect evidence to prosecute those crimes. Yet that is what the Attorney General now claims.

The Executive Branch's extremely broad interpretation of its foreign intelligence gathering authority led to widespread and well-documented

⁴ The Title III disclaimer provided: "Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or the hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities." 18 U.S.C. § 2511(3) (as enacted by Title III). Subsection 2511(3) was repealed in 1978 by FISA, which struck § 2511(3) and added § 2511(2)(e) and (f). *See* Pub. L. 95-511, sec. 201(b) and (c).

abuses. *See Zweibon v. Mitchell*, 516 F.2d 594, 616 n.53, 618, 634, 635 n.107 (D.C. Cir.1975); S. Rep. 95-604—Part 1, at 7-9, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908-10; *The USA PATRIOT Act In Practice: Shedding Light on the FISA Process: Hearing Before United States Senate Committee on the Judiciary*, 107th Cong. (Sept. 10, 2002) (hereinafter, “2002 FISA Hearings”) (Statement of Sen. Patrick Leahy) (noting that those illegitimately targeted had “included a Member and staff of the United States Congress, White House domestic affairs advisors, journalists, and many individuals and organizations engaged in no criminal activity but, like Dr. Martin Luther King, who expressed political views threatening to those in power.”); *id.* (Testimony of Kenneth C. Bass, III) (“During the Vietnam War [the President’s national security power] was invoked to undertake warrantless surveillance of a number of anti-war individuals and groups on a belief that their activities threatened national security. In some cases those surveillance targets were domestic groups with no provable ties to any foreign interest.”).

Responding to these abuses, Congress passed FISA in 1978. Like the motivation behind Title III, FISA’s purpose was twofold: “Congress sought to accommodate and advance both the government’s interest in pursuing legitimate intelligence activity and the individual’s interest in freedom from

improper government intrusion.” *United States v. Cavanagh*, 807 F.2d 787, 789 (9th Cir. 1987) (emphasis added); *see also United States v. Pelton*, 835 F.2d 1067, 1074 (4th Cir. 1987) (FISA passed to create “secure framework . . . [for] electronic surveillance for foreign intelligence purposes within the context of this Nation’s commitment to privacy and individual rights” (quoting S. Rep. No. 95-604, at 15, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916)), *cert. denied*, 486 U.S. 1010 (1988). However, FISA’s procedural safeguards are significantly more relaxed than those that Title III established for criminal cases protecting the national security.

4. The procedures of Title III and FISA are substantially different, and FISA was not intended to be an alternative to Title III in criminal cases affecting the national security

Through the enactment of Title III and FISA, Congress created two separate authorization schemes for government surveillance – one for criminal investigation and one for foreign intelligence purposes.⁵ In Title III, Congress enacted those standards it believed were necessary to meet Fourth Amendment requirements for using electronic surveillance in criminal investigations. In addition to requiring probable cause to believe that the subject is committing, has committed, or is about to commit one of a

⁵ The focus in this discussion is on the differences between FISA’s electronic surveillance provisions and Title III. However, there are similar distinctions between the FISA’s physical search provisions, *see* 50 U.S.C. §§ 1821-29, and those that govern physical searches conducted in the course of ordinary law enforcement investigations, *see* Fed. R. Crim. P. 41.

list of offenses, *see* 18 U.S.C. § 2518(3)(a), Title III surveillance requires probable cause to believe that the facility to be surveilled is being used by the target “in connection with the . . . offense,” *see* 18 U.S.C. § 2518(3)(d). Under Title III, surveillance targets must eventually be notified that their privacy has been compromised, *see* 18 U.S.C. § 2518(8)(d), and targets who later face criminal prosecution can obtain the application under which the interception was approved, *see* 18 U.S.C. § 2518(9). Title III surveillance orders are also normally limited to thirty days, subject to renewal only under the same requirements as govern initial applications. *See* 18 U.S.C. § 2518(5).

As the FISC noted in its May 17 Memorandum Opinion, *see* May 17 Opinion at 9-10, FISA surveillance offers the executive branch significantly greater latitude. *See* Attached Chart (comparing requirements under the two statutes). First, FISA surveillance orders require only probable cause to believe that the target is a foreign power or agent thereof, *see* 50 U.S.C. § 1805(a)(3)(A), and, if directed at a U.S. person, probable cause to believe that the target is, for example, “knowingly engage[d] in clandestine intelligence gathering activities,” 50 U.S.C. § 1801(b)(2)(A). Unlike Title III orders, FISA orders do not require probable cause to believe that the target is engaging in criminal activity. Second, FISA orders require

probable cause to believe that the facility to be surveilled is being used by the target, *see* 50 U.S.C. § 1805(a)(3)(B), but they require no showing that the target is using the facility in connection with a crime. Third, FISA contains no provision for notifying targets – or non-targets whose communications might have been intercepted incidentally – that their privacy has been compromised. Fourth, FISA orders have a term of 90 days which may be extended up to a full year in certain cases. *See* 50 U.S.C. § 1805(e). Fifth, FISA surveillance targets who later face criminal prosecution usually are not provided the application on which the surveillance was based and sometimes cannot even obtain intercepted communications through discovery, and are therefore severely limited in their ability to challenge the legality of the surveillance after the fact. *See* 50 U.S.C. § 1806(f).⁶

Reading the two statutes together, it is clear that Congress intended that Title III’s strong standards should govern electronic surveillance whose purpose is to protect national security through criminal prosecutions. It

⁶ Another provision of FISA, not amended by the Patriot Act, reinforces the conclusion that law enforcement officials cannot initiate FISA surveillances. Section 104(a)(7) of FISA provides that every FISA application shall include a certification from an Executive Branch official “employed in the area of national security.” This certification can be made only by the Assistant to the President for National Security Affairs or an executive branch official designated by the President “from among those officers employed in the area of national security or defense.” Pursuant to Executive Order 12139, only seven officials have been designated to make that determination: the Secretaries and Deputy Secretaries of State and Defense, and the Director and Deputy Director of Central Intelligence, and the Director of the FBI. The Attorney General is not among them, a clear indication that the FISA authority is to be exercised only when an official other than a prosecutor certifies that there is an intelligence purpose to undertake the surveillance.

would have been illogical for Congress to have created in FISA separate, *weaker* standards to govern the same government action.⁷ Because the rules that govern surveillance under FISA are more relaxed than those that govern Title III surveillance (and, indeed, because FISA does not reflect safeguards that the Fourth Amendment mandates for criminal investigations), it is not surprising that the government seeks to define the foreign-intelligence sphere as capaciously as possible. But the boundaries of the foreign-intelligence sphere must be determined not by executive whim but by statutory and constitutional principle. As discussed below, the USA Patriot Act did nothing to disrupt the longstanding distinction between foreign intelligence and law enforcement surveillance.

B. The Patriot Act confirmed and clarified the boundaries between the foreign intelligence and law enforcement spheres

1. The Patriot Act's "significant purpose" amendment clarified that foreign intelligence need not be the exclusive purpose of surveillance conducted under FISA's authority

Prior to the enactment of the Patriot Act in October 2001, the government could obtain FISA surveillance orders only on a certification

⁷ The definition of "foreign intelligence information" in FISA is very similar to the exemption language in section 2511(3) of Title III as originally enacted, *compare* 50 U.S.C. § 1801(e) *with* 18 U.S.C. § 2511(3) (as enacted by Title III), which reinforces that foreign intelligence under FISA covers activity not governed by Title III – namely, methods of protecting the national security other than through criminal prosecution.

that “the purpose” of the surveillance was foreign intelligence.⁸ As amended by the Patriot Act, FISA now allows the government to obtain surveillance orders on a certification that “a significant purpose” of the surveillance is foreign intelligence. 50 U.S.C. § 1804(a)(7)(B). Contrary to the government’s view, this change was not meant to dissolve the boundaries between the foreign intelligence and law enforcement spheres. Rather, the change was intended only to clarify that the government can obtain a FISA surveillance order even if foreign intelligence is not its exclusive purpose.

Congress’ amendments to FISA responded to two linked concerns, one relating to FISA authorizations and one relating to coordination and sharing between law enforcement and intelligence officials. The background to these concerns is laid out in a July 2001 GAO report to Congress. See United States General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited*, GAO-01-780 (July 2001), available online at <<http://www.gao.gov/new.items.d01780.pdf>>. The GAO report makes clear that, beginning in the 1990s, there developed considerable confusion and friction within the Justice Department regarding FISA’s authorization requirements and the permissible extent of cooperation between intelligence

⁸ Courts had interpreted the “purpose” language to require that foreign intelligence gathering be the “primary purpose” of surveillance. See Section III, *infra*.

and law enforcement officials. While law enforcement officers wanted intelligence officers to provide them with criminal evidence uncovered in the course of FISA surveillances, intelligence officers had become concerned that providing such information to law enforcement officers would lead the FISC to reject applications to renew surveillance orders on the grounds that foreign intelligence was no longer the primary purpose. *See id.* at 11. The GAO found that, in the view of Criminal Division officials, “the primary purpose test had been, in effect, interpreted by the FBI and Office of Intelligence Policy Review to mean ‘exclusive’ purpose.” *Id.* at 14. Efforts to correct the problem apparently made it worse. Procedures adopted by the Attorney General in 1995 “triggered coordination problems,” and some within the Justice Department remained concerned that coordination between intelligence officers and law enforcement officers would either jeopardize criminal prosecutions or lead the FISC to deny applications or renewal requests. *Id.* at 19. To the consternation of the FISC, these conflicts also led to a serious series of incidents in which the government withheld from the court and even misstated to the court information about the extent of law enforcement interest in the targets of FISA surveillance. *See* May 17 Opinion at 16-17.

The Patriot Act responded to these concerns with two amendments: the significant purpose amendment to section 104(a)(7)(B), Pub. L. 107-56, Section 218, 115 Stat. 291, and the coordination amendment to section 106, Pub. L. 107-56, Section 504, 115 Stat. 364, discussed below. The significant purpose amendment clarifies that the government can obtain a FISA order even if foreign intelligence is not its exclusive purpose; the aim of this amendment was to put to rest the mistaken interpretation identified by the GAO as a major source of conflict between the law enforcement and intelligence officers. In addition, the amendment clarifies that applications to renew surveillance orders need not be denied if criminal prosecution becomes one of the government's goals during the course of an investigation.

The Justice Department's July 26, 2002 response to a letter from the House Judiciary Committee confirms that the significant purpose amendment responded mainly to concern with coordination between law enforcement and intelligence investigations:

The "primary purpose" standard . . . has had its principal impact not with respect to the government's certification of purpose concerning the use of FISA itself, but rather in the FISC's tolerance of increased law enforcement investigations and activity connected to, and coordinated with, related intelligence investigations in which FISA is being used. Given the court's approach in this area, the "significant purpose" amendment has the potential for helping the government to coordinate its intelligence and law enforcement efforts to protect the United

States from foreign spies and terrorists.

Enclosure to Letter to Hon. John Conyers, Jr., from Assistant Attorney General Daniel J. Bryant, dated July 26, 2002, available online at <http://www.fas.org/irp/news/2002/08/doj072602.pdf>. Senators' statements at hearings recently convened by the Senate Judiciary Committee reinforce that the significant purpose amendment was not intended to dissolve the pre-existing boundary between authorization for foreign intelligence and law enforcement surveillance. *See* 2002 FISA Hearings (Statement of Sen. Patrick Leahy) (“[I]t was not the intent of these amendments to fundamentally change FISA from a foreign intelligence tool into a criminal law enforcement tool”); *id.* (Statement of Sen. Dianne Feinstein) (“I don’t believe any of us ever thought that the answer to the problem was to merge Title III and FISA”); *id.* (Statement of Sen. Arlen Specter) (“The word ‘significant’ was added to make it a little easier for law enforcement to have access to FISA material, but not to make law enforcement the primary purpose”).

2. The Patriot Act’s significant purpose amendment must be read in conjunction with the Patriot Act’s coordination amendment

The Patriot Act’s significant purpose amendment must be read in conjunction with the Act’s coordination amendment, which authorizes

increased coordination and sharing between law enforcement and intelligence officers. The coordination amendment was meant to clarify that intelligence and criminal investigators can and should coordinate and consult with one another to protect against threats to national security, and that such coordination should not in itself prevent the government from meeting the foreign intelligence purpose test. The coordination amendment states:

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against -

- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
- (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105.

115 Stat. 364, adding 50 U.S.C. §1806(k).

Even the mere fact of the amendment shows that Congress did not intend use of FISA for a primary law enforcement purpose. That is, in adopting an amendment entitled “Coordination with law enforcement,” Congress was making it clear that FISA surveillances would still be initiated and controlled by intelligence officials. By the text of the amendment,

“Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title” are distinct from “Federal law enforcement officers.” 115 Stat. 364. Under the Attorney General’s reading of FISA, they would be one and the same, and no coordination would be needed.

Contrary to the government’s claim that the FISC ignored the Patriot Act, the FISC language modifying the March 2002 procedures restates the coordination Amendment almost verbatim. To compare, the FISC’s May 17 Opinion states: “The FBI, Criminal Division, and OIPR may consult with each other to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or their agents.” May 17 Opinion at 26. Thus, the FISC understood the coordination amendment to address both sides of the equation: what law enforcement officials can do without destroying the intelligence purpose of a search – namely, consult and coordinate, and what they cannot do – namely, initiate, control, or direct the investigation.

3. The FISC order contains a set of objective rules that implement the Patriot Act by preventing law enforcement officials from initiating or controlling and directing FISA surveillances

The FISC order contains a set of objective rules that implement the Patriot Act by preventing law enforcement officials from using FISA as an end-run around the Fourth Amendment, as interpreted and enforced via the requirements of Title III and Federal Rule of Criminal Procedure 41:

(1) law enforcement officials may not turn to the lower standard of FISA as a way of initiating surveillance when they are conducting a criminal investigation.

(2) law enforcement officials may not take over a properly-predicated FISA surveillance and direct and control it for the purposes of a criminal investigation.

The appropriateness of these procedures is illustrated in the case under appeal. In July, the FISC granted a FISA application in a situation where there is both an intelligence investigation and a criminal investigation. The government had asked the FISC to grant the application on the basis of the unmodified March 2002 procedures. The Court refused, instead subjecting the order to the modified procedures. The fact that law enforcement officials and intelligence agents had consulted, coordinated, and will share

information did not, it is apparent, lead the court to conclude that the FISA surveillance was improperly predicated. Rather, consistent with the statutory scheme, the procedures correctly establish objective criteria to prevent law enforcement officials from directing and controlling FISA surveillance.

The government concedes in its brief that “the FISC and other courts generally have not interpreted [FISA] to permit electronic surveillance (or physical searches) primarily to obtain evidence for a prosecution.” Govt Br. at 25. After the Patriot Act, it remains true that FISA is addressed to foreign intelligence surveillance, and not to surveillance whose purpose is to gather evidence of criminal conduct.

As discussed below, the government’s construction of FISA – a construction that would make FISA’s lower standards available to the government even in criminal investigations – would render the statute unconstitutional. The canon of constitutional avoidance mandates that a court confronting a statute susceptible of two constructions must adopt the construction that avoids constitutional issues. *See, e.g., Harris v. United States*, 122 S.Ct. 2406, 2413 (2002); *United States ex rel. Attorney General v. Delaware & Hudson Co.*, 213 U.S. 366, 408 (1909). Equally important, amici believe it is inappropriate to determine the constitutional issues, and

perhaps even the important statutory questions in this case, in a non-adversarial proceeding. Both the proceedings below and the proceedings in this Court have been conducted ex parte. While warrant applications are ordinarily considered ex parte, there is no rationale for that rule where the questions presented are purely legal ones. If the Court reaches the constitutional issues, which amici believe is unnecessary, amici urge the Court first to appoint special counsel to argue in opposition to the government in an adversarial proceeding. In any event, a familiarity with the constitutional issues discussed below is vitally important to a full appreciation of the stakes in the statutory dispute.

III. FISA IS UNCONSTITUTIONAL TO THE EXTENT IT AUTHORIZES SURVEILLANCE WHOSE PRIMARY OR EXCLUSIVE PURPOSE IS TO OBTAIN EVIDENCE FOR A CRIMINAL PROSECUTION

The government boldly argues that the USA Patriot Act authorizes a waiver of the Fourth Amendment's usual requirements whenever the government engages in criminal investigations related to "national security." The government should not be permitted to turn the quest for foreign intelligence into a "pro forma justification for any degree of intrusion into zones of privacy guaranteed by the Fourth Amendment," *United States v. Brown*, 484 F.2d 418, 427 (5th Cir. 1973) (Goldberg, J., concurring), *cert. denied*, 415 U.S. 960 (1974). Indeed, "the whole point of Fourth

Amendment protection in this area is to avoid . . . Executive abuses through judicial review.” *Zweibon v. Mitchell*, 516 F.2d at 636 n.108. As discussed below, eliminating Fourth Amendment protections would also jeopardize other constitutional interests, including the First Amendment right to engage in lawful public dissent, and the warrant, notice, and judicial review rights guaranteed by the Fourth and Fifth Amendments. *See* Section IV, *infra*.

The government’s central contention is that FISA “does not discriminate between law enforcement and non-law enforcement protective methods” – that FISA is available even for investigations that are purely criminal, so long as the ultimate purpose of the investigation is to protect against foreign threats to national security. Govt. Br. at 37. The government vaguely suggests that its ability to protect the nation will be compromised if it cannot rely on FISA for investigations whose primary or exclusive purpose is to gather evidence of criminal conduct. Amici of course do not dispute that the government should be able to prosecute spies and terrorists. The government simply misses the constitutional point, however, when it argues that this need justifies use of FISA even for investigations that are purely criminal. As discussed above, the *raison d’être* of FISA is the collection of foreign intelligence information, and the legitimacy of its departures from the Fourth Amendment’s normal requirements rests entirely

on the fact that FISA searches and surveillance are directed primarily to the collection of foreign intelligence. If the Government’s primary or exclusive purpose in an investigation is the enforcement of criminal law, it must proceed according to the normal strictures of the Fourth Amendment. As the Supreme Court has noted, “it is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one’s home or office are invaded.” *Berger v. New York*, 388 U.S. at 63.

A. Ordinary Fourth Amendment requirements apply to all searches having law enforcement as their primary or exclusive purpose

Every court that has considered the constitutionality of FISA’s lower standards has upheld those standards because the primary purpose of the FISA surveillance is foreign intelligence, not law enforcement. Notably, these courts have emphasized that the Constitution – and not merely statutory law – forecloses the executive branch from invoking FISA in investigations whose primary purpose is law enforcement. In *United States v. Duggan*, for example, the Second Circuit held that FISA’s “purpose” language required foreign-intelligence information to be “the primary objective of the surveillance,” 743 F.2d 59, 77 (2d Cir. 1984), and noted that FISA’s language reflected a “constitutionally adequate balancing of the individual’s Fourth Amendment rights against the nation’s need to obtain

foreign intelligence information,” *id.* at 73. Similarly, in *United States v. Johnson*, the First Circuit construed FISA’s “purpose” language to mean that “the investigation of criminal activity cannot be the primary purpose of the surveillance,” 952 F.2d 565, 572 (1st Cir. 1991), *cert. denied*, 506 U.S. 816 (1992), and rooted its holding in the view that FISA should “not be used as an end-run around the Fourth Amendment’s prohibition of warrantless searches,” *id.*; *see also United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987), *cert. denied* 486 U.S. 1010 (1988). At the very least, these cases stand for the proposition that the government may not rely on a foreign-intelligence exception if the government’s primary purpose is law enforcement.

Even before FISA was enacted, it was accepted that any national-security exception to the Fourth Amendment’s usual requirements had to be strictly cabined and could not benefit investigations whose primary purpose was the enforcement of the criminal law. In *Keith*, the Supreme Court held that domestic threats to national security could not justify a departure from the Fourth Amendment’s prior judicial authorization requirement. *See Keith*, 407 U.S. at 320. Contrary to the government’s assertion, *Keith* did not suggest that procedures appropriate in the intelligence sphere could be used primarily to gather evidence of criminal conduct. Indeed, the

government itself argued in *Keith* that lower standards were justified only because “these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions.” *Id.* at 318-19 (emphasis added). *Keith* acknowledged the possibility that procedural requirements in the intelligence sphere may be different from those that apply in the criminal sphere:

Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.

Id. at 322-23. Importantly, however, the Court did not suggest that procedures appropriate in the intelligence sphere could be used primarily to gather evidence of criminal conduct.

After *Keith*, several circuit courts considered the status of foreign intelligence surveillance under the Fourth Amendment. *Zweibon v. Mitchell* involved an FBI wiretap of the Jewish Defense League. *See* 516 F.2d. at 606. The tap was installed without prior judicial approval and, according to the Attorney General, had been installed to “provide[] advance knowledge of any activities of JDL causing international embarrassment to this country.” *Id.* at 609. The court rejected the argument that the wiretap was proper

notwithstanding the government's failure to obtain prior judicial approval, basing its argument principally on the finding that a warrant procedure would not fetter the legitimate intelligence-gathering functions of the Executive Branch. *See id.* at 651. The court also noted the risk that expansive and unchecked executive surveillance powers might chill protected speech. *See id.* at 634. Although the surveillance in *Zweibon* was installed under a presidential directive in the name of foreign intelligence gathering for the protection of national security, the targets of the surveillance were neither foreign powers nor their agents. *See id.* at 614. The court opined in dicta, however, that “absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional.” *Id.* at 613-14 (emphasis added).⁹

At the time these cases were decided, there was of course no statutory basis for a “primary purpose” requirement; the requirement was rooted not in statutory law but in the Fourth Amendment. In *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), which involved surveillance conducted before FISA was enacted, *see id.* at 915 n. 4, the Fourth Circuit recognized a foreign-intelligence exception to the warrant requirement but

⁹ The Court also noted that a limitation of warrantless surveillance to agents of a foreign power would “not alter the fact that First Amendment rights of others are likely to be chilled.” *Zweibon v. Mitchell*, 516 F.2d at 635. “Under such a test,” the court noted, “a few alien members in a political organization would justify surveillance of the conversations of all members.” *Id.*

limited the exception to cases in which “the surveillance is conducted primarily for foreign intelligence reasons,” *see id.* at 915 (internal quotation marks omitted). The court emphasized that this requirement stemmed from the Fourth Amendment:

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

Id.

Other pre-FISA cases that recognized a foreign-intelligence exception to the Fourth Amendment’s usual requirements similarly cabined the circumstances in which the executive branch may invoke the exception. *See, e.g., United States v. Butenko*, 494 F.2d 593, 606 (3d Cir.) (“Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental.”), *cert. denied*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d at 426; *id.* at 427 (Goldberg, J., concurring) (“The judiciary must not be astigmatic in the presence of warrantless surveillance; rather judges must microscopically examine the

wiretaps in order to determine whether they had their origin in foreign intelligence or were merely camouflaged domestic intrusions.”).

- B. The Supreme Court’s “special needs” cases confirm that the Fourth Amendment’s ordinary requirements apply to all searches whose primary or exclusive purpose is criminal investigation

The Supreme Court has recognized limited exceptions to the probable cause requirement in a line of cases involving “special needs.” Under these cases, Justice Scalia has explained, “[a] search unsupported by probable cause can be constitutional . . . when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.” *Vernonia School District 47J v. Acton*, 515 U.S. at 653 (internal quotation marks omitted and emphasis added). The “special needs” doctrine simply has no application to searches whose primary purpose is law enforcement. Indeed, the Supreme Court clearly reiterated this well-settled rule only last term. *See Ferguson v. City of Charleston*, 532 U.S. 67, 80 (2001) (citing, among other cases, *Skinner v. Railway Labor Executives’ Assn.*, 489 U.S. 602 (1989); *Treasury Employees v. Von Raab*, 489 U.S. 656 (1989); *Vernonia School District 47J v. Acton*, 515 U.S. 646 (1995); *Griffin v. Wisconsin*, 483 U.S. 868 (1987)).

Ferguson involved a public hospital’s policy of testing pregnant patients for drug use and employing the threat of criminal prosecution as a

means of coercing patients into substance-abuse treatment. The Court invalidated the policy. “In other special needs cases,” the Court wrote, “we . . . tolerated suspension of the Fourth Amendment’s warrant or probable cause requirement in part because there was no law enforcement purpose behind the searches in those cases, and there was little, if any, entanglement with law enforcement.” *Id.* at 79 n.15; *see also id.* at 88 (Kennedy, J., concurring) (“The traditional warrant requirement and probable-cause requirements are waived in our previous cases on the explicit assumption that the evidence obtained in the search is not intended to be used for law enforcement purposes.”). In *Ferguson*, however, “the central and indispensable feature of the policy from its inception was the use of law enforcement.” *Id.* at 80.

The government concedes that a general interest in crime control cannot constitute a “special need” sufficient to dispense with the probable cause requirement, but it contends, relying on *City of Indianapolis v. Edmond*, 531 U.S. 32, 41-42 (2000), that “a ‘special interest’ concerning a particular type of crime” may suffice. Gov’t Br. at 73. In fact, *Edmond* only reinforces the rule that any search whose primary or exclusive purpose is law enforcement may proceed only on the basis of probable cause. *Edmond* involved vehicle checkpoints instituted in an effort to interdict illegal drugs.

The government asserted that the drug crimes were a “severe and intractable” problem, and the Court agreed that “traffic in illegal narcotics creates social harms of the first magnitude.” *Id.* at 42. The Court also noted that “[t]he law enforcement problems that the drug trade creates likewise remain daunting and complex, particularly in light of the myriad forms of spin-off crime that it spawns.” *Id.* Notwithstanding the seriousness of the law-enforcement interest with respect to the particular crimes at issue, however, the Court invalidated the checkpoint policy. “[T]he gravity of the threat alone,” Justice O’Connor wrote, “cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose.” *Id.* The dispositive fact, the Court held, was that the checkpoint policy was instituted “primarily for the ordinary enterprise of investigating crimes.” *Id.* at 44. Where the government’s “primary purpose . . . is to detect evidence of ordinary criminal wrongdoing,” *id.* at 38, the Fourth Amendment forecloses the government from conducting searches except based on probable cause.¹⁰

¹⁰ Justice O’Connor indicated in dicta that any departure from this rule could be justified, if at all, only in exigent circumstances. “The Fourth Amendment would almost certainly permit an appropriately tailored road block set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route.” *City of Indianapolis v. Edmond*, 531 U.S., at 44. Such exigencies, however, are “far removed” from ordinary criminal investigation. *Id.* Here, while the government asserts national security interests, it makes no showing of exigency. Indeed, FISA surveillance intended to bring a criminal prosecution would make no sense in the face of an imminent terrorist threat.

The “special needs” cases reflect that the Fourth Amendment is particularly concerned with intrusions whose purpose is to gather evidence of crime. There is no support, however, for the proposition – implied by the government’s argument – that the Fourth Amendment recognizes a hierarchy amongst crimes. The Fourth Amendment applies to all criminal investigations, not merely those that are concerned with minor crimes. The government’s assertion, of course, is not simply that espionage and terrorism crimes are especially serious ones, but that these crimes are special in a constitutional sense. Gov’t Br. at 73-74. The government does not attempt to locate any support for this audacious assertion in the text of the Fourth Amendment (where there is, in any event, no support to be found); rather it relies on the fact that the prosecution of these crimes serves the ultimate purpose of protecting national security. Gov’t Br. at 74. Notwithstanding the government’s assertion to the contrary, however, Fourth Amendment requirements do not turn on a criminal investigation’s ultimate purpose. As the Court explained in *Ferguson*:

The threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose . . . was to ensure the use of those means. In our opinion, the distinction is critical. Because law enforcement involvement always serves some broader social purpose or objective, under respondent’s view, virtually any nonconsensual suspicionless search could be immunized under

the special needs doctrine by defining the search solely in terms of its ultimate, rather than immediate, purpose.

532 U.S. at 83-84. Indeed, the Supreme Court addressed exactly this issue in *Abel v. United States*, 362 U.S. 217 (1960), which involved the prosecution of a KGB agent for espionage. The Court rejected the argument that a different Fourth Amendment standard should apply merely because of “the nature of the case, the fact that it was a prosecution for espionage.” *Id.* at 219-20. The nature of the case, the Court held, could have “no bearing whatever” on the Fourth Amendment questions at issue. *See id.* (discussing, in particular, questions of evidentiary admissibility).

The Supreme Court’s “special needs” cases clearly reaffirm that any search whose primary or exclusive purpose is criminal investigation may proceed only on the basis of probable cause. This basic constitutional protection is not suspended for investigations of crimes that are particularly serious, or for investigations whose ultimate purpose is to protect against threats to national security. Any investigation whose primary or exclusive purpose is to collect evidence of criminal conduct must adhere to the ordinary requirements of the Fourth Amendment.

C. The government's theory would suspend ordinary Fourth Amendment requirements not only in espionage and terrorism investigations but in any investigation related to national security

The government's theory that FISA is available even for investigations that are purely criminal is profoundly troubling in itself, but it is made more so by the government's failure consistently to specify the crimes that in its view are constitutionally "special," let alone point to a constitutional or even statutory basis for such a specification. While the government refers to espionage and international terrorism as crimes that are entitled to special constitutional status, *see, e.g.*, Govt. Br. at 38, it repeatedly asserts the arrant principle that FISA is available to purely criminal investigations so long as the government believes that the prosecution of the crime will protect national security. *See, e.g.*, Govt. Br. at 37 ("[i]t is enough that the government intends to "protect" national security from foreign threats"); Govt. Br. at 38-39 n.13 (legislative history does "not undermine the idea that FISA may used [sic] to obtain evidence for a prosecution designed to protect national security"). The suggestion appears to be that the government could bypass the ordinary requirements of the Fourth Amendment not just in espionage and international terrorism investigations – a disturbing proposition on its own – but that the government could bypass the Fourth Amendment in *any* criminal

investigation, however minor the crime being investigated, so long as the government believes that the prosecution is designed to protect national security from foreign threats.

The notion that a search or surveillance may be justified simply because the government invokes the rubric of “national security” flies in the face of the most basic principles of American constitutional democracy. The government’s theory would effectively allow the executive branch unilaterally to suspend the ordinary requirements of the Fourth Amendment simply by claiming that a prosecution is designed to address a threat to national security. This Court should not sanction the government’s attempt to exploit the rubric of “national security” as a means of avoiding the basic Constitutional requirement that the government stay clear of constitutionally protected areas until it has probable cause to believe that a crime has been committed.

IV. ANY EXPANSION IN FISA SURVEILLANCE AUTHORITY WOULD IMPLICATE NUMEROUS OTHER CONSTITUTIONAL INTERESTS

The government’s brief urges this Court to dissolve the constitutional borders that separate intelligence investigations from criminal ones and thereby dramatically to extend FISA’s reach. As discussed above, any such extension would effectively institutionalize an end-run around the Fourth

Amendment's usual requirements. Given the secrecy that cloaks FISA proceedings, any such extension would also jeopardize a host of other constitutionally protected interests.

Public oversight of foreign intelligence surveillance in the United States is extremely limited. As Senator Leahy testified to the Senate Judiciary Committee,

Over the last two decades the FISA process has occurred largely in secret. Clearly, specific investigations must be kept secret, but even the basic facts about the FISA process have been resistant to sunlight. The law interpreting FISA has been developed largely behind closed doors. The Justice Department and FBI personnel who prepare the FISA applications work behind closed doors. . . . Even the most general information on FISA surveillance, including how often FISA surveillance targets American citizens, or how often FISA surveillance is used in a criminal case[], is unknown to the public.

2002 FISA Hearings (statement of Sen. Patrick Leahy).

While some degree of secrecy may be intrinsic to the very nature of foreign intelligence surveillance, as a general matter such secrecy stands in profound tension with basic democratic values. In a democracy, public scrutiny is the principal check on government misconduct. *See 2002 FISA Hearings* (statement of Sen. Patrick Leahy) (“In matters of national security, we must give the Executive Branch the power it needs to do its job. But we must also have public oversight of its performance. When the Founding Fathers said ‘if men were all angels, we would need no laws,’ they did not

mean secret laws.”); L. Brandeis, *Other People's Money* 62 (National Home Library Foundation ed. 1933). (“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”); *Grosjean v. Am. Press Co.*, 297 U.S. 233, 250 (1936) (“An informed public is the most potent of all restraints upon misgovernment.”); *Detroit Free Press v. Ashcroft*, No. 02-1437, 2002 WL 1972919, at *1 (6th Cir. Aug. 26, 2002) (“The Framers did not trust any government to separate the true from the false for us. . . . They protected the people against secret government.” (internal quotation marks omitted)). More fundamentally, citizens cannot be said to have chosen their government in any meaningful sense if they are foreclosed from learning what the government’s policies are. Even accepting for the moment the necessity of the heavy veil of secrecy that has cloaked FISA proceedings over the past two decades, it must be acknowledged that if secrecy serves the nation, it does so at the expense of democracy. *See Detroit Free Press v. Ashcroft*, 2002 WL 1972919, at *1 (“Democracy dies behind closed doors.”).

- A. Allowing FISA to be invoked in criminal investigations would raise Fourth Amendment and Due Process concerns because FISA fails to require notice and denies individuals any meaningful opportunity to challenge illegal surveillance

Ordinarily the Fourth Amendment requires that the subject of a search be provided notice that her privacy has been compromised. *See Richards v. Wisconsin*, 520 U.S. 385 (1997) (rejecting blanket exception to knock-and-announce requirement for all felony drug investigations); *Wilson v. Arkansas*, 514 U.S. 927 (1995) (knock-and-announce requirement is “embedded in Anglo-American law”); *cf.* 18 U.S.C. § 2518(8) (requiring notice for electronic surveillance conducted pursuant to Title III); 18 U.S.C. § 3013a(b) (requiring notice in searches executed pursuant to Fed. R. Crim. P. 41, and allowing delayed notice only on individualized showing of necessity). The Fifth Amendment similarly requires that the government provide notice to anyone whom it intends to deprive of property. *See Fuentes v. Shevin*, 407 U.S. 67, 80 (1972) (“Parties whose rights are to be affected are entitled to be heard; and in order that they may enjoy that right they must first be notified.”). Yet those targeted for surveillance under FISA are never provided notice that their privacy has been compromised. Even if the absence of any notice requirement in FISA is constitutional as to surveillance conducted until now, expanding FISA’s application to surveillance whose primary or exclusive purpose is the enforcement of the

criminal law plainly raises new (and significantly more serious) constitutional issues. *See* May 15 Opinion, at 24 (noting that government’s proposed minimization procedures would “give the Department’s criminal law enforcement officials every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information,” including possibility of conducting searches without notice to the target).

FISA’s failure to require that surveillance targets eventually be notified that their privacy was compromised raises related Due Process concerns because it denies individuals whose communications were inappropriately intercepted any opportunity to challenge the government’s actions. Innocent people whose communications are intercepted will probably never find out about the intercept, and those who somehow find out have no way of holding the government to account. While surveillance targets whom the government ultimately prosecutes do receive notice if the government intends to introduce evidence obtained through FISA, *see* 50 U.S.C. § 1806(c), even in such circumstances the warrant application is not provided to the defendant and even intercepted communications may not be divulged unless the government seeks to introduce them in evidence or they are exculpatory; rather the court reviews the communications *in camera*, *see*

50 U.S.C. § 1806(f).¹¹ Although the FISC exercises a degree of oversight with respect to FISA surveillance through review of surveillance applications, the executive branch has traditionally been accorded great deference in this area. *See, e.g., United States v. Duggan*, 743 F.2d at 77 (noting that government’s “primary purpose” certification is “subjected to only minimal scrutiny by the courts”); *id.* (“The FISA judge . . . is not to second-guess the executive branch official’s certification that the objective of the surveillance is foreign intelligence information.”). In any event, such in camera, ex parte review is no substitute for an adversarial hearing.

The Supreme Court recognized in *Franks v. Delaware* that, in the Fourth Amendment context, judicial review is meaningful only if the subject of a search can challenge the propriety of the search in a proceeding that is both public and adversarial. *See* 438 U.S. 154, 168-72 (1978). *Franks* involved a defendant’s challenge to a police search; the defendant alleged that the affidavits upon which the search was based were deliberately false.

The Supreme Court held that a defendant who makes a preliminary showing

¹¹ Under 50 U.S.C. § 1806(e), “[a]ny person against whom evidence obtained or derived from an electronic surveillance . . . is to be . . . introduced or otherwise used or disclosed in any trial . . . may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that – (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval.” However, § 1806(f) requires that, upon the Attorney General’s request, the court must review the challenged evidence ex parte and in camera. The Attorney General makes such requests as a matter of course. *See, e.g., United States v. Nicholson*, 955 F.Supp. 588, 592 (E.D.Va. 1997) (“[T]his Court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance. To the contrary, every court examining FISA-obtained evidence has conducted its review in camera and ex parte.”).

that affidavits were deliberately false is entitled to an evidentiary hearing. The Court advanced several rationales for its holding, including that, because the pre-search proceeding is ex parte, the prior judicial authorization requirement would “not always . . . suffice to discourage lawless or reckless misconduct”. *Id.* at 169. “The usual reliance of our legal system on adversary proceedings,” the Court noted, “itself should be an indication that an ex parte inquiry is likely to be less vigorous.” *Id.*; *see also* 2002 FISA Hearings (testimony of Kenneth C. Bass, III) (“[A]ny process that departs from our normal adversary proceedings is subject to increased risk of error. When there is no counsel on ‘the other side,’ the court finds itself in an uncomfortable position of being critic as well as judge.”); May 17 Opinion, at 24 (raising concern that government’s proposed minimization procedures would allow Fourth Amendment searches on less than probable cause but preclude “adversarial discovery of the FISA applications and warrants.”) The *Franks* Court also noted that the government cannot be relied on to police its own conduct. “Self-scrutiny is a lofty ideal, but its exaltation reaches new heights if we expect a District Attorney to prosecute himself . . . for well-meaning violations of the search and seizure clause during a raid [he himself] ordered.” 438 U.S. at 169 (internal quotation marks omitted).

B. Any extension of FISA would chill protected speech and therefore raise serious First Amendment concerns

Expanding the circumstances in which the government may invade the individual's protected sphere without probable cause also presents the danger that the government's surveillance power will chill dissent, and indeed that the government may wield its power with the specific intent of chilling dissent. Traditionally, the warrant and probable cause requirements have served as important safeguards of First Amendment interests by precluding the government from intruding into an individual's protected sphere merely because of that individual's exercise of First Amendment rights. The Supreme Court wrote in *Keith*:

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

Keith, 407 U.S. at 313-14; *see also id.* at 314 (“The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public discourse, is

essential to our free society.”); *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001) (“In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one’s speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.” (internal quotation marks omitted)); *Zweibon v. Mitchell*, 516 F.2d at 633 (“Prior judicial review is important not only to protect the privacy interests of those whose conversations the government seeks to overhear, but also to protect free and robust exercise of the First Amendment rights of speech and association by those who might otherwise be chilled by the fear of unsupervised and unlimited Executive power to institute electronic surveillances.”). Any expansion of the government’s authority to conduct electronic surveillance under FISA could easily chill protected speech and implicate serious First Amendment concerns.

CONCLUSION

For the reasons stated above, amici urge the Court to affirm the decision of the FISC.

Respectfully submitted,

ANN BEESON
JAMEEL JAFFER
STEVEN R. SHAPIRO
American Civil Liberties Union
125 Broad Street
New York, NY 10004
Telephone: (212) 549-2601
Facsimile: (212) 549-2651

JAMES X. DEMPSEY
Center for Democracy and Technology
1634 Eye Street, NW, Suite 1100
Washington, DC 20006

KATE MARTIN
Center for National Security Studies
1120 19th Street, NW, 8th floor
Washington, DC 20036

DAVID L. SOBEL
Electronic Privacy Information Center
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009

LEE TIEN
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Counsel for *Amici Curiae*

Dated: September 19, 2002