ANDREA R. MEYER
OSB No. 93365
ACLU of Oregon Foundation
PO Box 40585
Portland, OR 97240
(503) 227-6928 (ph)
(503) 227-6948 (fax)

ANN BEESON
JAMEEL JAFFER
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500 (ph)
(212) 549-2651 (fax)

JOSHUA L. DRATEL
National Association of Criminal Defense Lawyers
14 Wall Street, 28th Floor
New York, New York 10005
(212) 732-0707 (ph)
(212) 571-6341 (fax)

Counsel for *Amici Curiae*

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

UNITED STATES OF AMERICA,

v.

JEFFREY LEON BATTLE, ET AL.,

Defendants.

No. CR 02-399 JO

BRIEF OF *AMICI CURIAE* IN SUPPORT OF DEFENDANTS' MOTION TO SUPPRESS FOREIGN INTELLIGENCE SURVEILLANCE EVIDENCE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

PRELIMINARY STATEMENT

Amici curiae American Civil Liberties Union Foundation ("ACLU") and National Association of Criminal Defense Lawyers ("NACDL") submit this brief in support of defendants' Motion to Suppress Foreign Intelligence Surveillance Evidence.

The surveillance at issue in this case was extraordinarily comprehensive and far-reaching. The government secretly entered defendants' homes, conducted physical searches and installed electronic eavesdrop devices. It recorded all activity within the home, virtually uninterrupted, for a period of two full months. The government also intercepted hundreds of defendants' e-mails and literally thousands of their telephone calls. The government's primary – perhaps even exclusive – purpose in monitoring the defendants was to obtain evidence to be used against them in a criminal prosecution. *See* Defendants' Memorandum, p.41 n.21. Yet rather than obtain a warrant for these intrusive searches under ordinary criminal rules, which impose strict requirements on surveillance in order to comport with the Fourth Amendment's prohibition on unreasonable searches and seizures, the government committed an end-run around the Constitution by conducting the surveillance under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, recently amended by Section 218 of the USA PATRIOT Act ("Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272 (2001). FISA was enacted to govern electronic surveillance for foreign intelligence purposes, and FISA's lower standards have been upheld by the federal courts specifically because they were limited to foreign intelligence gathering. The Patriot Act now authorizes FISA surveillance even where the government's primary purpose is criminal prosecution. Said another way, FISA creates for the first time a class of *criminal* investigations in which the government may disregard the core requirements of the Fourth Amendment.

Only one other court – the FISA Court of Review – has considered the constitutionality of FISA as amended. In a closed proceeding in which the government was the only party, the FISA Court of Review incorrectly upheld the statute. This case presents one of the first opportunities for a court to consider the facial validity of FISA as amended in the context of a criminal prosecution. Because the vast majority of FISA surveillance targets will never receive notice that their privacy has been violated, and because the very existence of FISA's broad surveillance powers chills expression protected by the First Amendment, *amici* urge the Court to consider the facial validity of FISA in this case.

The government's actions in this case starkly illustrate the constitutional defects in FISA as amended. Though the government intended to gather evidence for criminal prosecution, it avoided compliance with the probable cause, particularity, and due process requirements of the Fourth Amendment by obtaining surveillance orders under FISA rather than the ordinary criminal rules. Because the FISA provision authorizing the surveillance orders in this case is unconstitutional on its face and as applied to the defendants, *amici* urge the Court to suppress the evidence obtained by the government and to declare the statute facially invalid.

I. Overview

A. Statutory Context

FISA was enacted in 1978 to govern surveillance of foreign powers and their agents inside the United States. The statute created the FISA Court, a court composed of seven (now eleven) federal district court judges, and empowered this court to grant or deny government applications for surveillance orders. *See* 50 U.S.C. § 1803(a). FISA also set out

the conditions that the government must satisfy before the FISA Court can issue a surveillance order. *See* 50 U.S.C. § 1805(a).

The statute was a response to the government's abuse of surveillance powers during the preceding decades. It is now a matter of public record that, during the Cold War and McCarthy eras, the FBI routinely installed electronic surveillance devices on private property in order to monitor the conversations of suspected communists. *See* S. Rep. 95-604, at 11 (1977). Under a program called COINTELPRO, authorized by President Nixon in the 1970s, the FBI wiretapped civil rights leaders, including Martin Luther King, Jr., solely because of their political beliefs. *See generally* 2 Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, Final Report ("Church Committee Report"), S. Rep. 94-755 (1976). The CIA illegally surveilled as many as seven thousand Americans in Operation CHAOS, including individuals involved in the peace movement, student activists, and black nationalists. *See generally Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982). The Church Committee Report, issued in 1976, observed:

> We have seen segments of our Government, in their attitudes and action, adopt tactics unworthy of a democracy, and occasionally reminiscent of the tactics of totalitarian regimes. We have seen a consistent pattern in which programs initiated with limited goals, such as preventing criminal violence or identifying foreign spies, were expanded to what witnesses characterized as "vacuum cleaners," sweeping in information about lawful activities of American citizens.

Church Committee Report, at 3-4. The report warned:

> Unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature.

Church Committee Report, at 1.

FISA, enacted two years after the publication of the Church Committee Report, was Congress's answer to this warning. The statute established guidelines to restrict the executive's authority to conduct surveillance under the rubric of foreign intelligence.[1] In order to obtain a surveillance order from the FISA Court, the government was required to show probable cause to believe that the prospective surveillance target was a "foreign power" or an "agent of a foreign power." 50 U.S.C. § 1804(a)(4)(A). It was also required to certify, among other things, that "the purpose" (now, "significant purpose") of the surveillance was to obtain "foreign intelligence information." *Id.* § 1804(a)(7)(B).

FISA did not, however, hold the government to the standards ordinarily required by the Fourth Amendment. For instance, the government was permitted to conduct surveillance under FISA even if it could not articulate any reason to believe that the surveillance target was engaged in criminal activity. It was not required to meaningfully limit the duration and scope of its surveillance. In addition, it was not required to provide the defendants with timely notice that their privacy had been compromised.

The Patriot Act dramatically expanded the class of investigations in which FISA is available to the government. As noted above, prior to the Patriot Act the government could invoke FISA only by certifying that "the purpose" of the surveillance was to obtain foreign intelligence information. The Patriot Act replaced "the purpose" with "a significant

[1] As originally enacted, FISA addressed only wiretaps. The covert-entry search provision was added in 1994. *See* Pub. L. No. 103-359, Title VIII, § 807(a)(3), Oct. 14, 1994, 108 Stat. 3447. A provision addressing "pen register" and "trap and trace" devices was added in 1998, Pub. L. No. 105-272, Title VI, § 601(2), Oct. 20, 1998, 112 Stat. 2405, and a provision addressing business records was also added in 1998, Pub. L. No. 105-272, Title VI, § 602, Oct. 20, 1998, 112 Stat. 2411. Neither the pen register nor the records provision is at issue here, and, except as indicated, references herein to "FISA surveillance" are references to surveillance conducted under FISA's wiretap or covert-entry search provisions.

purpose." Pub. L. No. 107-56, 115 Stat. 272, § 218 (amending 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)). The amendment authorizes the government for the first time to obtain surveillance orders under FISA's relatively undemanding standards even where its primary purpose is to gather evidence of criminal activity. The consequence is that, in a wide range of criminal investigations, the government can now effect an end-run around the Fourth Amendment merely by asserting a desire to gather foreign intelligence information from the person it in fact intends to prosecute.

B. *In re Sealed Case 02-001* of the Foreign Intelligence Surveillance Court of Review

Oversight of FISA surveillance is exceedingly limited. The sparse information that is publicly available indicates that the FISA Court has never rejected outright a single surveillance application.[2] According to the Attorney General's annual reports, the FISA Court approved 15,264 surveillance applications between 1979 and 2002. During that period, the Court modified six applications before approving them, and rejected one application without prejudice. In other words, the FISA Court approved without modification 15,257 out of 15,264 applications, or 99.95% of the applications submitted.

Until last year, the FISA Court had never before published a decision, and the FISA Court of Review had never convened. In August of last year, however, the FISA Court published a decision for the first time. The decision, which it had rendered in May 2002, directly implicated but did not decide the constitutionality of FISA as amended by the Patriot Act. The decision rejected new procedures proposed by the Attorney General to govern all

[2] The Attorney General's annual reports are available at http://www.fas.org/irp/agency/doj/fisa/.

FISA surveillance targeting United States persons (the "2002 Procedures").[3] The 2002 Procedures, which were meant to implement the Attorney General's interpretation of the Patriot Act, authorized the FBI to rely on FISA even where its primary purpose was law enforcement. The FISA Court refused to endorse the 2002 Procedures as proposed, finding that they were designed to allow the FBI to evade the Fourth Amendment in criminal investigations and that they were inconsistent with FISA's minimization provisions. *See In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F.Supp.2d 611, 623 (U.S. For. Int. Surv. Ct. 2002) ("*In re All Matters*") ("The 2002 procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillances and Rule 41 searches.").[4] The FISA Court reasoned that the 2002 Procedures would create perverse organizational incentives and mean that

> criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute. . . . [T]he Department's criminal prosecutors [will have] every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information, including:

---

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

[4] The court's decision was informed by its finding that the government had abused its FISA surveillance authority in "an alarming number of instances." *In re All Matters*, at 620. The court noted, for example, that in September 2000 the government had come forward "to confess error in some 75 FISA applications related to major terrorist attacks against the United States." *Id*. The errors included "an erroneous statement in the FBI Director's FISA certification that the target of the FISA was not under criminal investigation"; "erroneous statements in the FISA affidavits of FBI agents concerning the separation of the overlapping intelligence and criminal investigations"; and "omissions of material facts from FBI FISA affidavits relating to a prior relationship between the FBI and a FISA target." *Id*. The court also noted that it had convened a special meeting in November 2000 "to consider the troubling number of inaccurate FBI affidavits in so many FISA applications," *id*., and that as a result of the meeting "[o]ne FBI agent was barred from appearing before the Court as a FISA affiant," *id* at 621.

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

based on a standard that the U.S. person is only using or about to use the places to be surveilled and searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants.

In re All Matters, at 624.

The FISA Court of Review convened for the first time in its history to hear the government's appeal. Though the government asked the Court of Review to reach the question of FISA's constitutionality, the government was the only party in this extraordinary litigation over the constitutionality of a major federal statute. Neither the target of the particular surveillance orders that gave rise to the FISA Court's ruling, nor anyone arguing that FISA was unconstitutional, was allowed to participate as a party.[5] Oral argument on appeal was closed to the public and conducted *ex parte.*

In November 2003, the FISA Court of Review reversed the lower FISA Court's ruling and explicitly upheld the constitutionality of FISA as amended by the Patriot Act, though it acknowledged that "the constitutional question presented in this case . . . has no definitive jurisprudential answer." *In re Sealed Case,* 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002). The Court of Review first addressed the question whether FISA orders are warrants within the meaning of the Fourth Amendment. The Court acknowledged the significant differences between FISA's procedural requirements and those of Title III. The

[5] The Court of Review accepted an amicus brief from the ACLU and civil rights groups, and another amicus brief from the National Association of Criminal Defense Lawyers.

Court conceded, "to the extent the two statutes diverge in constitutionally relevant areas . . . a FISA order may not be a 'warrant' contemplated by the Fourth Amendment." *Id* at 741. The Court declined to decide the issue, however, instead proceeding directly to the question whether FISA searches are reasonable. On this point the Court concluded,

> [W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore[] believe firmly … that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

Id. at 746. Because the FISA Court of Review ruled in favor of the government, there was no party to appeal the decision to the Supreme Court.[6]

In response to the Court of Review's decision, the Department of Justice implemented sweeping institutional changes, including doubling the number of National Security Law Unit attorneys responsible for filing FISA applications and creating a FISA unit within the FBI General Counsel's office. *See* Transcript, *Department of Justice Press Conference Re: Foreign Intelligence Surveillance Court of Review* (November 18, 2002)[7] The Attorney General characterized the surveillance powers granted by the Patriot Act as "revolution[ary]." *Id.* It appears that the FBI immediately began to rely on FISA in investigations that previously could have been conducted only under Title III or Rule 41.

The pending motion to suppress provides one of the first opportunities for a federal court to consider the constitutionality of FISA as amended in the context of an actual

---

[6] *Amici* moved to intervene directly in the Supreme Court for the purpose of filing a petition for certiorari; the Supreme Court denied the motion without opinion. *See* 123 S.Ct. 1615 (2003).

[7] The transcript is available at <http://www.uspolicy.be/issues/terrorism/ashcroft.1111902.htm>.

criminal prosecution. The facts of the case highlight the dangers of allowing the FBI to rely on foreign intelligence procedures where its primary intent is criminal prosecution.

C. Factual Background

All of the defendants in this case are United States citizens. The central allegation against the defendants is that they tried, unsuccessfully, to travel to Afghanistan in order to contribute their services to the Taliban and Al-Qaida. Specifically, defendants are charged with conspiracy to levy war against the United States; conspiracy to provide material support and resources to Al-Qaida; conspiracy to contribute services to Al-Qaida and the Taliban; and possessing firearms in furtherance of crimes of violence.

The government appears to have begun a criminal investigation of defendant Battle in early 2002. As described in more detail in defendants' Memorandum, the government developed an informant named Khalid Mostafa. Defendants' Memorandum, at 4-9. Informant Mostafa developed a close personal relationship with defendants Battle and Lewis. Government agents outfitted Mostafa with a bodywire; Mostafa then recorded numerous conversations, including conversations held during religious services inside a Portland mosque. The government also actively pursued the criminal investigation using a variety of other conventional methods. *See id.* at 7.

Neither *amici* nor counsel for defendants knows precisely when the FISA orders were issued because the government has invoked a provision that allows it to withhold the FISA applications and underlying documents. *See id.* at 7. The FISA surveillance appears to have begun in June of 2002. It appears that the criminal investigation was well underway before the government sought and obtained the FISA surveillance at issue in the current motion.

The government conducted extensive surveillance of the defendants under FISA. With respect to defendant Jeffrey Battle, the government conducted (i) wireless communications surveillance of a particular telephone number; (ii) electronic and data communications surveillance of a particular e-mail account; (iii) a physical search of the same e-mail account; and (iv) audio surveillance and physical search of his residence. *See* Gov't Response, pp.2-3.[8] With respect to defendant Patrice Lumumba Ford, the government conducted (i) wire communications surveillance of a particular telephone number; (ii) wireless communications surveillance of a particular telephone number; (iii) electronic and data communications surveillance of a particular e-mail account; and (iv) audio surveillance and physical search of his residence. *See* Gov't Response, p.3. The other defendants were apparently not the named targets of FISA surveillance, although some of their communications were intercepted.

As noted above, the FISA surveillance of defendants Battle and Ford was extremely intrusive. Through the covert installation of an eavesdropping device, the government recorded over a thousand hours of activity inside Battle's home, over a near-continuous period of two months. *See* Decl. of Arnuldo Araiza, ¶ 5; Defendants' Memorandum, p.9. The government has also acknowledged intercepting hundreds of e-mails and literally thousands of telephone calls. *See* Decl. of Arnuldo Araiza, ¶¶ 3-4.

[8] It appears that the government does not intend to introduce evidence obtained through the FISA surveillance of Battle's e-mail account. *See* Gov't Response, p.3.

II. The FBI's surveillance of the defendants in this case did not conform to constitutional requirements that govern the conduct of criminal investigations

A. FISA surveillance orders are not warrants within the meaning of the Fourth Amendment

As an initial matter, FISA surveillance orders are not warrants within the meaning of the Fourth Amendment. The Supreme Court has held that a warrant must be issued by a neutral, disinterested magistrate; must be based on a demonstration of probable cause to believe that the evidence sought will aid in a particular apprehension for a particular offense; and must particularly describe the things to be seized as well as the place to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). FISA court orders do not satisfy these requirements. On the contrary, FISA empowers the government to conduct the most intrusive kinds of surveillance without meaningful prior judicial review, without showing criminal probable cause, and without meeting particularity requirements. *See In re Sealed Case*, at 741 (acknowledging that FISA orders "may not be . . . 'warrant[s]' contemplated by the Fourth Amendment").

Because FISA court orders are not warrants, searches conducted under FISA are presumptively unreasonable. *See, e.g., Payton v. New York*, 445 U.S. 573, 586 (1980); *Chimel v. California*, 395 U.S. 752, 762-63 (1969). The surveillance at issue in this case cannot overcome that presumption. As discussed below, the surveillance of the defendants here fell far short of the requirements that the Supreme Court and Ninth Circuit have held to be reasonable in the context of criminal investigations.

B. The surveillance was conducted without compliance with the Fourth Amendment's probable cause requirement

The Fourth Amendment ordinarily prohibits the government from conducting intrusive surveillance without first demonstrating criminal probable cause – probable cause

to believe that "the evidence sought will aid in a particular apprehension or conviction for a particular offense." *See Dalia*, 441 U.S. at 255. Although the government's primary purpose in this case was to obtain evidence of criminal activity, it failed to satisfy the criminal probable cause requirement.

FISA authorizes the government to conduct intrusive surveillance if it can show what is known as "foreign intelligence probable cause" – probable cause to believe that the surveillance target is a foreign power or agent of a foreign power. *See* 50 U.S.C. § 1805(a)(3)(A). The statute does not require the government to advance any reason whatsoever – let alone probable cause – to believe that its surveillance will yield information about a particular criminal offense. Indeed, foreign-intelligence probable cause bears only a passing resemblance to criminal probable cause. In response to a Freedom of Information Act request filed by the ACLU and others in August 2002, the FBI released, among other things, a document from the FBI's National Security Law Unit entitled, "What do I have to do to get a FISA?" The document states, in relevant part:

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

"What do I have to do to get a FISA?," at 2 (Document released by FBI in response to August 21 Freedom of Information Act request submitted by ACLU et al.) (emphases added).[9] It is clear that foreign-intelligence probable cause is not "probable cause" within the ordinary meaning of the Fourth Amendment.

The surveillance at issue in this case was not premised on criminal probable cause and accordingly was unreasonable within the meaning of the Fourth Amendment.

C. The surveillance was conducted without compliance with the Fourth Amendment's particularity requirement

As noted above, the surveillance of defendants in this case continued unabated for over two months and thousands of hours. The government intercepted hundreds of e-mails and literally thousands of telephone calls. Because the duration of these intercepts was not strictly limited, the surveillance violated the Fourth Amendment's particularity requirement.

The Fourth Amendment ordinarily prohibits the government from conducting intrusive surveillance unless it first obtains a warrant describing with particularity the things to be seized as well as the place to be searched. *See Berger v. New York*, 388 U.S. 41, 58 (1967) (noting that Fourth Amendment particularity requirement was intended to prevent the government's reliance on "general warrants" that allow "the seizure of one thing under a warrant describing another"); *see also Maryland v. Garrison*, 480 U.S. 79, 84 (1987). ("The manifest purpose of [the] particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to

[9] This document is available at <http://www.aclu.org/patriot_foia/FOIA/Sept2002Doc.pdf>.

its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

In *Berger*, the Supreme Court noted that the importance of the particularity requirement "is especially great in the case of eavesdropping." *Berger*, 388 U.S. at 56. The Court explained: "By its very nature eavesdropping involves an intrusion on privacy that is broad in scope." *Id.* It continued: "[T]he indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments, and imposes a heavier responsibility on this Court in its supervision of the fairness of procedures." *Id.*; *see also id.* at 63 (internal quotation marks omitted) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."); *United States v. Smith*, 321 F.Supp. 424, 429 (C.D.Cal. 1971) ("Electronic surveillance is perhaps the most objectionable of all types of searches in light of the intention of the Fourth Amendment.").

With respect to eavesdropping devices and wiretaps, the particularity requirement demands not simply that the government describe in detail the communications it intends to intercept but also that the duration of the intercept be strictly limited. *See Berger*, 388 U.S. at 58-60.[10] In *Berger*, the Supreme Court struck down New York's eavesdropping statute in

[10] The government's argument that the Ninth Circuit has "squarely held that an order issued under FISA complies with the Fourth Amendment's particularity requirement" is flawed for two reasons. First, the case on which the government relies, *United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987), considered only the contention that FISA violates the particularity clause by allowing a general description of the information sought; the *Cavanagh* Court did not consider, and apparently was not asked to consider, whether the *duration* of FISA surveillance orders renders FISA unconstitutional. Second, *Cavanagh* addressed the particularity issue in the context of a statute whose ambit was limited to foreign intelligence investigations. The question whether FISA meets the particularity requirement in the context of *criminal* investigations has never arisen (and was not addressed in *Cavanagh*), because until recently the FBI could rely on FISA only where its primary purpose was to gather foreign intelligence. As discussed in Section III, *infra*, FISA's

part because the statute authorized surveillance orders with terms of up to two months. *See Berger*, 388 U.S. at 44 n.1. The Court wrote:

> [A]uthorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches and seizures pursuant to a single showing of probable cause. Prompt execution is also avoided. During such a long and continuous (24 hours a day) period the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation.

Id. at 59. Title III, which Congress enacted shortly after *Berger* was decided, limits the term of surveillance orders to 30 days. *See* 18 U.S.C. § 2518(5). FISA, by contrast, authorizes surveillance terms of up to 120 days. See 18 U.S.C. § 1805(e)(1)(B).[11]

The Ninth Circuit has confirmed that, at least in the context of criminal investigations, the 30-day limitation is constitutionally required. In *United States v. Koyomejian*, 970 F.2d 536 (9th Cir.), *cert. denied*, 506 U.S. 1005 (1992), the Court confronted the legality of silent video surveillance in a domestic criminal investigation. The Court held that neither Title III nor FISA speaks to such surveillance but that warrants authorizing silent video surveillance must nonetheless be limited to terms of no more than 30 days. *See id*. at 542 ("we look to Title [III] for guidance in implementing the fourth amendment in an area that Title [III] does not specifically cover" (internal quotation marks omitted)); *id*. (holding that warrant authorizing silent video surveillance "must not allow the period of surveillance to be longer than is necessary to achieve the objective of the authorization, or in any event longer than thirty days" (internal quotation marks and brackets

---

departures from ordinary Fourth Amendment principles are constitutionally indefensible where the government's primary purpose is to gather evidence of criminal activity.

[11] An order authorizing surveillance of a foreign power (rather than an agent of a foreign power) may have a term of up to one year. *See* 50 U.S.C. § 1805(e)(1)(A).

omitted)); *id* at 542 (Kozinski, J., dissenting) (agreeing with majority's reasoning with respect to 30-day limitation).

Given *Berger* and *Koyomejian*, there can be no argument that FISA's provisions relating to the duration of surveillance orders meet Fourth Amendment requirements for criminal investigations. As noted above, the FISA order in this case was in place for two months – a length of time found constitutionally unacceptable in *Berger*. In addition, FISA authorizes surveillance orders of as long as 120 days – twice the duration of the orders that the Supreme Court found constitutionally unacceptable in *Berger*, and four times the *maximum* duration that the Ninth Circuit found constitutionally permissible in *Koyomejian*. Accordingly, the surveillance at issue in this case was unreasonable within the meaning of the Fourth Amendment.

D. The surveillance was conducted without compliance with the Fourth Amendment's notice requirement

Defendants in this case were not notified of the FISA surveillance of their homes, e-mail accounts, and telephone communications until weeks or months after the surveillance took place. Even then, they learned of the surveillance only when the government decided to prosecute them. Given that the surveillance was conducted with the intent to gather evidence of criminal activity, the government's failure to notify the defendants of the surveillance was unreasonable.

The Fourth Amendment ordinarily requires that the subject of a search be notified that the search has taken place. *See Wilson v. Arkansas*, 514 U.S. 927 (1995) (holding that the common-law "knock-and-announce" principle informs Fourth Amendment reasonableness inquiry); *Miller v. United States*, 357 U.S. 301, 313 (1958) ("The requirement of prior notice of authority and purpose before forcing entry into a home is deeply rooted in

our heritage and should not be given grudging application."). While in some contexts the government is permitted to delay the provision of notice, *see, e.g., United States v. Donovan*, 429 U.S. 413, 429 n.19 (1977) (holding that delayed-notice provisions of Title III supply a constitutionally adequate substitute for contemporaneous notice), the Supreme Court has never upheld a statute that, like FISA, authorizes the government to search a person's home or intercept his communications without *ever* informing her that her privacy has been compromised. Indeed, in *Berger*, the Supreme Court struck down a state eavesdropping statute in part because the law did not make any provision for notice.

The non-provision of notice in FISA investigations is particularly problematic because notice is withheld as a categorical rule, and not upon an individualized showing of necessity. *See Richards v. Wisconsin*, 520 U.S. 385, 393-94 (1997) (rejecting categorical exception to knock-and-announce principle for searches executed in connection with felony drug investigations); *see also Berger*, 388 U.S. at 60 (striking down state eavesdropping statute in part because law "has no requirement for notice as do conventional warrants, *nor does it overcome this defect by requiring some showing of special facts.*" (emphasis added)).

Except in the very few investigations that end in criminal prosecutions, FISA targets *never* learn that their homes or offices have been searched or that their communications have been intercepted. Accordingly, most FISA targets have no way of challenging the legality of the surveillance or obtaining any remedy for violations of their constitutional rights.[12] *See*

[12] "Other abuses, such as the search incident to arrest, have been partly deterred by the threat of damage actions against offending officers, the risk of adverse publicity, or the possibility of reform through the political process. These latter safeguards, however, are ineffective against lawless wiretapping and 'bugging' of which their victims are totally unaware." *United States v. U.S. District Court for Eastern District of Michigan, Southern Division*, 407 U.S. 297, 325 (1972) (Douglas, J., concurring).

Franks v. Delaware, 438 U.S. 154, 168-72 (1978) (holding that subject of an allegedly illegal search must be afforded an opportunity to challenge the propriety of the search in a proceeding that is both public and adversarial).

Even those FISA targets who are prosecuted and receive notice that their privacy was compromised have no meaningful opportunity to obtain a remedy for violations of their constitutional rights. Just as occurred in this case, criminal defendants are routinely denied access to FISA surveillance applications and underlying affidavits. *See* 50 U.S.C. § 1806(f); *United States v. Nicholson*, 955 F.Supp. 588, 592 (E.D. Va. 1997). Having no access to the factual allegations in these documents severely handicaps a defendant's ability to argue that the surveillance orders violate the Fourth Amendment. The courts have never upheld similar restrictions in criminal prosecutions based on evidence obtained under Title III or Rule 41.

E. The surveillance was conducted without meaningful prior judicial review

The surveillance at issue in this case was conducted without meaningful judicial review. To conduct surveillance in an ordinary criminal investigation, the FBI must obtain the prior authorization of a neutral, disinterested magistrate who has the authority to determine whether the requirements of Rule 41 or Title III have been satisfied. *See* Fed. R. Crim. P. 41 (governing physical searches in criminal investigations); 18 U.S.C. § 2518 (governing electronic surveillance in criminal investigations); *see also Johnson v. United States*, 333 U.S. 10, 13-14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime"). The FISA

Court does not have a corresponding authority to determine whether, in any particular foreign intelligence investigation, the FBI has satisfied the requirements of FISA.

The government satisfies most of FISA's requirements simply by certifying that the requirements are met. *See* 50 U.S.C. § 1804(a)(7) (enumerating necessary certifications). While certain (but not all) of these certifications must be accompanied by "a statement of the basis for the certification," 50 U.S.C. § 1804(a)(7)(E), the statute makes clear that the FISA Court is not to scrutinize such statements, but rather is to defer to the government's certification unless it is "clearly erroneous on the basis of the statement made under § 1804(a)(7)(E)," *id*. § 1805(a)(5).[13] As the FISA Court of Review has acknowledged, "this standard of review is not, of course, comparable to a probable cause finding by the judge." *In re Sealed Case* at 739; *see also United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984) (noting that government's "primary purpose" certification is "subjected to only minimal scrutiny by the courts"); *id*. ("The FISA judge . . . is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information.").

Judicial oversight under Title III, by contrast, is substantially more robust. To obtain a surveillance order under Title III, the government must provide the court with "a full and complete statement of the facts and circumstances relied upon by the applicant[] to justify his belief that an order should be issued." 18 U.S.C. § 2518(1)(b). The court may "require the applicant to furnish additional testimony or documentary evidence in support of the application." *Id*. § 2518(2). The government cannot meet any of the statute's substantive

[13] In the case of surveillance targets who are not United States persons, the FBI's certifications are not reviewed even for clear error. *See* 50 U.S.C. § 1805(a)(5).

requirements merely by certifying that it has met them. On the contrary, with respect to most of the statute's substantive requirements, the statute requires the court to find probable cause to believe that they are satisfied. *See id*. § 2518(3).

The surveillance at issue in this case was conducted without meaningful prior judicial review and accordingly was unreasonable within the meaning of the Fourth Amendment.

III. FISA's departures from ordinary Fourth Amendment principles are constitutionally defensible only where the government's *primary purpose* is to gather foreign intelligence information

Even if FISA's departures from ordinary Fourth Amendment principles are reasonable where the government's primary purpose is monitoring the activities of foreign powers and their agents inside the United States, they are clearly unreasonable where the government's primary intent is to prosecute the surveillance target. Since 1978, when FISA was enacted, numerous federal courts have clearly and repeatedly emphasized that the reasonableness of FISA surveillance is predicated on the fact that the foreign intelligence exception is available to the government *only where its primary purpose is to gather foreign intelligence*. In direct conflict with that principle, Section 218 of the Patriot Act for the first time delineates a class of *criminal* investigations in which the government may disregard the core requirements of the Fourth Amendment. As discussed below, that class of cases remains undefined and could be virtually limitless. The Supreme Court has held, in the "special needs" cases, that the government may not justify such a broad departure from the Fourth Amendment where its primary purpose is criminal investigation.

A. Numerous federal courts have held that the Fourth Amendment forecloses the government from relying on the foreign intelligence exception where its primary purpose is to gather evidence of criminal activity

The possibility of a foreign intelligence exception to the Fourth Amendment's ordinary requirements appears to have been first proposed to the Supreme Court in *United States v. U.S. District Court for Eastern District of Michigan, Southern Division*, 407 U.S. 297 (1972) (*Keith*).[14] *Keith* involved the criminal prosecution of individuals accused of having planted a bomb at CIA offices in Ann Arbor, Michigan. None of the individuals was alleged to have any connection to a foreign power. The central issue before the Supreme Court was whether certain wiretaps, which the government had conducted without a warrant, were nonetheless lawful as a reasonable exercise of the President's authority to protect the national security. The Court wrote:

> We are told . . . that 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. It is said that this type of surveillance should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity, not ongoing intelligence gathering.

Keith, 407 U.S. at 318-19. The Court rejected these arguments, reasoning that the President's domestic security role "must be exercised in a manner compatible with the Fourth Amendment." *Id*. at 320. The Court acknowledged, however, that surveillance for intelligence purposes may implicate different concerns than surveillance for law enforcement purposes:

[14] The issue arose earlier in *United States v. Smith.* The court in that case held that "in wholly domestic situations there is no national security exemption from the warrant requirement of the Fourth Amendment," *id*. at 429, but reserved the question whether another argument might prevail in cases involving foreign powers, *id*. at 428.

> The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact target of such surveillance may be more difficult to identify than in surveillance operations against many types of crime . . . . 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.
>
> Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.

Keith, 407 U.S. at 322. This discussion, though addressed to surveillance of domestic groups, gave credence to the idea that the executive branch might permissibly conduct foreign intelligence surveillance, too, according to different standards than those that govern ordinary criminal investigations.

After *Keith*, several Circuit Courts recognized a foreign intelligence exception to ordinary Fourth Amendment requirements. Critically, however, these courts emphasized that the exception was limited to *intelligence* surveillance, and could not be relied on as a justification for disregarding ordinary Fourth Amendment requirements in *criminal* investigations. Thus, in *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir., 1980), the Fourth Circuit recognized a foreign intelligence exception to ordinary Fourth Amendment requirements but strictly limited the exception to cases in which "the surveillance is conducted primarily for foreign intelligence reasons." *See also id.* at 916 ("The exception applies only to foreign powers, their agents, and their collaborators. Moreover, even these actors receive the protection of the warrant requirement if the

government is primarily attempting to put together a criminal prosecution.").[15] The Court explained its reasoning:

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

Id. at 915. Other Circuits that acknowledged a foreign intelligence exception before FISA's enactment adopted similar reasoning. *See, e.g., United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974) ("Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental."), *cert. denied*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *id*. at 427 (Goldberg, J., concurring).

Importantly, each of these cases involved surveillance conducted *before* FISA was enacted – that is, before there was any statutory basis for a primary purpose restriction. Thus the basis for the restriction was found not in the statute but in the constitution. The Fourth Circuit made this abundantly clear:

> [T]he executive can proceed without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers and their assistants. We think that the unique role of the executive in foreign affairs and the separation of powers will not permit this court to allow the executive less on the facts of this case, *but we are also convinced that the Fourth Amendment will not permit us to grant the executive branch more*.

Truong, 629 F.2d at 916 (emphasis added).

---

[15] While *Truong* was not decided until 1980, it involved surveillance that took place before FISA's enactment in 1978. *See Truong*, 629 F.2d at 915 n.4.

The text of FISA as originally enacted did not expressly include a "primary purpose" requirement. Instead, it authorized the FBI to rely on a foreign intelligence exception for "the purpose" of obtaining foreign intelligence information. Most courts asked to consider FISA's constitutionality, however, generally interpreted that requirement as a primary purpose requirement, consistent with the Fourth Circuit's view that the Constitution does not permit the government to rely on the foreign intelligence exception where its primary purpose is to gather evidence of criminal activity. *See, e.g., United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991), *cert. denied*, 506 U.S. 816 (1992) (stating that "the investigation of criminal activity cannot be the primary purpose of the surveillance," and that FISA may "not be used as an end-run around the Fourth Amendment's prohibition of warrantless searches"); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987), *cert. denied* 486 U.S. 1010 (1988) (interpreting "purpose" to mean "primary purpose"); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987), *cert. denied*, 485 U.S. 937 (1988); *United States v. Duggan*, 743 F.2d at 77.

The Ninth Circuit has recognized a foreign intelligence exception to the Fourth Amendment's ordinary requirements, *see United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987), but has expressly declined to reach the question whether the government may rely on the exception where its primary purpose is to gather evidence of criminal activity, *see United States v. Sarkissian*, 841 F.2d 959 (9th Cir. 1988). In *Sarkissian*, the defendant challenged a district court's refusal to suppress evidence obtained under FISA, arguing that the government's purpose in effecting the surveillance was criminal investigation and that consequently the surveillance should have been effected under Title III rather than FISA.

The Court rejected the defendant's argument, holding that "[r]egardless of whether the test is one of purpose or primary purpose, . . . it is met in this case." *Id*. at 964.

The government obliquely suggests that the Ninth Circuit rejected the primary purpose requirement *sub rosa* in *Sarkissian*. Although the government acknowledges that the Ninth Circuit in that case expressly declined to decide the issue, the government contends that the Court found it irrelevant "that the government may choose to use FISA-derived information for a criminal prosecution." Gov't Response, p.42. What the Ninth Circuit in fact found irrelevant was *not* that the government "may choose to use FISA-derived information for a criminal prosecution," but rather that the government "may *later* choose to prosecute." *Sarkissian*, 841 F.2d at 965 (emphasis added). The difference is critical, because the primary purpose test is addressed not to the *use* of FISA evidence, but rather to the *predicate* for the surveillance. It is one thing to say, as the *Sarkissian* Court did, that the government "may later choose to prosecute" a person based on FISA evidence; FISA has always allowed the government to do this, *see* 50 U.S.C. § 1801(h)(3), and the primary purpose test has nothing to say about the matter. It is another thing altogether to say that the government may *initiate* FISA surveillance with the primary purpose of collecting evidence toward a criminal prosecution. It is this that the Fourth Amendment prohibits.[16]

Ironically, when the government first urged the Supreme Court to recognize an intelligence exception to the Fourth Amendment, it did so based on the argument "that these surveillances are directed *primarily* to the collecting and maintaining of intelligence with

[16] The government also argues against the primary purpose test on the grounds that *Truong* was concerned with warrantless surveillance, while surveillance conducted under FISA requires the prior approval of the FISA Court. *See* Gov't Response, p.43. As discussed above, however, *see* Section II.A, *supra*, FISA court orders are emphatically not warrants within the meaning of the Fourth Amendment.

respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions." *Keith,* 407 U.S. at 318-19 (emphasis added); *see also Smith,* 321 F.Supp. at 428 ("The government has emphasized that the purpose of the surveillance involved was not to gather evidence for use in a criminal prosecution but rather to provide intelligence information needed to protect against the illegal attacks of such organizations." (internal quotation marks omitted)). It was based on this argument that the Supreme Court opened the door to a foreign intelligence exception. Now, some thirty years later, the government contends that it must be permitted to rely on the foreign intelligence exception even where its primary purpose is to gather evidence of criminal activity. Accepting the government's new argument, however, requires rejecting the argument that justified the foreign intelligence exception in the first place.

B. FISA is unconstitutional because it would allow the government to evade Fourth Amendment requirements in a virtually limitless class of ordinary criminal investigations

Section 218 allows the government to evade Fourth Amendment requirements in criminal investigations merely by asserting that an investigation also has some connection to foreign intelligence. The consequence is that the government is now permitted to evade Fourth Amendment requirements in a virtually boundless class of ordinary criminal investigations.

FISA supplies no guidance as to how this class might be limited in any meaningful way. The government, relying principally on arguments adopted by the FISA Court of Review in *In re Sealed Case,* attempts to contain the class by arguing that FISA is available to it only in investigations of "foreign intelligence crimes" or of "ordinary crimes" connected to foreign intelligence crimes. But FISA nowhere uses the phrase "foreign intelligence

crime." The FISA Court of Review, borrowing some language from the definition of "foreign intelligence information," 50 U.S.C. § 1801 (e), and other language from FISA's definition of "agent of a foreign power," *id.* §1801(b), defined "foreign intelligence crime" to include terrorism, sabotage, and "enter[ing] the United States under a false or fraudulent identity for or on behalf of a foreign power," *In re Sealed Case,* 310 F.3d at 723 & n.10. In order to contain the gaping hole in the Fourth Amendment that Section 218 creates, the government, like the FISA Court of Review, must manufacture the definition out of whole cloth.

Limiting Section 218's significance to "foreign intelligence crimes" does not, in any event, solve the problem, for "foreign intelligence crime" is itself a category with no discernible limit. International terrorism, which the FISA Court of Review found to be a component of the category, is not a single crime but rather an entire class of crimes. *See* 50 U.S.C. § 1801(c) (defining "international terrorism" to include, for example, any violent crime that appears to be intended "to intimidate or coerce a civilian population"). And of course even if the government's definition of "foreign intelligence crime" imposed a meaningful limit on the government's ability to evade the Fourth Amendment in criminal investigations, that limit would be undermined by the government's theory that FISA is available to it not only with respect to "foreign intelligence crimes" but also with respect to "ordinary crimes" not wholly unconnected to "foreign intelligence crimes." *See* Gov't Response, p.33 (*citing In re Sealed Case*, 310 F.3d at 722-28).

The government insists that the "significant purpose" amendment was necessary because foreign intelligence and criminal investigations are often intertwined, and because the primary purpose limitation was unworkable. Gov't Response, p.37. But the implication

that the primary purpose test somehow prevented the government from using criminal prosecution as a tool to protect national security is untenable. In fact, the primary purpose limitation has *never* prevented the government from using criminal prosecution as a tool to protect national security. Its only effect is to dictate which standards the government must meet in order to engage in surveillance whose profound intrusiveness even the government does not dispute. The government is always entitled to engage in such surveillance if it can meet the requirements of the Fourth Amendment.[17] Because Section 218 now authorizes a departure from those standards in a broad and undefined class of cases, it creates an overwhelming incentive for the FBI to characterize criminal investigations as foreign intelligence investigations.

C. The Supreme Court's "special needs" cases confirm that the government cannot constitutionally rely on the foreign intelligence exception where its primary purpose is to gather evidence of criminal activity

The government proposes that "the need to protect the country from terrorist attack" justifies a departure from ordinary Fourth Amendment principles notwithstanding that the immediate and primary purpose of FISA surveillance may be to gather evidence of criminal activity. *See* Gov't Response, p.46. The question whether a special need can justify a departure from the Fourth Amendment's usual requirements has arisen before. The Supreme Court's consistent answer has been that "[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.*

[17] In addition, FISA has always authorized FBI intelligence agents to disseminate FISA material (such as wiretap transcripts) to FBI criminal investigators where the material constitutes evidence of criminal activity. *See* 50 U.S.C. § 1801(h)(3).

Acton, 515 U.S. 646, 653 (1995) (internal quotation marks omitted and emphasis added); *see also Graves v. City of Coeur d'Alene*, 2003 WL 21768966, at *11 n.22 (9th Cir. 2003).

The Supreme Court recently reaffirmed this well-settled rule in *Ferguson v. City of Charleston*, 532 U.S. 67 (2001). *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). In *Ferguson*, however, "the central and indispensable feature of the policy from its inception was the use of law enforcement." *Id*. at 80.

The Supreme Court's decision in *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), upon which the government wrongly relies, *see* Gov't Response, p.46, is to the same effect. *Edmond* involved vehicle checkpoints instituted in an effort to interdict illegal drugs. The government asserted that the crimes were a "severe and intractable" problem, and the Court agreed that "traffic in illegal narcotics creates social harms of the first magnitude." *Id*. at 42. Notwithstanding the seriousness of the law enforcement interest with respect to the particular crimes at issue, however, the Court invalidated the checkpoint policy. "[T]he gravity of the threat alone," Justice O'Connor wrote, "cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose." *Id.* at 33. Where the government's "primary purpose [is] to detect evidence of ordinary criminal wrongdoing," the Fourth Amendment forecloses the government from conducting searches except based on

criminal probable cause. *Id*. at 38; *see also Henderson v. City of Simi Valley*, 305 F.3d 1052 (9th Cir. 2002) (special needs exception applies only where challenged search has non-law enforcement function).

The government also cites *In re Sealed Case*, in which the FISA Court of Review reasoned that although the special needs cases apply only where the government's primary purpose is not law enforcement, the relevant question is not the immediate purpose of a FISA search but rather FISA's "programmatic purpose." *In re Sealed Case*, 310 F.3d at 745. In fact, the Supreme Court has emphatically rejected this argument. In *Ferguson*, for example, the government argued that the relevant question was the government's "ultimate purpose," and that the ultimate purpose of the hospital's policy was not law enforcement but public health. The Court wrote:

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

Ferguson, 532 U.S. at 83-84.[18] Similarly, though protecting the country from terrorist attack is obviously a worthy aim, that ultimate goal does not exempt the government from the Fourth Amendment when its immediate purpose is criminal prosecution.

[18] While Justice Kennedy took issue with the majority's focus on the policy's "immediate purpose," he concurred in the judgment, writing: "As the majority demonstrates and well explains, there was substantial law enforcement involvement in the policy from its inception. None of our special needs precedents has sanctioned the routine inclusion of law enforcement, both in the design of the policy and in using arrests, either threatened or real, to implement the system designed for special needs objectives. The special needs cases we have decided do not sustain the active use of law enforcement, including arrest and prosecutions, as an integral part of a program which seeks to achieve legitimate, civil objectives. The traditional warrant and probably cause requirements are waived in our

IV. FISA Should Be Facially Invalidated

As discussed above, the search in this case violated defendants' Fourth Amendment rights. Accordingly, defendants clearly have standing to seek facial invalidation of the statute. *See United States v. Posey*, 864 F.2d 1487, 1491 (9th Cir. 1989). Though *amici* recognize that facial invalidation is strong medicine, the remedy is appropriate – indeed, vital – here because on its face Section 218 authorizes searches that violate the Fourth Amendment, deprives the vast majority of its surveillance targets of any opportunity to vindicate their privacy rights, and chills expression protected by the First Amendment.

The government correctly notes that Section 218 must be facially invalidated if "no set of circumstances exists under which the Act would be valid." *United States v. Salerno*, 481 U.S. 739, 745 (1987). As discussed at length above, there is no doubt that Section 218 falls far short of Fourth Amendment requirements. Courts that upheld the pre-Patriot Act FISA against facial challenge did so only because the statute's application was limited to contexts in which the government's primary purpose was to gather foreign intelligence. *See* Section III, *supra*. Under FISA as amended, however, *every* FISA surveillance order empowers the government to disregard the Fourth Amendment even if its primary purpose is to gather evidence of a crime. In addition, *every* FISA order fails to satisfy several of the Fourth Amendment's requirements - the orders do not qualify as warrants, fail to require probable cause, fail the particularity requirement because of their lengthy duration, and provide inadequate notice. For these reasons, the facial challenge to Section 218 satisfies the *Salerno* test.

---

previous cases on the explicit assumption that the evidence obtained in the search is not intended to be used for law enforcement purposes." *Ferguson*, 532 U.S. at 88 (Kennedy, J., concurring).

The Supreme Court's facial invalidation of a New York state wiretapping statute in *Berger* provides a template for how this court should address the facial challenge in this case. 388 U.S. at 63. As in this case, the facial challenge in *Berger* was raised by a criminal defendant on a motion to suppress illegally obtained wiretap evidence. Because the statute that authorized the wiretap failed to meet constitutional requirements and "indisputably affected" the defendant, the Court held that he "clearly ha[d] standing to challenge the statute." 388 U.S. at 55. The Court then examined the statute and found it deficient in numerous respects.

In facially invalidating the statute, the *Berger* Court described the breadth of the constitutional threat at stake, writing that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." 388 U.S. at 63. 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). FISA's threat is equally sweeping, as evidenced by the breadth of surveillance conducted in the current case.

Facial invalidation of FISA is also imperative because, like the statute struck down in *Berger*, FISA does not require the government to provide even delayed notice to surveillance targets. *See* Section II.D, *supra*. The only surveillance targets who receive even limited notice of FISA surveillance are those targets who are ultimately prosecuted and against whom FISA evidence is introduced. But only a fraction of all FISA surveillance targets are

prosecuted. Yet surveillance targets whom the government does not prosecute have suffered the same Fourth Amendment injury as those who are prosecuted. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) (Fourth Amendment "prohibits unreasonable searches and seizures whether or not the evidence is sought to be used in a criminal trial, and a violation of the Amendment is fully accomplished at the time of an unreasonable governmental intrusion" (internal quotation marks omitted)). FISA should be struck down on its face to protect the vast majority of FISA surveillance targets who *never* learn that their privacy is invaded and thus have no opportunity to vindicate their constitutional rights.

Finally, facial invalidation is warranted because FISA also jeopardizes First Amendment rights. Traditionally, the Fourth Amendment's warrant and probable cause requirements have served as important safeguards of First Amendment interests by prevenging the government from intruding into an individual's protected sphere merely because of that individual's exercise of First Amendment rights. Expanding the circumstances in which the government may conduct searches without conforming to those requirements presents the danger that the government's surveillance power will chill activity that is protected under the First Amendment.

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

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

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

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

Id. at 633.

In reasoning that aptly applies to this case, one commentator analyzing the *Berger* opinion reasoned that facial invalidation was appropriate given the interrelated First Amendment and privacy rights threatened by electronic surveillance, and the inability of most victims to vindicate their rights:

> [T]his 'penunmbral' influence of the first amendment could provide a basis for judging the [eavesdrop] statute on its face. Further, an overbroad eavesdrop statute would seem to have the same 'chilling effect' on privacy that an overbroad picketing statute has on speech: the very knowledge that the police are authorized to eavesdrop without adequate judicial supervision will impair the value of the home or office as a place of refuge even if the police do not abuse their power. In addition, just as in free speech cases, it is by no means certain that all important issues would be litigated if a case-by-case approach were required, [because] the secrecy of eavesdrops makes it unlikely that issues arising out of unproductive eavesdrops would ever reach [the] court.

The Supreme Court, 1966 Term, 81 Harv. L. Rev. 69, 188 (1967).

Because FISA opens the door to surveillance abuses that seriously threaten both free speech and privacy rights, it should be facially invalidated.

CONCLUSION

For the reasons stated herein, *amici* respectfully urge the Court to grant defendants' Motion to Suppress Foreign Intelligence Surveillance Act Evidence and to declare FISA invalid on its face.

Respectfully submitted,

ANDREA R. MEYER
OSB No. 93365
ACLU of Oregon Foundation
PO Box 40585
Portland, OR 97204
(503) 227-6928

ANN BEESON
JAMEEL JAFFER
American Civil Liberties Union
125 Broad Street
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2629

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

Dated: September 18, 2003