### IN THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

#### CASE NO. 02-001

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

### BRIEF ON BEHALF OF AMICUS CURIAE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF AFFIRMANCE

John D. Cline Zachary A. Ives Freedman Boyd Daniels Hollander Goldberg & Cline P.A. 20 First Plaza, Suite 700 Albuquerque, NM 87102 (505) 842-9960

Joshua Dratel Co-Chair, NACDL Amicus Committee 14 Wall St., 28th Floor New York, NY 10005 (212) 732-0707

Counsel for Amicus Curiae National Association of Criminal Defense Lawyers

## **TABLE OF CONTENTS**

TABLE OF A	UTHO	RITIESii	
INTEREST O	F AMI	CUS CURIAE1	
		IE ISSUE	
		JUMENT	
I.	AN UI	NBROKEN LINE OF DECISIONS REQUIRES	
	A TRA	ADITIONAL WARRANT AND PROBABLE CAUSE	
	FOR E	LECTRONIC SURVEILLANCE AND PHYSICAL	
	SEAR	CHES UNLESS THE "PRIMARY PURPOSE" OF THE	
	GOVE	RNMENT ACTION IS THE COLLECTION OF	
	FORE	IGN INTELLIGENCE	
	A. <u>Katz</u>	z, <u>Berger</u> , and <u>Keith</u> 7	
	B.	The Federal Decisions Following <u>Katz</u> , <u>Berger</u> , and <u>Keith</u>	
	C.	The "Special Needs"	
	C.	Cases	
		Cases	
II.	CONTRARY TO THE DOJ'S ARGUMENT, FISA DOES		
	NOT OFFER SUFFICIENT PROTECTIONS TO JUSTIFY		
	ABANDONING THE FOURTH AMENDMENT WARRANT		
		PROBABLE CAUSE REQUIREMENTS	
CONCLUSIO	N		
CONCLUDIO			

## **TABLE OF AUTHORITIES**

## CASES

bel v. <u>United States</u> , 362 U.S. 217 (1960)17
bourezk v. <u>Reagan,</u> 785 F.2d 1043 (D.C. Cir. 1986), <u>aff'd by an equally divided Court</u> , 484 U.S. 1 (1987)23
lderman v. <u>United States,</u> 394 U.S. 165 (1969)25, 26
merican-Arab Anti-Discrimination Committee v. Reno, 70 F.3d 1045 (9th Cir. 1995)24
erger v. <u>New York,</u> 388 U.S. 41 (1967)7, 8, 13
<u>ity of Indianapolis</u> v. <u>Edmond,</u> 531 U.S. 32 (2000)16, 17, 18, 19
etroit Free Press v. <u>Ashcroft,</u> 2002 WL 1972919 (6th Cir. Aug. 26, 2002)24
erguson v. <u>City of Charleston,</u> 532 U.S. 67 (2001)
ranks v. <u>Delaware,</u> 438 U.S. 154 (1978)26, 27, 29
<u>ippo</u> v. <u>West Virginia,</u> 528 U.S. 11, (1999)17

<u>In re Kevork,</u> 634 F. Supp. 1002 (C.D. Cal. 1985), <u>aff'd</u> , 788 F.2d 566 (9th Cir. 1986)22
<u>Johnson</u> v. <u>United States</u> , 333 U.S. 10 (1948)
<u>Katz</u> v. <u>United States</u> , 389 U.S. 347 (1967)7, 9, 13
<u>Mincey</u> v. <u>Arizona,</u> 437 U.S. 385 (1978)
<u>Richards</u> v. <u>Wisconsin</u> , 520 U.S. 385 (1997)17
<u>United States</u> v. <u>Badia</u> , 827 F.2d 1458 (11th Cir. 1987)14, 22
<u>United States</u> v. <u>Belfield</u> , 692 F.2d 141 (D.C. Cir. 1982)22, 23
<u>United States</u> v. <u>Bin Laden</u> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000)
<u>United States</u> v. <u>Brown</u> , 484 F.2d 418 (5th Cir. 1973)14
<u>United States</u> v. <u>Butenko</u> , 494 F.2d 593 (3d Cir 1974)14
<u>United States</u> v. <u>Duggan</u> , 743 F.2d 59 (2d Cir. 1984)15, 22, 28, 29
<u>United States</u> v. <u>Humphrey</u> , 456 F. Supp. 51 (E.D. Va. 1978)14
<u>United States</u> v. <u>Isa,</u> 923 F.2d 1300 (8th Cir. 1991)22
<u>United States</u> v. <u>James Daniel Good Real Property</u> , 510 U.S. 43 (1993)
<u>United States</u> v. Johnson, 952 F.2d 565 (1st Cir. 1991)

United	States v. Megahey, 553 = Supp (E D N V (1082)) 15
	553 F. Supp. 1180 (E.D.N.Y. 1982)
<u>United</u>	<u>States</u> v. <u>Nicholson</u> , 955 F. Supp. 588 (E.D. Va. 1997)23
United	States v. Sarkissian, $841 \pm 24.050$ (9th Circ 1088) 15
	841 F.2d 959 (9th Cir. 1988)15
	<u>States</u> v. <u>Squillacote</u> ,
	221 F.3d 542 (4th Cir. 2000), cert. denied, 532 U.S. 971 (2001)22, 28
	<u>cert</u> . <u>demed</u> , 532 U.S. 971 (2001)22, 28
United	<u>States</u> v. <u>Truong Dinh Hung</u> ,
	629 F.2d 908 (4th Cir. 1980)14
United	States v. United States District Court (Keith),
	407 U.S. 297 (1972)

# CONSTITUTION, STATUTES, AND RULES

U.S. Const. Amend. IV.	passim
U.S. Const. Amend. V	27
18 U.S.C. § 2518	13
Classified Information Procedures Act,	
18 U.S.C. App. III	27
50 U.S.C. § 1801(i)	3
50 U.S.C. § 1801(h)	
50 U.S.C. § 1805.	27
50 U.S.C. § 1805(a)	27
50 U.S.C. § 1806(f)	21, 22, 27
50 U.S.C. § 1824(a)	27

## **OTHER AUTHORITIES**

Jennifer C. Evans, Hijacking Civil Liberties: The USA

<u>PATRIOT Act of 2001</u> , 33 Loy. U. Chi. L.J. 933 (2002)	6
Sharon H. Rackow, How the USA PATRIOT Act Will Permit Governmental	
Infringement Upon the Privacy of Americans in the Name of	
'Intelligence' Investigations, 150 U. Pa. L. Rev. 1651 (2002)	6

#### **INTEREST OF AMICUS CURIAE**

The National Association of Criminal Defense Lawyers is a District of Columbia nonprofit organization whose membership is comprised of over 10,000 lawyers and 28,000 affiliate members representing every state. The NACDL was founded in 1958 to promote study and research in the field of criminal law; to disseminate and advance knowledge of the law in the area of criminal practice; and to encourage the integrity, independence, and expertise of defense lawyers in criminal cases. NACDL members serve in positions bringing them into daily contact with the criminal justice system in the state and federal courts.

The NACDL is the only national bar organization working on behalf of public and private criminal defense lawyers. The American Bar Association recognizes the NACDL as an affiliated organization and awards it full representation in the ABA House of Delegates. The NACDL is dedicated to the preservation and improvement of our adversary system of justice.

The NACDL has long been concerned with the threat that the Foreign Intelligence Surveillance Act poses to the Fourth Amendment protection against unreasonable searches and seizures and with the secret, ex parte manner in which FISA issues are routinely decided. Because of these concerns, the NACDL has decided to take this rare opportunity to offer the Court its views on the critical constitutional issue that the Foreign Intelligence Surveillance Court's May 17, 2002 and July 19, 2002 decisions present.

#### STATEMENT OF THE ISSUE

Does the Fourth Amendment require a warrant and probable cause to conduct electronic surveillance or a physical search of an American citizen, where the primary purpose of the surveillance or search is criminal investigation and the collection of foreign intelligence information is a "significant" secondary purpose?

1

#### SUMMARY OF ARGUMENT

1. In the aftermath of the September 11 tragedy, the Department of Justice obtained from Congress the power to resort to FISA surveillance, rather than surveillance based upon a traditional warrant and probable cause, when foreign intelligence gathering is a "significant purpose" of the collection effort, even if criminal investigation is the "primary purpose" of the surveillance. Having convinced Congress to amend FISA in this respect, the DOJ now seeks to use the new standard, in stark violation of the Fourth Amendment, to place criminal prosecutors and investigators in charge of directing FISA surveillance against United States persons.<sup>1</sup>

2. The "significant purpose" provision of FISA, particularly as interpreted by the DOJ, violates the Fourth Amendment. A long line of court of appeals decisions, before and after FISA, has held that surveillance may be conducted without a traditional warrant and probable cause only when foreign intelligence collection is the "primary purpose" of the surveillance. The Supreme Court's recent "special needs" cases--particularly <u>Ferguson</u> v. <u>City of Charleston</u>, 532 U.S. 67 (2001)--have reiterated the "primary purpose" standard as the proper dividing line between searches that require a warrant and probable cause and those that do not.

3. The DOJ insists that the "significant purpose" standard satisfies the Fourth Amendment because of what it calls "the added protections afforded by FISA." But those socalled "protections" are almost entirely illusory. The Foreign Intelligence Surveillance Court functions ex parte and in secret. FISA requires the FISC to accept DOJ certifications concerning the purpose and other aspects of the surveillance unless they are "clearly erroneous," and it gives

<sup>&</sup>lt;sup>1</sup> We confine our discussion to the constitutionality of surveillance directed against "United States persons" as defined in FISA--that is, citizens of the United States or permanent resident aliens. <u>See</u> 50 U.S.C. § 1801(i). The surveillance of non-United States persons presents different constitutional issues, which we do not address here.

the FISC no means of investigating to determine whether that standard has been satisfied. Not surprisingly under these circumstances, the FISC almost always grants the government's applications. According to the Attorney General's annual reports from 1979 to 2001, the FISC approved 14,036 applications or extensions authorizing FISA surveillance or searches during that period; it modified only four applications before granting approval; and on one occasion, in 1997, it did not approve the application but granted the DOJ leave to amend and resubmit it. In other words, between 1979 and 2001, the FISC approved without modification 14,031 out of 14,036 applications, or 99.96% of the total. According to the Attorney General's reports, the court did not reject outright a single application.

4. When the prosecution seeks to use FISA evidence in a criminal prosecution, district courts uniformly prohibit defense counsel from reviewing the FISA application, the FISC order authorizing the surveillance, and the associated documents. The results of these secret, ex parte procedures are predictable. In FISA litigation, unlike any other form of litigation known to the American criminal justice system, the government effectively bats a thousand: its applications are virtually always granted, the fruits of its surveillance and searches are never suppressed, and--not coincidentally--no defendant ever gains access to the underlying FISA materials.

5. As established by Congress and interpreted by the courts, FISA has become a secret means by which the executive branch can conduct extraordinarily intrusive surveillance of American citizens without satisfying the usual probable cause requirements and use the fruits of that surveillance in criminal prosecutions without any meaningful opportunity for the target of the surveillance to challenge its legality. The May 17, 2002 FISC opinion ("Opinion") discloses the unsavory result of this ex parte, unconstitutional process: without the prospect of adversarial

3

proceedings, the executive branch has systematically misled the FISC about the purpose and use of its secret surveillance. This brief--and the brief of other amici--seeks to ensure that, at least on appeal, perspectives in addition to the government's will be heard and considered.

#### ARGUMENT

### I. AN UNBROKEN LINE OF DECISIONS REQUIRES A TRADITIONAL WARRANT AND PROBABLE CAUSE FOR ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES UNLESS THE "PRIMARY PURPOSE" OF THE GOVERNMENT ACTION IS THE COLLECTION OF FOREIGN INTELLIGENCE.

The Department of Justice seeks authority from this Court for prosecutors and agents conducting criminal investigations to direct the use of FISA surveillance--including both electronic surveillance such as wiretaps and physical searches--as long as a DOJ official certifies that a "significant purpose" of the surveillance is to obtain foreign intelligence information and the other requirements of FISA are met. In short, according to the DOJ's redacted brief, the executive wants to use FISA, rather than Title III and ordinary warrant procedures, even when the primary purpose of the surveillance is criminal prosecution, as long as the surveillance has some foreign intelligence connection that is more than "trivial," "incidental," or "pretextual."

The May 17, 2002 opinion of the FISC and the brief of amici American Civil Liberties Union, et al., make a compelling case that FISA, both in its original form and as amended by the USA PATRIOT Act, does not permit criminal investigators to use the statute to conduct criminal investigations. But the more fundamental flaw in the DOJ's position--one that cannot be remedied by statutory amendment or interpretation--lies in the fact that use of FISA to conduct criminal investigations violates the Fourth Amendment prohibition against unreasonable

4

searches and seizures.<sup>2</sup>

<sup>&</sup>lt;sup>2</sup> For discussions of the Fourth Amendment implications of the "significant purpose" provision, see Jennifer C. Evans, <u>Hijacking Civil Liberties: The USA PATRIOT Act of 2001</u>, 33 Loy. U. Chi. L.J. 933, 974-77 (2002), and Sharon H. Rackow, <u>How the USA PATRIOT Act Will Permit</u> <u>Governmental Infringement Upon the Privacy of Americans in the Name of 'Intelligence'</u> <u>Investigations</u>, 150 U. Pa. L. Rev. 1651, 1674-83 (2002).

#### A. <u>Katz</u>, <u>Berger</u>, and <u>Keith</u>.

The Supreme Court first applied the Fourth Amendment to electronic surveillance thirtyfive years ago in <u>Katz</u> v. <u>United States</u>, 389 U.S. 347 (1967), and <u>Berger</u> v. <u>New York</u>, 388 U.S. 41 (1967). <u>Katz</u> involved the surreptitious recording of telephone calls through a recording device attached to the outside of a telephone booth. The <u>Katz</u> Court declared that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." <u>Id</u>. at 353. The Court held that the warrantless surveillance violated the Fourth Amendment, in part because the government agents failed, "before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate." <u>Id</u>. at 356. The Court rejected the government's request for a "telephone booth" exception to the warrant requirement. <u>Id</u>. at 358. It expressly left open, however, "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security." <u>Id</u>. at 358 n.23.

In <u>Berger</u>, which arose from electronic surveillance conducted by state law enforcement officers, the Court emphasized that the traditional probable cause and particularity requirements apply to warrants or other orders authorizing such surveillance. <u>See</u> 388 U.S. at 55-56. The Court found that the New York statute authorizing the surveillance violated the Fourth Amendment (1) because it did not "requir[e] belief that any particular offense has been or is being committed; nor that the 'property' sought, the conversations, be particularly described"; (2) because it failed to limit the duration of the surveillance or to impose sufficiently stringent requirements on renewals of the authorization; and (3) because the statute "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some

6

showing of special facts." Id. at 58-60.

Berger rejected the state's argument that Fourth Amendment requirements should be relaxed because the surveillance statute was essential in its fight against organized crime. In terms that ring as true today as they did three decades ago, the Court declared: [W]e cannot forgive the requirements of the Fourth Amendment in the name of law enforcement. This is no formality that we require today but a fundamental rule that has long been recognized as basic to the privacy of every home in America. While the requirements of the Fourth Amendment are not inflexible, or obtusely unyielding to the legitimate needs of law enforcement, 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. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.

388 U.S. at 62-63 (quotation and citation omitted); see, e.g., Mincey v. Arizona, 437 U.S. 385, 393 (1978) ("[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment. . . . The investigation of crime would always be simplified if warrants were unnecessary. But the Fourth Amendment reflects the view of those who wrote the Bill of Rights that the privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law."). The FISC opinion makes clear that the "threat to liberty" that eavesdropping poses has only grown with technological advances over the past three decades. Opinion at 9 (noting the "exceptionally thorough acquisition and collection through a broad array of contemporaneous electronic surveillance techniques" that FISA authorizes).

The Supreme Court addressed the question left open in <u>Katz</u>--the limits that the Fourth Amendment places on electronic surveillance conducted in the name of national security--in <u>United States</u> v. <u>United States District Court (Keith)</u>, 407 U.S. 297 (1972). <u>Keith</u> considered the constitutional limits on surveillance directed at domestic security threats; the Court noted that the case "requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." <u>Id</u>. at 308; <u>see id</u>. at 321-22 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."). Although the Court recognized both the weight of the executive's interest in protecting the national security and the value of electronic surveillance in detecting security threats, it found that "[t]here is, understandably, a deep-seated uneasiness and apprehension that this [surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy." <u>Id</u>. at 312-13 (footnote omitted). The Court emphasized the need to protect both First and Fourth Amendment rights against government investigation based on alleged threats to national security:

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. The danger to political dissent is acute where the Government attempts to act under so vague a concept as "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

Id. at 314. The Court emphasized the importance of the Fourth Amendment warrant requirement in protecting the right of privacy. It identified as "the very heart of the Fourth Amendment

directive" that

where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation. Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate." The further requirement of "probable cause" instructs the magistrate that baseless searches shall not proceed.

Id. at 316 (citations omitted). And the Court made clear that the decision to conduct electronic

surveillance cannot be left to the discretion of law enforcement officials: These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

<u>Id</u>. at 316-17 (citation and footnote omitted). The Court rejected the executive's argument that an exception to the Fourth Amendment warrant requirement should be recognized for domestic security surveillance. In particular, the Court did not find persuasive the executive's claims that "internal security matters are too subtle and complex for judicial evaluation" and that "prior judicial approval will fracture the secrecy essential to official intelligence gathering." <u>Id</u>. at 320.

Finally, <u>Keith</u> underscored the differences between surveillance for criminal investigative purposes and surveillance for intelligence purposes. It noted, for example, that "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information"; that "[t]he exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III"; and that "[o]ften, 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." <u>Id</u>. at 322. In light of these "potential distinctions between Title III criminal surveillances and those involving the domestic security," the Court suggested that Congress "may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III," <u>id</u>.--a suggestion that led ultimately to the enactment of FISA in 1979. The Court added that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government <u>for intelligence information</u> and the protected rights of our citizens." <u>Id</u>. at 322-23 (emphasis added).

#### B. The Federal Decisions Following <u>Katz</u>, <u>Berger</u>, and <u>Keith</u>.

Read together, <u>Katz</u>, <u>Berger</u>, and <u>Keith</u> draw a line between surveillance conducted by law enforcement officials for the purpose of investigating crime--which requires the traditional warrant based on probable cause, as outlined in <u>Berger</u> and codified in 18 U.S.C. § 2518--and surveillance conducted by intelligence officials for the purpose of obtaining intelligence information.

Until the USA PATRIOT Act, both Title III and FISA clearly recognized this constitutionally-mandated distinction. And in the thirty years following <u>Keith</u>--before and after the enactment of FISA--courts have relied upon the Supreme Court's distinction between "criminal surveillances" and surveillance conducted for intelligence purposes to hold that electronic surveillance may proceed without the protections of a traditional warrant based on probable cause only if a court determines that the "primary purpose" of the surveillance is to obtain foreign intelligence information. <u>See, e.g., United States</u> v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) ("Although evidence obtained under FISA subsequently may be used in criminal prosecutions ... the investigation of criminal activity cannot be the primary purpose of the

10

surveillance. [FISA] is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches."); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (FISA application and related documents "establish that the telephone surveillance of Arocena did not have as its purpose the primary objective of investigating a criminal act"); United States v. Truong Dinh Hung, 629 F.2d 908, 915-16 (4th Cir. 1980) ("[T]he executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons."), aff'g United States v. Humphrey, 456 F. Supp. 51, 57-58 (E.D. Va. 1978) (same); United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974) (en banc) ("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."); United States v. Brown, 484 F.2d 418, 424 (5th Cir. 1973) ("There is no indication that defendant's telephone conversations were monitored for the purpose of gaining information to use at his trial, a practice we would immediately proscribe with appropriate remedy."); United States v. Bin Laden, 126 F. Supp.2d 264, 277-78 (S.D.N.Y. 2000) (foreign intelligence exception to warrant requirement for searches abroad where, among other requirements, the search is "conducted 'primarily' for foreign intelligence purposes"); United States v. Megahey, 553 F. Supp. 1180, 1188-89 (E.D.N.Y. 1982) (foreign intelligence exception to warrant requirement applies when surveillance is conducted "primarily" for foreign intelligence reasons), aff'd sub nom. United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).<sup>3</sup>

<sup>&</sup>lt;sup>3</sup> After citing and relying on these cases for years, the DOJ now insists that they were "wrongly decided." It cites only <u>United States</u> v. <u>Sarkissian</u>, 841 F.2d 959 (9th Cir. 1988), as potentially contrary authority. But as the DOJ itself concedes, <u>Sarkissian</u> declined to decide whether "primary purpose" is the appropriate standard because, according to the court, "[r]egardless of whether the test is one of purpose or primary purpose, our review of the government's FISA

This unbroken line of authority leaves little doubt that the "significant purpose" provision of FISA, particularly as interpreted by the DOJ, violates the Fourth Amendment. Indeed, even as Congress rushed to pass the USA PATRIOT Act in October 2001, a number of Members expressed reservations about the constitutionality of the "significant purpose" amendment to FISA in light of the settled "primary purpose" requirement rooted in the Fourth Amendment. <u>E.g.</u>, 147 Cong. Rec. S10558, S10593 (Oct. 11, 2001) (Sen. Leahy); <u>id</u>. at S10568 (Sen. Specter), S10585, S10593 (Sen. Cantwell), S10597 (Sen. Kennedy); <u>id</u>. at E1896 (Oct. 12, 2001) (Rep. Mink), H6760 (Rep. Scott), H6761 (Rep. Lofgren), H6767 (Rep. Convers), H6772 (Rep. Udall).

#### C. The "Special Needs" Cases.

The Supreme Court's "special needs" cases--on which the DOJ inexplicably purports to rely--underscore the principle that searches and seizures that have law enforcement as their primary purpose must satisfy the traditional warrant and probable cause requirements. In <u>City of Indianapolis</u> v. <u>Edmond</u>, 531 U.S. 32 (2000), for example, the Court found unconstitutional a checkpoint program that involved warrantless and suspicionless stops of motorists for "the primary purpose of interdicting illegal narcotics." <u>Id</u>. at 40. The Court noted that "[w]e have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing." <u>Id</u>. at 41.

The <u>Edmond</u> Court rejected two arguments that parallel the DOJ's arguments here. First, the Court dismissed the claim that "the severe and intractable nature of the drug problem" justified the checkpoint program. <u>Id</u>. at 42. In terms that squarely refute the DOJ's contention here, the Court declared:

There is no doubt that traffic in illegal narcotics creates social

materials convinces us that it is met in this case." Id. at 964.

harms of the first magnitude. The 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. But the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose. Rather, in determining whether individualized suspicion is required, we must consider the nature of the interests threatened and their connection to the particular law enforcement practices at issue. We are particularly reluctant to recognize exceptions to the general rule of individualized suspicion where governmental authorities primarily pursue their general crime control ends.

Id. at 42-43 (citations omitted). Similarly here, terrorism-related crimes undoubtedly inflict "socialharms of the first magnitude," but the "gravity of the threat alone" cannot justify abandoning the traditional protections of the Fourth Amendment.<sup>4</sup> In a variety of other contexts as well the Supreme Court has refused to recognize Fourth Amendment exceptions based on the seriousness of the crime under investigation. <u>See, e.g., Flippo</u> v. <u>West Virginia</u>, 528 U.S. 11, 13-14 (1999) (per curiam) (no "murder-scene" exception to warrant requirement); <u>Richards</u> v. <u>Wisconsin</u>, 520 U.S. 385, 391-95 (1997) (refusing to recognize blanket exception to knock-andannounce requirement in drug cases); <u>Abel</u> v. <u>United States</u>, 362 U.S. 217, 219-20 (1960) (applying Fourth Amendment to espionage case, Court declares: "Of course the nature of the case, the fact that it was a prosecution for espionage, has no bearing whatever upon the legal considerations relevant to the admissibility of evidence.").

Second, <u>Edmond</u> rejected the argument that the checkpoint program "is justified by its lawful secondary purposes of keeping impaired motorists off the road and verifying licenses and

<sup>&</sup>lt;sup>4</sup> The Court recognized that the Fourth Amendment equation changes when exigent circumstances exist, such as, for example, the need to "thwart an imminent terrorist attack." 531 U.S. at 44. As <u>Edmond</u> makes clear, the "exigent circumstances" exception to the Fourth Amendment warrant requirement already accommodates such emergencies; no further relaxation of Fourth Amendment protections is necessary.

registrations," id. at 46--an argument that parallels the DOJ's contention here that it may proceed under FISA as long as it has the "lawful secondary purpose" of collecting foreign intelligence information. Edmond noted that if such "lawful secondary purposes" sufficed to exempt a search or seizure from the usual Fourth Amendment requirements, "law enforcement authorities would be able to establish checkpoints for virtually any purpose so long as they also included a license or sobriety check." Id. The Court concluded: "For this reason, we examine the available evidence to determine the primary purpose of the checkpoint program. While we recognize the challenges inherent in a purpose inquiry, courts routinely engage in this enterprise in many areas of constitutional jurisprudence as a means of sifting abusive governmental conduct from that which is lawful." Id. at 46-47. Similarly here, if it were enough to avoid the Fourth Amendment warrant and probable cause requirements that an electronic surveillance or physical search had some connection to foreign intelligence that was more than "trivial," "incidental," or "pretextual," federal criminal investigators could use those highly intrusive techniques for "virtually any purpose," as long as a DOJ official could certify to such a foreign intelligence connection and the other requirements of FISA were satisfied.

The Supreme Court reinforced the holding of <u>Edmond</u> in <u>Ferguson</u> v. <u>City of Charleston</u>, 532 U.S. 67 (2001). <u>Ferguson</u> involved a state hospital's performance of non-consensual, warrantless drug screens on pregnant women, the results of which were turned over to law enforcement officers. <u>See id</u>. at 69-70. The Court concluded that the screens violated the Fourth Amendment because the "primary purpose" of the program was to "generate evidence <u>for law</u> <u>enforcement purposes</u>." <u>Id</u>. at 83-84 (emphasis in original).<sup>5</sup> Just as the DOJ argues here that its

<sup>&</sup>lt;sup>5</sup> Similarly, the Court distinguished prior "special needs" cases, in which it had upheld warrantless or suspicionless searches, on the ground that "there was no law enforcement purpose behind the searches in those cases, and there was little, if any, entanglement with law

proposed use of FISA for law enforcement purposes would serve broader foreign intelligence or national security goals, the City of Charleston argued in <u>Ferguson</u> that its drug screening program served the broader goal of "get[ting] the women in question into substance abuse

treatment and off of drugs." Id. at 82-83. The Court squarely rejected this contention: The threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose of [the drug screening] policy was to ensure the use of those means. In our opinion, this 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. Such an approach is inconsistent with the Fourth Amendment. Given the primary purpose of the Charleston program, which was to use the threat of arrest and prosecution in order to force women into treatment, and given the extensive involvement of law enforcement officials at every stage of the policy, this case simply does not fit within the closely guarded category of "special needs."

Id. at 83-84 (footnotes omitted). Ferguson--which the DOJ dismisses in a footnote--leaves no

doubt that the government's attempt to use the relaxed FISA standards for surveillance and

searches that have the primary purpose of law enforcement violates the Fourth Amendment.

## II. CONTRARY TO THE DOJ'S ARGUMENT, FISA DOES NOT OFFER SUFFICIENT PROTECTIONS TO JUSTIFY ABANDONING THE FOURTH AMENDMENT WARRANT AND PROBABLE CAUSE REQUIREMENTS.

We have addressed the DOJ's principal arguments for an exception to the Fourth

Amendment warrant and probable cause requirements in the course of the preceding discussion.

One such argument, however--that "reductions in th[e] purpose-related [privacy] protections are

enforcement." 532 U.S. at 79 n.15.

reasonable given the added protections afforded by FISA"--requires a further response.

At the outset, the DOJ's emphasis on the "added protections afforded by FISA" seems odd, in light of the disclosure in the May 17, 2002 FISC decision that the executive branch, by its own admission, made "misstatements" and omitted material facts in more than seventy-five FISA applications. Opinion at 16-17. These are the misstatements and omissions that the government has chosen to disclose; it is impossible for anyone outside the executive branch to know how many additional falsehoods and errors have gone unreported. That so many "misstatements" could have occurred without detection by the FISC casts significant doubt on the value of FISA's purported "protections."

Nor should the revelation that the executive branch has systematically misled the FISC come as a surprise. The substance and factual aspects of FISA proceedings occur entirely ex parte and in secret, not only before the FISC, but even in United States District Court when a criminal defendant seeks to suppress the fruits of FISA surveillance. When a defendant contests the legality of FISA evidence, the Attorney General may file an affidavit in the district court that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). Upon the filing of such an affidavit, the district court must review the government's application to the FISC, the FISC order authorizing electronic surveillance or a physical search, and other such materials in camera and ex parte, unless disclosure of the FISA materials to the defense is "necessary to make an accurate determination of the legality of the surveillance." Id.

In practice, § 1806(f) has completely barred defense counsel from access to the application and other materials underlying FISA orders issued by the FISC. To our knowledge, the Attorney General has filed an affidavit in every case where a defendant has sought access to

the government's FISA application and related materials; no district court has ever found under § 1806(f) that disclosure to the defense was "necessary to make an accurate determination of the legality of the surveillance"; and no court of appeals has ever reversed a district court's decision to deny defense access to FISA materials under § 1806(f). See, e.g., United States v. Squillacote, 221 F.3d 542, 554 (4th Cir. 2000), cert. denied, 532 U.S. 971 (2001); United States v. Isa, 923 F.2d 1300, 1306 (8th Cir. 1991); Badia, 827 F.2d at 1463-64; United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); United States v. Belfield, 692 F.2d 141, 146-49 (D.C. Cir. 1982); In re Kevork, 634 F. Supp. 1002, 1009 (C.D. Cal. 1985), aff'd on other grounds, 788 F.2d 566 (9th Cir. 1986). As a district court observed in 1997, "[E]very court examining FISA-obtained evidence has conducted its review in camera and ex parte." United States v. Nicholson, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997) (citing cases). It is surely no coincidence that "misstatements" have flourished in a regime where the defense never obtains access to the underlying materials and all significant proceedings occur in camera and ex parte.<sup>6</sup>

The use of ex parte procedures to decide the merits of FISA issues represents an extraordinary departure from the normal judicial process in this country. The District of Columbia Circuit has declared that "[o]nly in the most extraordinary circumstances does our

<sup>&</sup>lt;sup>6</sup> It is doubtful that the drafters of FISA intended § 1806(f) to function as a complete prohibition against defense access to FISA materials. According to the legislative history of the statute, disclosure is necessary under § 1806(f) "where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misinterpretation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order." <u>Belfield</u>, 692 F.2d at 147 (quoting S. Rep. No. 701, 95th Cong., 2d Sess. 64 (1979)). It is hard to imagine that in the dozens of criminal cases where district courts have determined the legality of FISA surveillance, these circumstances--or other, equally or more compelling circumstances--have never appeared.

precedent countenance court reliance upon <u>ex parte</u> evidence to decide the merits of a dispute." <u>Abourezk</u> v. <u>Reagan</u>, 785 F.2d 1043, 1061 (D.C. Cir. 1986), <u>aff'd by an equally divided Court</u>, 484 U.S. 1 (1987). Courts enforce this principle because "[i]t is a hallmark of our adversary system that we safeguard party access to the evidence tendered in support of a requested court judgment. The openness of judicial proceedings serves to preserve both the appearance and the reality of fairness in the adjudications of United States courts. It is therefore the firmly held main rule that a court may not dispose of the merits of a case on the basis of <u>ex parte</u>, <u>in camera</u> submissions." <u>Id</u>. at 1060-61; <u>cf</u>. <u>Detroit Free Press</u> v. <u>Ashcroft</u>, 2002 WL 1972919, at \*1 (6th Cir. Aug. 26, 2002) ("Democracies die behind closed doors.").

Courts generally bar the use of secret evidence and ex parte proceedings outside the FISA context because of the grave risk of error that such procedures entail. The Supreme Court has declared that "'[f]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights.... No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.'" <u>United States v. James Daniel Good Real Property</u>, 510 U.S. 43, 55 (1993) (quoting Joint Anti-Fascist Refugee Committee v. McGrath, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). As the Ninth Circuit observed in a secret evidence case, "One would be hard pressed to design a procedure more likely to result in erroneous deprivations.'... [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." <u>American-Arab Anti-Discrimination Committee</u> v. <u>Reno</u>, 70 F.3d 1045, 1069 (9th Cir. 1995) (quoting district court); <u>see</u>, e.g., <u>id</u>. at 1070 (noting "enormous risk of error" in use of secret evidence).

Two Fourth Amendment decisions from the Supreme Court highlight the importance of

adversarial proceedings. In <u>Alderman</u> v. <u>United States</u>, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to its case against the defendants. The Court rejected the government's suggestion that the district court make that determination ex parte and

### in camera. The Court observed that

[a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Id. at 182. In ordering disclosure of improperly recorded conversations, the Court declared: Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

Id. at 184. Similarly, in Franks v. Delaware, 438 U.S. 154 (1978), the Court held that a

defendant must be permitted to attack the veracity of the affidavit underlying a search warrant,

upon a preliminary showing of an intentional or reckless material falsehood. The Court rested its

decision in significant part on the ex parte nature of the procedure for issuing a search warrant

and the value of adversarial proceedings:

[T]he hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily <u>ex parte</u>, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an <u>ex parte</u> inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be

marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

<u>Id</u>. at 169.

The same considerations that the Supreme Court found compelling in <u>Alderman</u> and <u>Franks</u> militate against ex parte procedures in the FISA context. Without adversarial proceedings, systematic executive branch misconduct went entirely undetected by the FISC until the DOJ chose to reveal it. In light of the almost complete exclusion of criminal defendants and their counsel from the FISA review process, and the correspondingly low risk that misconduct will be detected, it is understandable, if inexcusable, that law enforcement officials "engaged in the often competitive enterprise of ferreting out crime," <u>Johnson v. United States</u>, 333 U.S. 10, 14 (1948), have come to believe that FISA offers a convenient means of circumventing the traditional Title III and search warrant processes.<sup>7</sup>

The protection afforded FISA targets is particularly weak in light of the limited scope of the review performed by the FISC and (if the target is charged with a crime) by the district court. Under 50 U.S.C. § 1805, the FISC "shall" issue an order as requested or modified approving electronic surveillance if it finds, "on the basis of the facts submitted by the applicant," probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power and that the facilities or places at which the surveillance is directed are being used, or are

<sup>&</sup>lt;sup>7</sup> We believe that the complete prohibition courts have erected under § 1806(f) against defense review of FISA applications, orders, and related materials, without consideration of procedures such as set out in the Classified Information Procedures Act, 18 U.S.C. App. III, for providing access to classified information under appropriate protective orders, violates defendants' right to due process under U.S. Const. Amend. V. That issue is not before this Court, however, and we do not address it further.

about to be used, by a foreign power or an agent of a foreign power, and if it further finds that the proposed minimization procedures meet the definition in § 1801(h), that the application contains the certifications required under § 1804 (including a certification as to the purpose of the surveillance), and that the certifications are not "clearly erroneous." 50 U.S.C. § 1805(a); <u>see</u> <u>id</u>. § 1824(a) (similar requirements for issuance of a FISA order authorizing a physical search); <u>Squillacote</u>, 221 F.3d at 553 (summarizing requirements for issuance of a FISA order); <u>Duggan</u>, 743 F.2d at 73-74 (same); Opinion at 9-11 (same).

As <u>Duggan</u> makes clear, the FISC's ex parte review of a FISA application is highly deferential to the executive branch. In particular, the executive's certification concerning the purpose of the surveillance or search--which, as discussed above, has critical constitutional significance--"is, under FISA, subjected to only minimal scrutiny by the courts. . . . The FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." 743 F.2d at 77; <u>see</u> Opinion at 5 ("Since May 1979, [the FISC] has often recognized the expertise of the government in foreign intelligence collection and counterintelligence investigations of espionage and international terrorism, and accorded great weight to the government's interpretation of FISA's standards."). And the subsequent ex parte review by the district court (assuming a criminal prosecution is brought and the defendant challenges the legality of the surveillance) adds little additional protection. According to <u>Duggan</u>, "when a person affected by a FISA surveillance challenges the FISA Court's order, a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has a FISA Judge." 743 F.2d at 77.<sup>8</sup>

<sup>&</sup>lt;sup>8</sup> In a passage that highlights the absence of protections for a FISA target, <u>Duggan</u> notes that a target might be entitled to a <u>Franks</u> hearing concerning the truthfulness of the certifications in a FISA application, but only if he makes a "substantial preliminary showing that a false statement

Not only is judicial review of FISA surveillance and searches invariably in camera and ex parte, therefore, without the benefit of adversarial testing; by statute the review provides "only minimal scrutiny." Given the one-sided proceedings under FISA and the highly deferential standard of review, it is hardly surprising that, according to the Attorney General's annual reports from 1979 to 2001 (available at http://fas.org/irp/agency/doj/fisa), the FISC approved 14,036 applications or extensions authorizing FISA surveillance or searches during that period; it modified only four applications before granting approval; and on one occasion, in 1997, it did not approve the application but granted the DOJ leave to amend and resubmit it. In other words, between 1979 and 2001, the FISC approved without modification 14,031 out of 14,036 applications, or 99.96% of the total. Not once did the court reject outright a FISA application. Nor has subsequent review by district courts presiding over criminal prosecutions proven effective. To our knowledge, no district court has ever suppressed the results of FISA surveillance or a FISA search, and no court of appeals has ever reversed a district court's denial of a motion to suppress FISA information. As these statistics suggest, the purported "additional protection" (to use the DOJ's phrase) of ex parte review under the "minimal scrutiny" standard that FISA contemplates plainly does not justify dispensing with the traditional Fourth Amendment warrant and probable cause requirements when the electronic surveillance or physical search has the primary purpose of gathering evidence for law enforcement use.

knowingly and intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the certification." 743 F.2d at 77 n.6 (quoting <u>Franks</u>, 438 U.S. at 155-56). In the real world of FISA, the purported right that <u>Duggan</u> recognizes is meaningless, because defendants never gain access to the FISA application and the FISC order and thus cannot possibly make a "substantial preliminary showing" that the application contains false statements or that the order relied on those statements.

## CONCLUSION

For the foregoing reasons, the July 19, 2002 decision of the Foreign Intelligence Surveillance Court, incorporating the procedures set forth in that Court's May 17, 2002 decision, should be affirmed. Respectfully submitted,

## JOHN D. CLINE

ZACHARY A. IVES Freedman Boyd Daniels Hollander Goldberg & Cline P.A. 20 First Plaza, Suite 700 Albuquerque, NM 87102 (505) 842-9960

JOSHUA DRATEL Co-Chair, NACDL Amicus Committee 14 Wall St., 28th Floor New York, NY 10005 (212) 732-0707

Counsel for Amicus Curiae National Association of Criminal Defense Lawyers

### **CERTIFICATE OF SERVICE**

I hereby certify that on the 26th day of September, 2002, copies of the foregoing

were sent by first-class mail, postage prepaid, to:

Jonathan L. Marcus Department of Justice 950 Pennsylvania Ave., N.W. Washington, D.C. 20530

Ann Beeson American Civil Liberties Union 125 Broad Street New York, N.Y. 10004

James X. Dempsey Center for Democracy and Technology 1634 Eye Street, N.W., Suite 1100 Washington, D.C. 20006

Kate Martin Center for National Security Studies 1120 19th Street, N.W., Eighth Floor Washington, D.C. 20036

David L. Sobel Electronic Privacy Information Center 1718 Connecticut Ave., N.W., Suite 200 Washington, D.C. 20009

Lee Tien Electronic Frontier Foundation 454 Shotwell Street San Francisco, Cal. 94110

John D. Cline