UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMNESTY INTERNATIONAL USA; GLOBAL FUND FOR WOMEN; GLOBAL RIGHTS; HUMAN RIGHTS WATCH; INTERNATIONAL CRIMINAL DEFENCE ATTORNEYS ASSOCIATION; THE NATION MAGAZINE; PEN AMERICAN CENTER; SERVICE EMPLOYEES INTERNATIONAL UNION; WASHINGTON OFFICE ON LATIN AMERICA; DANIEL N. ARSHACK; DAVID NEVIN; SCOTT MCKAY; and SYLVIA ROYCE,

Plaintiffs,

v.

JOHN M. McCONNELL, in his official capacity as Director of National Intelligence; LT. GEN. KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; and MICHAEL B. MUKASEY, in his official capacity as Attorney General of the Unites States,

Defendants.

MEMORANDUM IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT

Case No. 08-cv-06259 (JKG)

ECF CASE

JAMEEL JAFFER
MELISSA GOODMAN
L. DANIELLE TULLY
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2583
jjaffer@aclu.org

(additional counsel on following page)

NEW YORK CIVIL LIBERTIES UNION FOUNDATION, by
CHRISTOPHER DUNN
ARTHUR EISENBERG
New York Civil Liberties Union
125 Broad Street, 19th Floor
New York, NY 10004
(212) 607-3300

CHARLES S. SIMS
THEODORE K. CHENG
MATTHEW J. MORRIS
Proskauer Rose LLP
1585 Broadway
New York, NY 10036
212-969-3000

September 12, 2008

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

Other Authorities

INTRODUCTION

This case involves a challenge to the constitutionality of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801, *et seq.* ("FISA"), as amended by the FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008) ("FAA" or "Act"). The President signed the FAA into law on July 10, 2008, and plaintiffs commenced this action the same day.

The FAA, which all but eviscerated a regulatory framework that had been in place since 1978, is by far the most sweeping surveillance statute ever enacted by the U.S. Congress. It permits the government to monitor the international communications of U.S. citizens and residents without identifying the people to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without observing meaningful limitations on the retention, analysis, and dissemination of acquired information; without obtaining individualized warrants based on criminal or foreign intelligence probable cause; and, indeed, without even making prior *administrative* determinations that the targets of surveillance are foreign agents or connected in any way, however tenuously, to terrorism. The FAA allows the dragnet acquisition of Americans' international communications, and in some contexts it allows warrantless acquisition of their domestic communications as well.

Under the new law, the executive branch could acquire:

- All telephone and e-mail communications to and from countries of foreign policy interest – for example, Russia, Venezuela, or Israel – including communications made to and from U.S. citizens and residents.

- All telephone and e-mail communications to and from the leaders of the Pakistani lawyers' movement for democracy, with the specific purpose of learning whether those leaders are sharing information with American journalists and, if so, what information is being shared and with which journalists.

- All of the communications of European attorneys who work with American attorneys on behalf of prisoners held at Guantánamo, including communications in which the two sets of attorneys share information about their clients and strategize about litigation.

Indeed, under the new law the executive branch could acquire *all* of the international communications of U.S. citizens and residents on the theory that the surveillance is directed at collecting foreign intelligence information and targeted at people outside the United States. Moreover, the challenged law permits the government to conduct all of this surveillance *inside the United States* with virtually no oversight by the courts and none of the particularized tailoring required by the Constitution.

Plaintiffs are attorneys and human rights, labor, legal, and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States. Because of the nature of their communications and the identities and geographic location of the individuals with whom they communicate, plaintiffs reasonably believe that their communications will be monitored under the challenged law. By effecting an unprecedented expansion of the executive's power to engage in electronic surveillance of U.S. citizens' and residents' communications, the challenged law compromises plaintiffs' ability to gather information, represent their clients, and engage in domestic and international advocacy. It requires plaintiffs to take costly and burdensome measures to protect the confidentiality of sensitive and privileged communications, and it undermines plaintiffs' ability to engage in communications that are relevant and necessary to their work.

The FAA is unconstitutional on its face, and plaintiffs are entitled to judgment as a matter of law. The Act violates the Fourth Amendment by authorizing warrantless and unreasonable

searches. It violates the First Amendment because it sweeps within its ambit constitutionally protected speech that the government has no legitimate interest in acquiring and because it fails to provide adequate procedural safeguards. It violates Article III and the principle of separation of powers because it requires the Foreign Intelligence Surveillance Court ("FISC") to issue advisory opinions on matters that are not cases or controversies and because it permits the executive branch to continue surveillance even if the FISC determines the surveillance to be unconstitutional. Plaintiffs respectfully seek a declaration that the Act is unconstitutional and a permanent injunction against the law's use.

LEGAL AND FACTUAL BACKGROUND

The Foreign Intelligence Surveillance Act

In 1978, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the FISC and empowered it to grant or deny government applications for surveillance orders in foreign intelligence investigations. *See* 50 U.S.C. § 1803(a).

Congress enacted FISA after the U.S. Supreme Court held, in *United States v. United States Dist. Court for the E. Dist. of Mich.* (hereinafter, "*Keith*"), 407 U.S. 297 (1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. FISA was a response to that decision and to years of in-depth congressional investigation that revealed that the executive branch had engaged in widespread warrantless surveillance of U.S. citizens – including journalists, activists, and members of Congress – "who engaged in no criminal activity and who posed no genuine threat to the national security." S. Rep. No. 95-604(I), at 6 (1977), *reprinted at* 1978 U.S.C.C.A.N. 3904, 3909 (internal quotation marks omitted).

Congress has amended FISA multiple times. In its current form, the statute regulates, among other things, "electronic surveillance," which is defined to include:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; [and]
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States . . . .

50 U.S.C. § 1801(f).

Before passage of the FAA, FISA generally foreclosed the government from engaging in "electronic surveillance" without first obtaining an individualized and particularized order from the FISC. To obtain an order, the government was required to submit an application that identified or described the target of the surveillance; explained the government's basis for believing that "the target of the electronic surveillance [was] a foreign power or an agent of a foreign power"; explained the government's basis for believing that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power"; described the procedures the government would use to "minimiz[e]" the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons; described the nature of the foreign intelligence information sought and the type of communications that would be subject to surveillance; and certified that a "significant purpose" of the surveillance was to obtain "foreign intelligence information." *Id.* § 1804(a) (2006). "Foreign intelligence information" was defined

broadly (and is still defined broadly) to include, among other things, information concerning terrorism, national security, and foreign affairs.

The FISC could issue such an order only if it found, *inter alia*, that there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," *id*. § 1805(a)(2)(A); and that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power," *id*. § 1805(a)(2)(B).[1]

The President's Warrantless Surveillance Program

In the fall of 2001, President Bush secretly authorized the National Security Agency ("NSA") to inaugurate a program of warrantless electronic surveillance inside the United States (the "Program"). Plaintiffs' Statement of Undisputed Facts in Support of Motion for Summary Judgment ("SUF") 1A (Jaffer Decl. ¶3, Exh. A). President Bush publicly acknowledged the Program after *The New York Times* reported its existence in December 2005. SUF 1B (Jaffer Decl. ¶4, Exh. B). The President reauthorized the Program repeatedly between 2001 and 2007. SUF 2 (Jaffer Decl. ¶5, Exh. C).

According to public statements made by senior government officials, the Program involved the interception of e-mails and telephone calls that originated or terminated inside the United States. SUF 3A (Jaffer Decl. ¶6, Exh. D). The interceptions were not predicated on judicial warrants or any other form of judicial authorization; nor were they predicated on any determination of criminal or foreign-intelligence probable cause. Instead, according to then-Attorney General Alberto Gonzales and then-NSA Director General Michael Hayden, NSA "shift supervisors" initiated surveillance when in their judgment there was a "reasonable basis to

[1] This Court described FISA in more detail in *United States v. Sattar*, 2003 WL 22137012 (S.D.N.Y. 2003).

conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." SUF 4A, 4B, 5 (Jaffer Decl. ¶¶ 6-8, Exhs. D-F).

On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISC had "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization." SUF 5 (Jaffer Decl. ¶8, Exh. F). The Attorney General further stated that "[a]s a result of these orders, any electronic surveillance that was occurring as part of the [Program] will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court." SUF 5 (Jaffer Decl. ¶8, Exh. F).

The FISC orders issued in January 2007 were modified in the spring of that same year. The modifications reportedly narrowed the authority that the FISC had extended to the executive branch in January. SUF 6, 7 (Jaffer Decl. ¶9, Exh. G). Following the FISC's modification of its January 2007 orders, Director of National Intelligence ("DNI") John M. McConnell appealed to Congress to amend FISA. SUF 8 (Jaffer Decl. ¶10, Exh. H).

The Protect America Act

Congress enacted the Protect America Act in August 2007, Pub. L. No. 110-55 (2007). The Act expanded the executive's surveillance authority and provided legislative sanction for surveillance that the President had previously been conducting under the Program. Because of a "sunset" provision, however, the amendments made by the Protect America Act ceased to have effect on Feb. 17, 2008.

The FISA Amendments Act of 2008

In anticipation of the Protect America Act's expiration, the administration lobbied Congress for permanent changes to FISA. President Bush signed the FAA into law on July 10, 2008. Like the Protect America Act, the FAA provides legislative sanction for the warrantless surveillance of U.S. citizens' and residents' communications. It also provides immunity to telecommunications corporations that facilitated the Program.[2]

While leaving FISA in place insofar as communications *known* to be purely domestic are concerned, the FAA revolutionizes the FISA regime by allowing the mass acquisition of U.S. citizens' and residents' international telephone and e-mail communications.[3] Under section 702(a) of the Act, the Attorney General and DNI can "authorize jointly, for a period of up to one year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." FAA § 702(a). While the Act prohibits the government from, *inter alia*, "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," *id*. § 702(b)(1), an acquisition authorized under section 702(a) may encompass the international communications of U.S. citizens and residents. Indeed, the Attorney General and the DNI may authorize a mass acquisition under section 702(a) even if *all* of the communications to be acquired under the program originate or terminate inside the United States.

[2] While the FAA amended FISA, the provisions of FISA that pre-existed the FAA continue to have effect with respect to foreign intelligence surveillance that does not involve "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." FAA § 702(a). Throughout this brief, plaintiffs use the term "FISA" to refer to the provisions that govern traditional FISA surveillance as distinguished from the provisions that now govern surveillance under the FAA.

[3] Throughout this brief, plaintiffs describe communications as "international" if they either originate or terminate (but not both) outside the United States. Plaintiffs use the phrase "foreign-to-foreign" to refer to communications that both originate and terminate outside the United States.

Before authorizing surveillance under section 702(a) – or, in some circumstances, within seven days of authorizing such surveillance – the Attorney General and the DNI must submit an application for an order (hereinafter, a "mass acquisition order") to the FISC. FAA §§ 702(a), (c)(2). To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISC "a written certification and supporting affidavit" attesting that the FISC has approved, or that the government has submitted to the FISC for approval, procedures ("targeting procedures") reasonably designed to (i) ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and (ii) "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id.* § 702(g)(2)(A)(i). The certification and supporting affidavit must attest that the FISC has approved, or that the government has submitted to the FISC for approval, procedures ("minimization procedures") that meet the definition of "minimization procedures" under 50 U.S.C. §§ 1801(h) or 1821(4). The certification and supporting affidavit must also attest, *inter alia*, that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in section 702(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information." FAA § 702(g)(2)(A)(iii)-(vii).[4]

[4] In addition to giving the executive branch nearly unfettered access to Americans' international communications, the FAA allows the government to acquire some purely domestic communications as well. While the FAA prohibits the government from "intentionally acquir[ing] any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States," FAA § 702(b)(4), this limitation applies only if the government "knows" that the communication is purely domestic; the government possesses this knowledge "at the time of acquisition"; and the government acquires the communication "intentionally." One effect of section 702(b)(4) is to resolve any uncertainty

The Act does not require the government to demonstrate to the FISC that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, e-mail addresses, places, premises, or property at which its surveillance will be directed. FAA § 702(g)(4). Thus, the government may obtain a mass acquisition order without identifying the people (or even the group of people) to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without specifying the particular communications to be collected; without obtaining individualized warrants based on criminal or foreign intelligence probable cause; and without making even a prior administrative determination that the acquisition relates to a particular foreign agent or foreign power. A single mass acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

Equally striking is the Act's failure to place meaningful limits on the government's retention, analysis, and dissemination of information that relates to U.S. citizens and residents. While the Act requires the government to adopt "minimization procedures" that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination of nonpublicly available information concerning unconsenting United States persons," the statute contemplates minimization procedures that are generic and programmatic rather than tailored to the surveillance of individualized targets. Moreover, the statute does not prescribe specific minimization procedures, does not give the FISA court any authority to oversee the

---

about the location of the sender and recipients in favor of the government; if there is uncertainty as to the location of any party to a communication, the communication can be acquired.

implementation of the procedures, and specifically allows the government to retain and disseminate information – including information relating to U.S. citizens and residents – if the government concludes that it is "foreign intelligence information." FAA § 702(e) (referencing 50 U.S.C. §§ 1801(h)(1), 1821(4)(A)). Nothing in the Act forecloses the government from compiling databases of such "foreign intelligence information" and searching those databases for information about specific U.S. citizens and residents. Again, the statute defines the phrase "foreign intelligence information" exceedingly broadly.

The role of the FISC in authorizing and supervising surveillance conducted under the FAA is "narrowly circumscribed." *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted). The FISC is required to issue a mass acquisition order if it finds that the government's certification "contains all the required elements" and that the "targeting and minimization procedures" are consistent with the requirements of the statute and the Fourth Amendment. FAA § 702(i)(3)(A). The FISC does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not supervise the implementation of the government's targeting or minimization procedures. Moreover, even if the FISC rejects the government's certification or procedures, the government "may continue" its surveillance activities during the pendency of any appeal or further court proceedings. *Id*. § 702(i)(4)(B). In other words, the statute permits the government to continue its surveillance activities even if the FISC has concluded that those activities are inconsistent with the statute or are unconstitutional.

The Implications of the FAA for Plaintiffs

Plaintiffs are attorneys and human rights, labor, legal, and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States. SUF 9A (Royce Decl. ¶¶2-6; Mariner Decl. ¶¶2, 5-9; Walsh Decl. ¶¶3, 5; Klein Decl. ¶¶2-4).

Because of the nature of their communications and the identities and geographic location of the individuals with whom they communicate, plaintiffs reasonably believe that their communications will be acquired, analyzed, retained, and disseminated under the challenged law. Some of the plaintiffs communicate by telephone and e-mail with people the United States government believes or believed to be associated with terrorist organizations. SUF 9B (Royce Decl. ¶¶3-6 (discussing Royce's communications in relation to her representation of Mohammedou Ould Salahi, a prisoner held at Guantánamo Bay); Mariner Decl. ¶8 (discussing Mariner's communications with individuals who were previously held in CIA custody abroad); Walsh Decl. ¶6 (discussing WOLA staff members' communications with individuals charged under El Salvador's anti-terrorism legislation)). Some of the plaintiffs communicate by telephone and e-mail with political and human rights activists who oppose governments that are supported economically or militarily by the United States. SUF 9C (Klein Decl. ¶¶6-7 (discussing Klein's communications with foreign political activists and political groups in, among other countries, Colombia); Walsh Decl. ¶6 (discussing WOLA staff members' communications with leaders of protest movements in El Salvador)). Some of the plaintiffs communicate by telephone and e-mail with people located in geographic areas that are a special focus of the U.S. government's counterterrorism or diplomatic efforts. SUF 9D (Mariner Decl.

¶8 (discussing Mariner's communications with people in the Middle East, North Africa, Central Asia, and South Asia); Walsh Decl. ¶¶5, 11 (discussing WOLA staff members' communications with people in, among other countries, Colombia, Cuba, and Venezuela.)). All of the plaintiffs exchange information that constitutes "foreign intelligence information" within the meaning of the FAA. SUF 9E (Royce Decl. ¶8; Mariner Decl. ¶8; Walsh Decl. ¶¶5-6, 8-9, 11; Klein Decl. ¶¶5-6).

The FAA injures plaintiffs by disrupting their ability to engage in confidential communications that are integral to their professional activities. SUF 9G (Royce Decl. ¶¶7-9; Mariner Decl. ¶¶9-11; Walsh Decl. ¶¶ 7, 9-13; Klein Decl. ¶¶7-9). As John Walsh, the Senior Associate responsible for Andes and Drug Policy at plaintiff Washington Office on Latin America ("WOLA"), explains in his declaration:

> I and my colleagues at WOLA depend on our ability to communicate confidentially via telephone and e-mail to forge strong relationships with individuals and organizations abroad. These relationships, and the communications they engender, are essential to our ability to provide insightful and well-grounded analysis to Congress, the administration, the media, and the broader public. Especially in countries in which politics and violence are intertwined, the confidentiality of our international communications is integral to our research, advocacy, and coalition-building work.

SUF 9G (Walsh Decl. ¶7).

The challenged law compromises plaintiffs' ability to locate witnesses, cultivate sources, gather information, communicate confidential information to their clients, and to engage in other legitimate and constitutionally protected communications. SUF 9H (Royce Decl. ¶9; Mariner Decl. ¶10; Walsh Decl. ¶¶9-13; Klein Decl. ¶9). Joanne Mariner, the Terrorism and Counterterrorism Program Director for plaintiff Human Rights Watch, explains that the FAA reduces the likelihood that victims of human rights abuses will share information with her:

> Many of the people with whom I communicate fear reprisals from their own governments, from non-governmental actors (including terrorist organizations), and from the United States government. These individuals share information with me because they trust me to treat their information with appropriate sensitivity . . . . By significantly increasing the likelihood that my communications will be acquired by the U.S. government, the new surveillance law compromises my ability to gather information that is relevant and necessary to my work.

SUF 9H (Mariner Decl. ¶¶9-10); *see also* SUF 9F (Walsh Decl. ¶8 (explaining that some of Mr. Walsh's sources in Colombia share information with Mr. Walsh on condition of anonymity and that many would not communicate with him if they believed their identities would not be kept confidential)).

The challenged law also has serious ramifications for those of the plaintiffs who are journalists. Naomi Klein, an investigative reporter and regular contributor to *The Nation* magazine, explains that many of her sources live under repressive governments that the United States supports economically and militarily:

> Some of my sources will decline to share information with me if they believe that their communications are being monitored by the United States. In some cases they fear that the United States itself will retaliate against them for their political activities – for example, by placing them on "watch lists" and refusing them visas should they try to visit the United States. More often, though, they fear that the United States will share information about them with their own governments, and that their own governments will retaliate against them as a result.

SUF 9G (Klein Decl. ¶8).

The challenged law has particularly serious consequences for those of the plaintiffs who are attorneys. SUF 9H (Royce Decl. ¶¶6-9). Sylvia Royce, a defense attorney, explains that the challenged law impairs her ability to represent her client at Guantánamo because, among other things, it forces her to limit the information she shares with experts, witnesses, and co-counsel who reside outside of the United States. As Ms. Royce explains in her declaration:

> I would like to have an open exchange of views on legal strategy with my co-counsel, but I have a duty not to allow client confidences and legal strategy to by captured by persons outside the attorney-client relationship, and least of all by the U.S. government, which in this case is the opposing party.

SUF 9H (Royce Decl. ¶7).

The challenged law also forces plaintiffs to take costly and burdensome measures to protect the confidentiality of sensitive and privileged communications. SUF 9K (Mariner Decl. ¶10 (stating that she will have to resort to time-consuming, costly, and sometime dangerous travel abroad to gather information in person that she would have otherwise gathered by telephone or e-mail); Klein Decl. ¶9 (same)).

While some of the plaintiffs have operated under the threat of government surveillance – either by the U.S. government or by other governments – in the past, the new law has a much greater impact on their work. SUF 9L (Walsh Decl. ¶11). As Ms. Mariner explains:

> Given the nature and geographic focus of my work, the risk of government surveillance is not entirely new, and I have always used passwords and encryption to protect the confidentiality of my information and communications. In the past, however, U.S. government surveillance was both narrow and judicially supervised. I am concerned that now the U.S. government may be able to engage in almost entirely unsupervised surveillance and this surveillance can be directed very broadly and at anyone at all – at political dissidents, foreign government officials, witnesses, experts, human rights organizations (including, for example, Human Rights Watch's counterparts in other countries), or even victims of human rights abuses who are not suspected of having done anything wrong. This kind of unchecked surveillance has much more significant implications for my work and the work of other human rights researchers. A risk that was previously limited to a subset of communications with a small subset of people is now a risk that we must evaluate and address every time we make an international telephone call or send an e-mail to an individual located abroad.

SUF 9L (Mariner Decl. ¶11).

ARGUMENT

Summary judgment is appropriate if "there is no genuine issue as to any material fact and . . . the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c); *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Anderson v. Liberty Lobby, Inc*., 477 U.S. 242, 247 (1986); *Lang v. Retirement Living Publ'g Co*., 949 F.2d 576, 580 (2d Cir. 1991).

I. THE FAA VIOLATES THE FOURTH AMENDMENT.

A. The FAA authorizes "general searches" that the Framers specifically foreclosed.

"The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists." *Virginia v. Moore*, 128 S.Ct. 1598, 1603 (2008); *see also Steagald v. United States*, 451 U.S. 204, 220 (1981); *Boyd v. United States*, 116 U.S. 616, 627 (1886). In England, general warrants had been employed to discover the authors of allegedly seditious libel. *See* Nelson B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution, in* The Johns Hopkins University Studies in Historical and Political Science, 43-50, vol. LV, no. 2 (Baltimore: The Johns Hopkins Press, 1937) (hereinafter "Lasson"). Some of the warrants were related to a specific incident but "general as to the persons to be arrested and the places to be searched and the papers to be seized." *Id.* at 43. Others were "specific as to the person but general as to papers" to be searched. *Id.* at 47.

Writs of assistance, which were used in the colonies, invested government officials with similarly sweeping authority. They gave "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965). They "were not restricted to searches of specific places or to seizures of specific goods," "did not require either an oath or information supplying cause," and "survived

indefinitely." Morgan Cloud, *Searching Through History; Searching For History*, 63 U. Chi. L. Rev. 1707, 1738 (1996); *see also* Barbara C. Salken, *The General Warrant of the Twentieth Century? A Fourth Amendment Solution to Unchecked Discretion to Arrest for Traffic Offenses*, 62 Temp. L. Rev. 221, 254 (1989) (hereinafter "Salken") (officers "decide[d] whom to search and for what to search" without "a showing of individualized suspicion"). The writs were thought to be even more pernicious than the British general warrants, because whereas general warrants were often connected to particular cases of libel and limited in object and time, Lasson at 54, writs were "not returnable at all after execution," granted search authority for the life of the sovereign, and gave the searching officer "absolute and unlimited" discretion, *id*. James Otis denounced the writs as "the worst instrument of arbitrary power." *Stanford*, 379 U.S. at 481.[5]

The Framers crafted the Fourth Amendment to guard against those aspects of general searches and writs of assistance that they found most objectionable: the lack of judicial oversight; the lack of any individualized suspicion requirement; the lack of any meaningful limitation on the scope of a search or on the duration of the search authority; and the absence of any requirement that the authorizing document specifically describe the persons, places, or things to be searched. *See, e.g.*, Salken at 256; *see also* William John Cuddihy, The Fourth Amendment: Origins and Original Meaning 1499 (1990) (unpublished Ph.D. dissertation at Claremont Graduate School) (stating that the "[p]rohibition of the general warrant was part of a larger scheme to extinguish general searches more categorically").

[5] Notably, "[t]he historic occasion of that denunciation, in 1761 at Boston, has been characterized as 'perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. 'Then and there,' said John Adams, 'then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'" *Payton v. New York*, 445 U.S. 573, 584 n.21 (1980).

Although the searches the FAA authorizes are electronic rather than physical, the Act invests government officers with precisely the powers that the Fourth Amendment was meant to extinguish. As discussed further below, the Act permits the government to conduct dragnet surveillance that may implicate the privacy rights of thousands or millions of U.S. citizens and residents who have no connection to foreign powers or criminal activity. The Act permits the government to conduct exactly the kinds of searches that the Framers were most intent on foreclosing. *Cf. Berger v. New York*, 388 U.S. 41, 49 (1967) (striking down electronic surveillance statute that, like "general warrants," left "too much to the discretion of the officer executing the order" and gave the government "a roving commission to seize any and all conversations" (internal quotation marks omitted)).

B. Residents of the United States have a constitutionally protected privacy interest in the content of their telephone calls and e-mails.

Citizens and residents of the United States have a constitutionally protected privacy interest in the content of their telephone calls and e-mails. *United States v. Katz*, 389 U.S. 347, 353 (1967); *see also Keith*, 407 U.S. at 313 ("[*Katz*] implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."); *Alderman v. United States*, 394 U.S. 165, 177 (1969) ("the Fourth Amendment protects a person's private conversations as well as his private premises"). In *Berger*, the Supreme Court struck down a New York statute that permitted the collection of evidence through the installation of electronic eavesdropping devices, noting that "[b]y its very nature eavesdropping involves an intrusion on privacy that is broad in scope," 388 U.S. at 56, and that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices," *id*. at 63. Holding the statute unconstitutional, the Court wrote: "[I]t 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." *Id*. at 63.

The Fourth Amendment's protection extends not just to domestic communications but to international communications as well. Thus the Supreme Court found that the Fourth Amendment was implicated in *United States v. Ramsey*, 431 U.S. 606, 616-20 (1977), which concerned a statute that authorized customs officers to open envelopes and packages sent from outside the United States. *See also Birnbaum v. United States*, 588 F.2d 319, 325 (2d Cir. 1979); *United States v. Doe*, 472 F.2d 982, 984 (2d Cir. 1973). More recently, Judge Sand found that the Fourth Amendment was implicated by the government's electronic surveillance of a U.S. citizen living in Kenya – though by definition *all* of that person's telephone calls were international or foreign-to-foreign. *United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000). The Second Circuit and other courts have held that the Fourth Amendment is engaged even by *foreign* governments' surveillance of Americans abroad if the U.S. government is sufficiently involved in the surveillance. *See United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992); *United States v. Peterson*, 812 F.2d 486 (9th Cir. 1987); *Berlin Democratic Club v. Rumsfeld*, 410 F. Supp. 144 (D.D.C. 1976). These courts, like Judge Sand in *Bin Laden*, reached this conclusion even though all of the communications at issue were international or foreign-to-foreign.

The Supreme Court has repeatedly underscored that the Fourth Amendment is implicated by "governmental incursions into conversational privacy." *Keith*, 407 U.S. at 313. In the context presented here, the Fourth Amendment's procedural protections are of special significance because of the risk that "unrestricted power of search and seizure" will be used as "an instrument for stifling liberty of expression." *Marcus v. Search Warrant*, 367 U.S. 717, 729

(1961). The Supreme Court has emphasized time and again that, where government surveillance implicates rights protected by the First Amendment, "the requirements of the Fourth Amendment must be applied with scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (internal quotation marks omitted); *see also Maryland v. Macon*, 472 U.S. 463, 468 (1985); *Stanford*, 379 U.S. at 485.

C. The FAA violates the Fourth Amendment's warrant clause.

i. The warrant clause forecloses the government from conducting searches without prior judicial authorization based on probable cause and describing with particularity the things to be seized and the place to be searched.

The Fourth Amendment requires that search warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Supreme Court has interpreted these words to require three things: first, that any warrant be issued by a neutral, disinterested magistrate; second, that those seeking the warrant demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense; and third, that any warrant particularly describe the things to be seized as well as the place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979). Warrantless searches are "*per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." *United States v. Karo*, 468 U.S. 705, 717 (1984); *Payton*, 445 U.S. 573; *Chimel v. California*, 395 U.S. 752, 768 (1969); *Katz*, 389 U.S. at 357.

More than two centuries of jurisprudence have invested the requirements of the warrant clause with clear content. The requirement of a "neutral, disinterested magistrate" is a requirement that that "the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police." *Katz*, 389 U.S. at 357; *see also Shadwick v. City of Tampa*,

407 U.S. 345, 350 (1972) (stating that a "neutral, disinterested magistrate" must be someone other than an executive officer "engaged in the often competitive enterprise of ferreting out crime"); *Keith*, 407 U.S. at 316-17 ("The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised."); *McDonald v. United States*, 335 U.S. 451, 455-56 (1948) ("The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals.").

The requirement of probable cause is meant to ensure that "baseless searches shall not proceed." *Keith* at 316. Probable cause "is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness." *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 534 (1967).

The requirement of particularity, finally, is meant to "limit[] the authorization to search to the specific areas and things for which there is probable cause to search" in order to "ensure[] that the search will be carefully tailored." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also United States v. Silberman*, 732 F. Supp. 1057, 1061-62 (1990) ("[T]he particularity clause requires that a statute authorizing a search or seizure must provide some means of limiting the place to be searched in a manner sufficient to protect a person's legitimate right to be free from unreasonable searches and seizures."); *see also United States v. Bianco*, 998 F.2d 1112, 1115 (2d Cir. 1993) (stating that the particularlity requirement "prevents a general, exploratory rummaging in a person's belongings" (internal quotation marks omitted)). The particularity requirement is designed to leave nothing "to the discretion of the officer executing the warrant." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976).

The Supreme Court has said that the importance of the particularity requirement "is especially great in the case of eavesdropping" because eavesdropping inevitably leads to the interception of intimate conversations that are unrelated to the investigation. *Berger*, 388 U.S. at 65 (Douglas, J., concurring) ("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."); *see also United States v. Tortorello*, 480 F.2d 764, 779 (2d Cir. 1973). In the context of electronic surveillance, the requirement of particularity generally demands that the government identify or describe the person to be surveilled, the facilities to be monitored, as well as the particular communications to be seized. *United States v. Donovan*, 429 U.S. 413, 427 n.15 & 428 (1977).

ii. The requirements of the warrant clause apply to surveillance conducted under the FAA.

The requirements of the warrant clause apply to the government's surveillance of Americans' telephone and e-mail communications. *Dalia*, 441 U.S. at 256 n.18 ("electronic surveillance undeniably is a Fourth Amendment intrusion requiring a warrant"); *Keith*, 407 U.S. at 313 ("the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitates the application of Fourth Amendment safeguards"); *Katz*, 389 U.S. at 356; *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985) ("even narrowly circumscribed electronic surveillance must have prior judicial sanction"); *Tortorello*, 480 F.2d at 773.[6]

[6] The courts have recognized an exception to the warrant requirement "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). The special needs cases have no relevance

The warrant requirement applies not only to surveillance conducted for law enforcement purposes but to surveillance conducted for intelligence purposes as well. In *Keith*, the government argued that the President, acting through the Attorney General, could constitutionally "authorize electronic surveillance in internal security matters without prior judicial approval." *Keith*, 407 U.S. at 299. In support of its position, the government argued that surveillance conducted for intelligence purposes "should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity"; that courts "have neither the knowledge nor the techniques necessary to determine whether there was probable cause to believe that surveillance was necessary to protect national security"; and that judicial oversight of intelligence surveillance "would create serious potential dangers to the national security and to the lives of informants and agents." *Id*. at 319.

The Court emphatically rejected these arguments. To the government's effort to distinguish intelligence surveillance from law enforcement surveillance, the court wrote that "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech." *Id*. at 320. To the government's claim that security matters would be "too subtle and complex for judicial evaluation," the Court responded that the judiciary "regularly deal[s] with the most difficult issues of our society" and that there was "no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases." *Id*.; *see also id*. ("If a threat is too subtle or complex for our senior law enforcement officers to convey

---

here, however, because, as discussed below, the country's experience with FISA shows that a warrant and probable cause requirement are workable. Moreover, the special needs exception has generally been limited to contexts in which the search is minimally intrusive and the discretion of executive officers is strictly confined. *See, e.g.*, *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 624 (1989). Neither of these things is true under the FAA.

its significance to a court, one may question whether there is probable cause for surveillance."). Finally, to the government's contention that the warrant requirement would "fracture the secrecy essential to official intelligence gathering," the Court responded that the judiciary had experience dealing with sensitive and confidential matters and that in any event warrant application proceedings were ordinarily *ex parte*. *Id*. at 320-21.

Keith involved surveillance conducted for domestic intelligence purposes, but foreign intelligence surveillance, like domestic intelligence surveillance, must be conducted in compliance with the Constitution. *See, e.g.*, *United States v. Curtiss-Wright*, 299 U.S. 304, 320 (1967); *Home Bldg. & Loan Ass'n v. Blaisdell*, 290 U.S. 398 (1934); *United States v. Butenko*, 494 F.2d 593, 603 (3d Cir. 1974); *see also Coolidge v. New Hampshire*, 403 U.S. 443, 461 (1971); *Bin Laden*, 126 F. Supp. 2d at 273. This is certainly true of surveillance that, like the surveillance conducted under the FAA, is effected inside the United States. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 278 (1990) (Kennedy, J., concurring) (finding that a warrant was not required for the search of a non-resident alien's home in Mexico but stating that "[i]f the search had occurred in a residence within the United States, I have little doubt that the full protections of the Fourth Amendment would apply"); H.R. Rep. No. 110-373, at 15 n.26 (2007) ("In judging the reasonableness of the search . . . the location of the intercept can be as important as the location of the U.S. person under surveillance.").

All of the *Keith* Court's reasons for refusing to exempt domestic intelligence surveillance from the warrant requirement apply with equal force to foreign intelligence surveillance as well – and certainly to foreign intelligence surveillance conducted inside the United States. First, intelligence surveillance conducted inside the United States presents the same risks to "constitutionally protected privacy of speech" whether the asserted threats are foreign or

domestic in origin; both forms of surveillance can be used to "oversee political dissent" and both forms of surveillance could as easily lead to the "indiscriminate wiretapping and bugging of law-abiding citizens" that the *Keith* Court feared. *See Keith*, 407 U.S. at 321; *see also* S. Rep. No. 95-701, *reprinted at* 1978 U.S.C.C.A.N. at 3984 (stating Senate Intelligence Committee's judgment that the arguments in favor of prior judicial review "apply with even greater force to foreign counterintelligence surveillance"). The risks are even greater if, as under the FAA, there is no requirement that the government's surveillance activities be directed at specific foreign agents. This major deficiency in the FAA is discussed further below. *See* section I.C.iii.[7]

Second, the courts are just as capable of overseeing intelligence surveillance relating to foreign threats as they are of overseeing intelligence surveillance relating to domestic threats. Indeed, for the past 30 years, the courts *have* been overseeing intelligence surveillance relating to agents of foreign powers because, since its enactment in 1978, FISA has required the government to obtain individualized judicial authorization – based on probable cause that the target is an agent of a foreign power – before conducting foreign intelligence surveillance inside the nation's borders. There is nothing unworkable about FISA's core requirement of judicial authorization. Since 1978, the government has brought literally dozens of prosecutions based on evidence obtained through FISA. *See e.g., Sattar*, 2003 WL 22137012 at *6 (collecting cases); *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va.1997) (same). Moreover, reports issued by the Justice Department indicate that, of the 25,358 FISA applications submitted

[7] Notably, in *Keith* the government argued that it would be difficult if not impossible to distinguish domestic threats from foreign ones. *See Zweibon v. Mitchell*, 516 F.2d 594, 652 (D.C. Cir. 1975) (en banc) (plurality opinion) (discussing the Solicitor General's brief in *Keith*); *United States v. Hoffman*, 334 F. Supp. 504, 506 (D.D.C. 1971) ("The government contends that foreign and domestic affairs are inextricably intertwined and that any attempt to legally distinguish the impact of foreign affairs from the matters of internal subversive activities is an exercise in futility.").

by the executive branch between 1978 and 2007, the FISA Court granted 24,950 without modification, granted 399 with modification, and denied only nine. *See* FISA Annual Reports to Congress 1979-2007, *at* http://www.fas.org/irp/agency/doj/fisa/#rept. Thus, FISA judges have granted virtually every application that the government has submitted.

Finally, the country's experience with FISA also shows that judicial oversight can operate without compromising the secrecy that is necessary in the intelligence context. The FISC meets in secret, rarely publishes its opinions, and generally allows only the government to appear before it. *See In re Motion for Release of Court Records*, 526 F. Supp. 2d. 484, 488 (FISA Ct. 2007) ("Other courts operate primarily in public, with secrecy the exception; the FISC operates primarily in secret, with public access the exception."). The entire system is organized around the need to preserve the confidentiality of sources and methods. To plaintiffs' knowledge, the executive branch has never suggested that the oversight of the FISA court presents a danger to national security. Indeed, in recent years some experts have questioned whether the FISA system is *too* secretive.[8]

In the wake of *Keith*, the D.C. Circuit suggested that a warrant should be required even for foreign intelligence surveillance directed at suspected foreign powers and agents. *Zweibon*, 516 F.2d at 614 (stating *in dicta* that "we believe that an analysis of the policies implicated by

[8] *See* Secret Law and the Threat to Democratic and Accountable Government: Hearing Before the Subcomm. on the Constitution of the Senate Judiciary Committee, 110th Cong. (2008) (testimony of J. William Leonard, Former Director Information Security Oversight Office) (stating, with respect to recent opinions of the FISA Court, "When you think about the significant surveillance capability that this government has, I think it's [of] profound interest [to] every American to know to what extent and under what circumstances they may in fact be subject to government surveillance."); *id*. (testimony of Steven Aftergood, Director, Project on Government Secrecy, Federation of American Scientists) ("[I]t has become evident that there is a body of common law derived from the decisions of the Foreign Intelligence Surveillance Court that potentially implicates the privacy interests of all Americans. Yet knowledge of that law is deliberately withheld from the public. In this way, 'secret law' has been normalized to a previously unknown extent and to the detriment, I believe, of American democracy.").

foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional"); *Berlin Democratic Club*, 410 F. Supp. at 159. While other circuit courts recognized a foreign intelligence exception, *see., e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-15 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *Butenko*, 494 F.2d at 604-05; *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973), all of these cases involved surveillance conducted before the enactment of FISA, and FISA seriously undermines their rationale, *see Bin Laden*, 126 F. Supp. 2d at 272 n.8.[9] Equally important here, these cases limited the foreign intelligence exception to contexts in which (i) the government's surveillance was directed at a specific foreign agent or foreign power; (ii) the government's primary purpose was to gather foreign intelligence information; and (iii) and either the President or Attorney General personally approved the surveillance. *See Truong*, 629 F.2d at 912; *United States v. Ehrlichman*, 546 F.2d 910, 925 (D.C. Cir. 1976); *Bin Laden*, 126 F. Supp. 2d at 277. The FAA contains none of these limitations.

iii. The FAA authorizes the executive branch to conduct surveillance without compliance with the warrant requirement.

The FAA authorizes the executive branch to conduct electronic surveillance without compliance with the warrant clause. First, the Act fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Katz*, 389 U.S. at 357. While the government may not initiate an acquisition under section 702(a) without first applying for a mass acquisition order from the FISC (or obtaining such an order within seven days of initiating the acquisition), the FISC's role in this context is to review general procedures relating

[9] In *In re Sealed Case*, the Foreign Intelligence Surveillance Court of Review noted that pre-FISA cases had recognized a foreign intelligence exception, but the Court did not reach the issue itself. 310 F.3d 717, 742 (FISA Ct. Rev., 2002).

to targeting and minimization; every decision relevant to the surveillance of *specific* surveillance targets is made by executive officers and never presented to the FISC. Indeed nothing in the Act requires the government even to *inform* the Court who its surveillance targets are (beyond to say that the targets are outside the United States), what the purpose of its surveillance is (beyond to say that a "significant purpose" of the surveillance is foreign intelligence), or which Americans' privacy is likely to be implicated by the acquisition. *Cf.* 18 U.S.C. § 2518(1)(b) (requiring government's application for Title III warrant to include, *inter alia*, details as to the particular offense that has been committed, a description of the nature and location of facilities to be monitored, a description of the type of communications to be intercepted, and the identity of the individual to be monitored); 50 U.S.C. § 1804(a) (setting out similar requirements for FISA warrants). The Fourth Amendment reflects a judgment that "[t]he right of privacy [is] too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals," *McDonald*, 335 U.S. at 455-56, but this is precisely what the FAA does: it entrusts to the discretion of the executive branch – the *unreviewed* discretion of the executive branch – the decisions that affect the privacy rights of Americans.

Second, the Act fails to condition government surveillance on the existence of probable cause. The Act permits the government to conduct acquisitions under section 702(a) without proving to a court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. *Cf.* 18 U.S.C. § 2518(3) (permitting government to conduct surveillance under Title III only after court makes probable cause determination) *and* 50 U.S.C. § 1805(a)(2) (corresponding provision for FISA). Indeed, the FAA permits the government to conduct acquisitions without even making an *administrative* determination that its targets fall into any of these categories. Accordingly, the government's surveillance targets may

be political activists, victims of human rights abuses, journalists, or researchers. The government's targets may even be entire geographic regions. *See* Letter from Att'y Gen. Michael B. Mukasey and DNI McConnell to Hon. Harry Reid (Feb. 5, 2008) (arguing that the intelligence community should not be prevented "from targeting a particular group of buildings or a geographic area abroad"). Theoretically, the government's target could be "the United Kingdom" or "the Middle East." It is important to recognize that the absence of an individualized suspicion requirement has ramifications for U.S. citizens and residents even though the government's ostensible targets are foreign citizens outside the United States. The absence of an individualized suspicion requirement means that the government can engage in the wholesale collection of *Americans'* international communications – that it can, for example, knowingly and intentionally collect all communications between the New York and London offices of Amnesty International, or that it can collect all communications between Human Rights Watch in New York and human rights researchers in South and Central Asia. Indeed, under the FAA the government can obtain *all* communications between New York and London so long as the ostensible targets for this mass acquisition are non-U.S. persons believed to be in the United Kingdom.[10]

Third, the Act fails to impose any meaningful limit on the scope of surveillance conducted under the Act. Unlike FISA, it does not require the government to identify the

[10] As noted above, even the NSA's warrantless wiretapping program permitted judicially unsupervised surveillance only after an administrative determination that there was a "reasonable basis" to believe that one party to the communication was "a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." The FAA lacks even this protection. *See* Cong. Rec. S568 (February 4, 2008) ("Even the administration's illegal warrantless wiretapping program, as described when it was publicly confirmed in 2005, at least focused on particular al-Qaida terrorists. But what we are talking about now is different. This is the authority to conduct a huge dragnet that will sweep up innocent Americans at home, combines with and utter lack of oversight mechanisms to prevent abuse" (statement of Sen. Feingold during debate on S. 2248, FISA Amendments Act of 2008)).

individuals to be monitored. *Cf.* 18 U.S.C. § 2518(1)(b)(iv) (requiring Title III application to include "the identity of the person, if known, committing the offense and whose communications are to be intercepted"); 50 U.S.C. § 1804(a)(2) (requiring FISA application to describe "the identity, if known, or a description of the target of the electronic surveillance"). It does not require the government to identify the facilities, telephone lines, e-mail addresses, places, premises, or property at which its surveillance will be directed. *Cf.* 18 U.S.C. § 2518(1)(b)(ii); 50 U.S.C. § 1804(a)(3)(b). It does not limit the kinds of communications the government can acquire, beyond requiring that a programmatic purpose of the government's surveillance be to gather foreign intelligence. *Cf.* 50 U.S.C. § 1804(a)(6) (allowing issuance of FISA order only upon certification that a significant purpose *of the specific intercept* is to obtain foreign intelligence information). Nor does it require the government to identify "the particular conversations to be seized." *Donovan*, 429 U.S. at 427 n.15; *cf.* 18 U.S.C. § 2518(1)(b)(iii); 50 U.S.C. § 1804(a)(6). Nor, finally, does it place any reasonable limit on the duration of mass acquisition orders. *Compare* FAA § 702(a) (allowing surveillance programs to continue for up to 1 year), *with* 50 U.S.C. § 1805(d)(1) (providing that surveillance orders issued under FISA are generally limited to 90 or 120 days) *and* 18 U.S.C. § 2518(5) (providing that surveillance orders issued under Title III are limited to 30 days). The FAA simply does not ensure that surveillance conducted under the Act "will be carefully tailored." *Garrison*, 480 U.S. at 84.

In sum, the FAA invests executive officers with the power to conduct highly intrusive surveillance without complying with the most fundamental requirements of the Fourth Amendment. The Act cannot survive constitutional scrutiny.

D.

The FAA violates the Fourth Amendment's reasonableness requirement.

As discussed above, the FAA is unconstitutional because it permits the executive to conduct surveillance without compliance with the warrant clause. However, the Act would be unconstitutional even if the warrant clause were inapplicable, because "the ultimate touchstone of the Fourth Amendment" is "reasonableness," *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006), and the reasonableness requirement applies even where the warrant requirement does not, *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985); *United States v. Glaziou*, 402 F.2d 8 (2d Cir. 1968); *Truong*, 629 F.2d at 916; *Bin Laden*, 126 F. Supp. 2d at 277 ("[a]ll warrantless searches are still governed by the reasonableness requirement"); *see also In re Sealed Case*, 310 F.3d 717, 737 (For. Int. Surv. Ct. Rev., 2002) (assessing reasonableness of FISA); *Figueroa*, 757 F.2d at 471-72 (assessing reasonableness of Title III); *United States v. Duggan*, 743 F.2d 59, 74 (2d Cir. 1984) (assessing reasonableness of FISA); *Tortorello*, 480 F.2d 764 (same). Reasonableness is determined by examining the "totality of circumstances" to "assess[ ], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (internal quotation marks omitted); *see also Virginia v. Moore*, 128 S.Ct. at 1603.

In the context of electronic surveillance, reasonableness demands that statutes have "precise and discriminate" requirements and that the government's surveillance authority is "carefully circumscribed so as to prevent unauthorized invasions of privacy." *Berger*, 388 U.S. at 58 (internal quotation marks omitted); *see also United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973) ("we must look . . . to the totality of the circumstances and the overall impact of the statute to see if it authorizes indiscriminate and irresponsible use of electronic surveillance or if it

authorizes a reasonable search under the Fourth Amendment" (emphasis added)). As discussed above, *see* sections I.A, B, in *Berger* the Supreme Court found New York's wiretapping law to be unreasonable because it gave executive officers "a roving commission to 'seize' any and all conversations" and provided a "blanket grant of permission to eavesdrop without adequate judicial supervision or protective procedures." *Berger*, 388 U.S. at 60.

Courts that have assessed the reasonableness of electronic surveillance have routinely looked to FISA and Title III as a measure of reasonableness. *See, e.g., United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986) (evaluating reasonableness of video surveillance); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1438 (10th Cir. 1990) (same); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987) (same); *United States v. Torres*, 751 F.2d 875, 884 (7th Cir. 1984) (same). While the constitutional limitations on foreign intelligence surveillance may differ in some respects from those applicable to law enforcement surveillance, *Keith*, 407 U.S. at 323-24, "the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns," *In re Sealed Case*, 310 F.3d at 737.

Under the factors the courts have traditionally considered in evaluating the constitutionality of surveillance statutes, the FAA is plainly unreasonable.

i. <u>The FAA fails to require the government to identify the people to be surveilled or the facilities to be monitored.</u>

As noted above, *see* section I.C.iii, the FAA departs radically from FISA and Title III by permitting the government to engage in intrusive surveillance without ever identifying its surveillance targets to a court. *See* 50 U.S.C. § 1804(a)(2) (requiring application for FISA order to include "the identity, if known, or a description of the specific target of the electronic surveillance"); 18 U.S.C. § 2518(1)(b) (requiring application for Title III order to include "the identity of the person, if known, committing the offense and whose communications are to be

intercepted"); *see also Donovan*, 429 U.S. at 428; *United States v. Kahn*, 415 U.S. 143 (1974) (noting that Title III generally requires government to identify targets for which it has probable cause). The FAA also departs from FISA and Title III by failing to require the government to identify the facilities – for example, the telephone numbers or e-mail addresses – that it intends to monitor. *Compare* FAA § 702(g)(4) ("[a] certification made under this subsection is *not* required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted" (emphasis added)) *with* 18 U.S.C. § 2518(1)(b)(ii) (requiring description of nature and location of targeted facilities) *and* 50 U.S.C. § 1804(a)(3)(b) (requiring government to supply basis for belief that facilities to be targeted are being used by foreign power or agent of foreign power).

Notably, these two requirements – that the government identify the people to be surveilled and the facilities to be monitored – are meant to protect the rights of third parties whose communications may be overheard incidentally. *See, e.g.*, *Bianco*, 998 F.2d at 1124 (stating that requirement that government identify the person to be surveillance "protects the fourth amendment interests of innocent third parties" (internal quotation marks omitted)); *see also Silberman*, 732 F. Supp. at 1062.

The FAA's failure to require the government to identify the people to be surveilled and the facilities to be monitored is sufficient in itself to render the statute unconstitutional. Many of the courts that have upheld FISA and Title III against constitutional challenge have referenced or expressly relied on those statutes' identification requirements. *See, e.g.*, *Duggan*, 743 F.2d at 73 (FISA); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (FISA); *Tortorello*, 480 F.2d at 773 (Title III). To plaintiffs' knowledge, no court has *ever* upheld a surveillance statute that did not require the government to identify either the people to be surveilled or the facilities

to be monitored. To the contrary, the Supreme Court has strongly suggested that such a statute would be unconstitutional. *Cf. Kahn*, 415 U.S. at 155 n.15 ("a warrant failing to name the owner of the premises at which a search is directed, while not the best practice, has been held to pass muster under the Fourth Amendment" but only "as long as the property to be seized is described with sufficient specificity"); *see also Bianco*, 998 F.2d at 1124 (upholding constitutionality of "roving bug" warrant that did not specify facilities but noting that the warrant specified, among other things, the identities of the people to be surveilled). By failing to require the government to identify its surveillance targets, the FAA licenses exactly what the Supreme Court sought to foreclose in *Berger* – a "roving commission to 'seize' any and all conversations."

ii. The FAA fails to require a judicial (or even administrative) determination of individualized suspicion.

The FAA also departs from FISA and Title III by allowing the seizure and review of communications without a judicial – or even administrative – determination of individualized suspicion. *See* section I.C.iii, *supra*. There is no requirement that the government show that the targets of its surveillance are foreign agents, engaged in criminal activity, or even associated with terrorism. Nor does the FAA require an *administrative* determination of individualized suspicion. Again, this is a deficiency that distinguishes the FAA from even the NSA's warrantless wiretapping program.

The absence of an individualized suspicion requirement renders the FAA unconstitutional. "To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing." *Chandler v. Miller*, 520 U.S. 305, 313 (1997); *Chambers v. Maroney*, 399 U.S. 42, 51 (1970) ("In enforcing the Fourth Amendment's prohibition against unreasonable searches and seizures, the Court has insisted upon probable cause as a minimum requirement for a reasonable search permitted by the Constitution."). As a

general matter, the courts have insisted on individualized suspicion even when a warrant is not required. *See, e.g.*, *Kirk v. Louisiana*, 536 U.S. 635, 638 (2002); *United States v. Watson*, 423 U.S. 411, 423-24 (1976); *Carroll v. United States*, 267 U.S. 132 (1925); *United States v. Asbury*, 586 F.2d 973 (2d Cir. 1978); *United States v. Cardona-Sandoval*, 6 F.3d 15, 23 (1st Cir. 1993).[11]

Courts that have upheld Title III and FISA against constitutional challenges have relied in part on those statutes' individualized suspicion provisions. *See, e.g.*, *Duggan*, 743 F.2d at 73 (FISA); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (FISA); *Pelton*, 835 F.2d at 1075 (FISA); *Tortorello*, 480 F.2d at 773 (Title III); *In the matter of Kevork*, 634 F. Supp. 1002, 1013 (C.D. Cal. 1985) (FISA), *aff'd*, 788 F.2d 566 (9th Cir. 1986); *United States v. Falvey*, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (finding FISA reasonable because, *inter alia*, "it require[d] that a federal district court judge – not the Executive branch – make a finding of probable cause to believe that the target of surveillance is an agent of a foreign power" and provides "an effective external control on arbitrary executive action" (internal quotation marks omitted)).

The absence of an individualized suspicion requirement is sufficient in itself to render the FAA unreasonable.

iii. <u>The FAA fails to limit the scope and nature of the communications to be acquired.</u>

The FAA also departs from FISA and Title III in failing to meaningfully limit the scope and nature of communications that the government can obtain under the Act. *Cf.* Cong. Rec. H5770 (June 20, 2008) (statement of Rep. Speier during debate on H.R. 6304) ("It is fundamentally untrue to say that Americans will not be placed under surveillance after this bill

[11] Courts have relaxed the individualized suspicion requirement in cases involving "special needs," but as discussed above, *see* note 6, those cases have no application here.

becomes law. The truth is, any American will subject their phone and e-mail conversations to the broad government surveillance web simply by calling a son or daughter studying abroad, sending an e-mail to a foreign relative, even calling an American company whose customer service center is located overseas.") First, the Act allows the government to authorize acquisitions "to obtain foreign intelligence information," but it defines that phrase to encompass not only information relating to terrorism but also information relating to the national defense and to the foreign affairs of the United States. As discussed above, many of plaintiffs' legitimate and constitutionally protected communications fall within the scope of this definition. Second, the Act allows the government to obtain mass acquisition orders even when its primary purpose is to collect something other than foreign intelligence information – so long as "a significant purpose" of its acquisition is to obtain foreign intelligence information. FAA § 702(g)(2)(A)(v). Thus the government could obtain a mass acquisition order with the chief purpose of (for example) collecting information about domestic groups opposed to the war in Iraq, so long as a significant purpose of its acquisition is to obtain foreign intelligence information and the ostensible targets of its acquisition are reasonably believed to be outside the United States. Third, as discussed further below, *see* section I.D.vi, the "significant purpose" requirement is a *programmatic* requirement – it applies to mass acquisition orders, not to individualized targets. The effect of the FAA is to allow the government to sweep up any – and indeed *every* – international communication.

The FAA thus fails to limit the scope and nature of communications that the government can obtain. This deficiency is made more profound by the fact that the FAA also fails to require the government to *identify* the communications it intends to obtain through any particular acquisition under section 702(a). An application for a Title III warrant must include (in addition

to identifying the person to be surveilled and the facilities to be monitored), "a particular description of the type of communications sought to be intercepted," 18 U.S.C. § 2518(1)(b)(ii); *see also id*. § 2518(4)(c) (stating that Title III order must include "a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates"); *id*. § 2518(3)(b) (requiring court to determine whether "there is probable cause for belief that particular communications concerning that offense will be obtained through [the] interception"). Similarly, an application for a FISA order must include a "description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance." 50 U.S.C. § 1804(a)(5). A FISA application must also include a certification from a senior official "that the certifying official deems the information sought to be foreign intelligence information," *id*. § 1804(a)(6)(A), and that "designates the type of foreign intelligence information being sought," *id*. § 1804(a)(6)(D). The FAA includes no analogous requirements.

The FAA's failure to require the government to identify the nature of the communications to be acquired is a failure of constitutional significance. Thus, the Supreme Court in *Berger* struck down New York's eavesdropping law because, *inter alia*, it failed to require the government to "particularly describe[ ]" the communications, conversations, and discussions sought. *Id*. at 59. Notably, the Supreme Court found the statute constitutionally deficient even though the government was required to identify the people to be surveilled and the facilities to be monitored – safeguards that are absent in the FAA. Courts that have assessed the reasonableness of FISA and Title III have relied at least in part on those statutes' provisions requiring the government to describe the nature of the communications to be acquired. *See, e.g.*,

In re Sealed Case, 310 F.3d at 739; *Tortorello*, 480 F.2d at 773; *Bobo*, 477 F.2d at 982; *United States v. Cafero*, 473 F.2d 489, 498 (3d Cir. 1972).

The FAA's failure to meaningfully limit the scope and nature of communications that can be acquired under the law renders the statute unconstitutional.

iv. The FAA fails adequately to limit the duration of surveillance orders.

As noted above, *see* section I.C.iii, the FAA departs from FISA and Title III in yet another way – by authorizing surveillance programs of up to one year in duration. This, too, is a departure of constitutional significance, as is clear from the Supreme Court's decision in *Berger*. The Supreme Court's decision in that case was motivated in part by the fact that New York's eavesdropping statute permitted surveillance orders of as long as two months. *Berger*, 388 U.S. at 44 n.1. In finding that term too long, the Court observed that the "authorization 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." *Id.* at 59. It also expressed concern that "[d]uring 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 investigations." *Id.*

Unsurprisingly, the courts that have assessed the reasonableness of FISA and Title III have relied at least in part on those statute's provisions limiting the duration of individual intercepts. *See, e.g.*, *In re Sealed Case*, 310 F.3d at 740; *Tortorello*, 480 F.2d at 774. Thus, in rejecting a constitutional challenge to Title III, the Third Circuit wrote:

> [T]he offensive autocracy of the calendar condemned in *Berger* has been supplanted by judicial authority in the first instance, by the right of *sua sponte* judicial review at any time, and by the expiration of statutory authority to continue the interception once the objective has been achieved. Carte blanch is given no one. Executing officers are not free to intercept beyond attainment of their objective for an hour, a day, seven days, or twenty-nine days. They are

> allotted time to achieve an objective, period. Should they intercept beyond this time, they have violated the Act.

Cafero, 473 F.2d at 496.

The FAA allows surveillance programs not of 30 days (as under Title III), nor of 90 or 120 days (as under FISA), but of up to one year. The Act is unreasonable because it fails adequately to limit the duration of surveillance orders.

v. The FAA fails to ensure meaningful and court-supervised minimization.

The FAA also departs from FISA and Title III in failing adequately to ensure that the government minimize the acquisition, retention, and dissemination of information pertaining to U.S. persons. Title III requires the government to conduct surveillance "in such a way as to minimize the interception of innocent and irrelevant conversations," *see* 18 U.S.C. § 2518(5); *see also* 18 U.S.C. § 2518(5) (stating that "every order shall contain a provision" regarding the general minimization requirement), and strictly limits the use and dissemination of material obtained under the statute, *see* 18 U.S.C. § 2517. FISA similarly requires the government to minimize the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons. *See* 50 U.S.C. § 1801(h). It requires that every order authorizing surveillance of a particular target contain specific minimization procedures that will govern that particular surveillance. *See* 50 U.S.C. § 1804(a)(4); 50 U.S.C. § 1805(a)(3); 50 U.S.C. § 1805(c)(2)(A). FISA also specifically provides the FISA court with authority to oversee the government's minimization on an individualized basis *during the course of the actual surveillance*. *See* 50 U.S.C. § 1805(d)(3); *see also* 18 U.S.C. § 2518(6). Thus, under FISA, minimization is required with respect to every individual surveillance target and, equally important, minimization is judicially supervised during the course of the surveillance. *See* David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 9:1, 9-2 (2007)

(explaining that "each FISA application must describe specific minimization procedures that the Attorney General believes are appropriate for the particular surveillance or search in question," that "the FISC may modify the proposed minimization procedures," that the order "must direct that the (modified) procedures be followed . . . in conducting the surveillance," and that the FISC "enjoys the authority to review the government's compliance with minimization procedures").

Courts assessing the reasonableness of FISA and Title III, including the Second Circuit, have found those statutes' minimization procedures to be relevant to their constitutionality. *See, e.g.*, *In re Sealed Case*, 310 F.3d at 740-41 (stating that courts have found FISA's minimization requirements to be "constitutionally significant"); *Pelton*, 835 F.2d at 1075 (finding FISA reasonable in part because it required "the use of 'minimization procedures' for the protection of the targets of surveillance"); *Duggan*, 743 F.2d at 74 (finding FISA reasonable because, among other things, FISA orders require procedures "to minimize the intrusion upon the target's privacy"); *Figueroa*, 757 F.2d at 471 (in assessing constitutionality of Title III, noting that "[i]nnocent parties are protected from unreasonable surveillance by the [minimization requirement]"); *United States v. Turner*, 528 F.2d 143, 156 (9th Cir. 1975) (finding Title III constitutional because, among other things, "measures [must] be adopted to reduce the extent of . . . interception [of irrelevant or innocent communications] to a practical minimum"). All of these courts have suggested or stated expressly that the Fourth Amendment requires meaningful minimization in order to protect the privacy rights of innocent third parties.

Although the FAA requires the government to adopt and the FISC to approve minimization procedures, FAA § 702(e) & 702(i)(2)(C), these procedures are neither individualized nor subject to ongoing judicial supervision. Under the FAA, minimization is not individualized but programmatic; minimization procedures apply not to surveillance of specific

targets but rather to surveillance programs, the specific targets of which may be known only to the executive branch. Moreover, the FISC is granted no authority to supervise the government's compliance with the minimization procedures during the course of an acquisition or even to inquire about the treatment of U.S. person communications. *Cf.* 50 U.S.C. § 1805(d)(3). There is no requirement that incidentally-acquired international communications be destroyed. *Cf.* 50 U.S.C. § 1801(h)(4) (prohibiting retention for more than 72 hours any U.S. communications obtained in the course of warrantless surveillance of facilities used exclusively by foreign power). There is no requirement that the government seek judicial approval before it analyzes, retains, or disseminates U.S. communications. *Cf.* 50 U.S.C. § 1801(h)(4) (requiring court order in order to "disclose[ ], disseminate[ ], use[ ] . . . or retain[ ] for longer than 72 hours" U.S. communications obtained in the course of warrantless surveillance of facilities used exclusively by foreign powers).

The FAA's meager minimization provisions are particularly problematic because the FAA does not provide for individualized judicial review at the acquisition stage. Under FISA and Title III, minimization operates as a second-level protection against the acquisition, retention, and dissemination of information relating to U.S. persons; the first level of protection comes from the requirement of individualized judicial authorization for each specific surveillance target. *Cf. Scott v. United States*, 436 U.S. 128, 130-31 (1978) ("[t]he scheme of the Fourth Amendment becomes meaningful only when it is assured that at some point the conduct of those charged with enforcing the laws can be subjected to the more detached, neutral scrutiny of a judge who must evaluate the reasonableness of a particular search or seizure in light of the particular circumstances" (quoting *Terry v. Ohio*, 392 U.S. 1 (1968))); *United States v. James*, 494 F.2d 1007, 1021 (D.C. Cir. 1971) (observing that "[t]he most striking feature of Title III is

its reliance upon a judicial officer to supervise wiretap operations. Close scrutiny by a federal or state judge during all phases of the intercept, from the authorization through reporting and inventory, enhances the protection of individual rights." (internal quotation marks omitted)); *Cavanagh*, 807 F.2d at 790 (holding that FISA provides for "responsible oversight of the government's activities"). Under the FAA, by contrast, there is no first-level protection, because the statute does not call for individualized judicial authorization of specific surveillance targets (or for that matter, of specific facilities to be monitored or specific communications to be acquired). Unlike FISA and Title III, the FAA permits dragnet surveillance – it permits the mass acquisition of Americans' international telephone calls and e-mails. In this context, minimization requirements should be at least as stringent as they are in the context of FISA surveillance of facilities used exclusively by foreign powers. *See* 50 U.S.C. § 1801(h)(4).

vi. The FAA fails to require that the primary purpose of the government's surveillance be "foreign intelligence."

The FAA is also unreasonable insofar as it permits the government to conduct dragnet surveillance of international communications so long as merely "a significant purpose of the acquisition is to obtain foreign intelligence information." FAA § 702(g)(2)(A)(v). The significant purpose standard allows the government to engage in FAA surveillance even if its primary purpose is to discover evidence of criminal activity.

The Supreme Court has suggested that the procedural safeguards the Fourth Amendment demands for foreign intelligence surveillance may differ in some respects from those required in law enforcement surveillance. *See Keith*, 407 U.S. at 322. Both the Supreme Court and the circuit courts have permitted departures from the Fourth Amendment's ordinary requirements only where the government's primary purpose is to collect foreign intelligence information. *Truong*, 629 F.2d at 915-16; *see also Butenko*, 494 F.2d at 606; *Brown*, 484 F.2d at 427

(Goldberg, J., concurring); *Keith*, 407 U.S. at 318-19 (emphasizing surveillance "directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and [was] not an attempt to gather evidence for specific criminal prosecutions.").

The primary purpose limitation is rooted in the Fourth Amendment. When Congress enacted FISA in 1978, it limited the statute's availability to contexts in which the government's "purpose" was to gather foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B). Courts, sometimes expressly referencing the Fourth Amendment, construed the statutory standard to limit the availability of FISA to contexts in which the government's "primary purpose" was foreign intelligence. *See, e.g.*, *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (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. Megahey*, 553 F. Supp. 1180 (E.D.N.Y. 1982), *aff'd Duggan*, 743 F.2d at 59; *see also Pelton*, 835 F.2d at 1067 (interpreting "purpose" to mean "primary purpose"). In 2001, Congress amended FISA to allow the government to rely on the statute so long as a "significant purpose" of its surveillance is to gather foreign intelligence information. USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). While some courts have upheld FISA despite this amendment, *see, e.g.*, *In re Sealed Case*, 310 F.3d at 742-44; *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 306-09 (D. Conn. 2008), at least one court has found that the amendment renders FISA unconstitutional, *Mayfield v. United States*, 504 F. Supp. 2d 1037 (D. Or. 2007).

Whether or not the "significant purpose" standard is constitutional in the context of FISA, a framework that requires prior judicial authorization for each specific surveillance target, the "significant purpose" standard is unreasonable in the context of FAA surveillance. The effect of

the FAA's "significant purpose" language is to permit the government to evade ordinary Fourth Amendment requirements even where its principal purpose is to gather evidence of criminal activity. *See Mayfield*, 504 F. Supp. 2d at 1036-37. The FAA's purpose requirement – unlike FISA's purpose requirement – applies not to individualized and particularized surveillance orders but to entire programs of surveillance. Under the FAA, the government must certify that a significant purpose of a mass acquisition is to gather foreign intelligence information, but once the FISC has endorsed an acquisition, nothing in the statute forecloses the government from targeting particular individuals primarily or entirely for the purpose of collecting evidence of criminal activity. Nor is the FISC even in a position, under the FAA, to review on an individualized basis what the government's purpose in targeting particular individuals or groups may be.

vii. The FAA fails sufficiently to protect domestic communications.

In addition to giving the executive branch unfettered access to Americans' international communications, the Act permits it to obtain certain domestic communications. The Act's provision limiting the acquisition of purely domestic communications restricts the executive branch from "intentionally acquir[ing] any communication as to which the sender and all intended recipients are *known at the time of the acquisition* to be located in the United States." FAA § 702(b)(4) (emphasis added). While this provision may protect some domestic communications, its more significant effect is to require that any uncertainty about location be resolved in favor of the government. Under the FAA, the government can collect *any* communication so long as it does not know for a fact that all parties to the communication are located inside the United States.

The FAA is likely to have dramatic implications for the privacy of Americans' purely domestic communications. The administration itself has indicated that uncertainty about location is the rule rather than the exception. *See, e.g.*, *Hearing Before the H. Judiciary Comm. on the Foreign Intelligence Surveillance Act and Protect America Act*, 110th Cong. 110-79 (2007) (statement of DNI McConnell) ("Sir, in the old days, Cold War days, location was much, much easier. Today, with mobile communications, it is more difficult. So a target can move around. There are some keys that can assist, but we can't know for certain[]."). As a result, the FAA is likely to result in the government's acquisition of purely domestic communications.

The FAA's failure to sufficiently protect domestic communications renders the Act unreasonable.

II. THE FAA VIOLATES THE FIRST AMENDMENT.

The Supreme Court has recognized that government surveillance can have a profound chilling effect on First Amendment rights. In *Keith*, the Court addressed this point at length, writing:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. 'Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power,' . . . 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 the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent . . . .
>
> 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.

Keith, 407 U.S. at 313-14 (internal citations omitted).

As discussed above, *Keith* involved the question whether the government could constitutionally conduct warrantless surveillance to protect against domestic security threats, but in many other contexts the Supreme Court has recognized that the government's surveillance and investigatory activities can infringe on rights protected by the First Amendment. Thus in *NAACP v. Alabama*, a case in which the Supreme Court invalidated an Alabama order that would have required the *NAACP* to disclose its membership lists, the Supreme Court wrote:

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations . . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs . . . .

357 U.S. 449, 462 (1958). *Accord Watkins v. United States*, 354 U.S. 178, 197 (1957) (noting, in invalidating conviction for refusal to divulge sensitive associational information, that "forced revelations [that] concern matters that are unorthodox, unpopular, or even hateful to the general public, the reaction in the life of the witness may be disastrous"); *see also McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (stating that the First Amendment protects speaker against compelled disclosure of identity); *Tally v. California*, 362 U.S. 60 (1960) (same).

Because government surveillance and investigative activities can have such an invidious effect on rights protected by the First Amendment, the Supreme Court has said that Fourth Amendment safeguards must be strictly enforced where the information sought to be collected implicates the First Amendment. *See, e.g.*, *Zurcher*, 436 U.S. at 564 (holding that mandates of

the Fourth Amendment must be applied with "scrupulous exactitude" in this context); *id.* ("[w]here presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field"). The Court has made clear, however, that the First Amendment also supplies its own protection against laws that burden speech. Thus, in *McIntyre*, a case that involved a statute requiring disclosure of the identity of persons distributing election literature, the Supreme Court wrote: "When a law burdens core political speech, we apply exacting scrutiny and we uphold the restriction only if it is narrowly tailored to serve an overriding interest." *McIntyre*, 514 U.S. at 347 (internal quotations and citation omitted); *see also In Re Primus*, 436 U.S. 412, 432 (1978) (stating that government-imposed burdens upon constitutionally protected communications must withstand "exacting scrutiny" and can be sustained, consistent with the First Amendment, only if the burdens are "closely drawn to avoid unnecessary abridgement of associational freedoms"). Indeed, the Supreme Court has said that even where a challenged statute burdens speech only incidentally, the statute can withstand scrutiny under the First Amendment only "if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *United States v. O'Brien*, 391 U.S. 367, 377 (1968).[12]

The FAA imposes a substantial burden on rights protected by the First Amendment. As plaintiffs explain in their declarations, the law compromises plaintiffs' ability to gather

[12] Notably, the Second Circuit has applied the First Amendment's "strict scrutiny" test even in cases involving physical searches at the international border, a unique context in which the government's power is at its zenith. *See Tabbaa v. Chertoff*, 509 F.3d 89, 102 (2d Cir. 2007) (finding that government's detention of plaintiff U.S. citizens returning from religious conference in Canada had substantially burdened plaintiffs' First Amendment rights and holding that government's actions could be sustained only if justified by "compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms" (internal quotation marks omitted)).

information, engage in advocacy, and communicate with colleagues, clients, journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States. In the debate that preceded the enactment of the FAA, some members of Congress anticipated exactly the kinds of harms that plaintiffs have described. For example, Senator Cardin of Maryland stated:

> Also formidable, although incalculable, is the chilling effect which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy within lawful limits, without having to sacrifice the expectation of privacy they rightfully hold. Warrantless electronic surveillance can violate that understanding and impair the public confidence so necessary to an uninhibited political life.

Cong. Rec. S574 (February 4, 2008) (statement of Sen. Cardin during debate on FAA).

Because the Act imposes a substantial burden on First Amendment rights and lacks the particularity that the Fourth Amendment requires, it necessarily sweeps within its ambit constitutionally protected speech that the government has no legitimate interest in acquiring. As discussed above, the Act permits the government to conduct intrusive surveillance of people who are neither foreign agents nor criminals and to collect vast databases of information that has nothing to do with foreign intelligence or terrorism. Indeed, the Act sweeps so broadly that literally no international communication is beyond its reach.

More precision is required when First Amendment rights are at stake. *Se. Promotions Ltd. v. Conrad*, 420 U.S. 546, 561 (1975); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963) ("the freedoms of expression must be ringed about with adequate bulwarks"); *Speiser v. Randall*, 357 U.S. 513, 520-21 (1958) ("the more important the rights at stake the more

important must be the procedural safeguards surrounding those rights"); *see also Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 168 (2002) (striking down local ordinance that burdened First Amendment activity through requirement of a permit for door-to-door canvassing on the grounds that the ordinance "[was] not tailored to the Village's stated interests"); *McIntyre*, 514 U.S. at 351-53 (striking down compelled disclosure statute on grounds that statute reached speech that was beyond state's legitimate interests); *NAACP*, 357 U.S. at 463-66 (striking down order to disclose membership lists on grounds that order was not supported by state's purported justification). Notably, the phrase "scrupulous exactitude," as used in *Zurcher*, was drawn from an earlier Supreme Court decision, *Stanford v. Texas*, 380 U.S. 926 (1965), a decision that particularly criticized the use of "general warrants" directed *at expressive activity*. As discussed above, *see* section I.A, this is precisely what the FAA allows.

III. **THE FAA VIOLATES ARTICLE III**.

The FAA's scheme of judicial review violates Article III and the principle of separation of powers because the FISC issues orders in the absence of any case or controversy, reviewing only the legality and constitutionality of the government's programmatic procedures in the abstract and leaving all questions about individual monitoring to the executive branch.

The judicial power is limited to resolving cases or controversies. As the Supreme Court recently explained, the Article III case or controversy requirement "confine[s] the business of federal courts to questions presented in an adversary context and in a form historically viewed as capable of resolution through the judicial process." *EPA v. Massachusetts*, 127 S.Ct. 1438, 1452 (2007) (internal quotation marks omitted). A "case arises, within the meaning of the Constitution, when any question respecting the Constitution, treatise or laws of the United States has assumed such a form that the judicial power is capable of acting on it . . . . [T]here must be

an actual controversy over an issue, not a desire for an abstract declaration of the law." *In re Summers*, 325 U.S. 561, 566-67 (1945) (internal quotation marks omitted). The judiciary "is entitled to decide constitutional issues only when the facts of a particular case require their resolution for a just adjudication on the merits." *Colon v. Howard*, 215 F.3d 227, 235 (2d Cir. 2000) (Walker, J., concurring) (internal quotation marks omitted); *see also United Pub. Workers of Am. v. Mitchell*, 330 U.S. 75, 89 (1947) ("as is well known the federal courts established pursuant to Article III of the Constitution do not render advisory opinions. For adjudication of constitutional issues concrete legal issues, presented in actual cases, not abstractions are requisite" (internal quotation marks omitted)).

Under the FAA, the FISC is not presented with a case or controversy fit for judicial resolution. As explained above, the FAA authorizes surveillance that will result in the mass acquisition of U.S. residents' communications without any individualized review or approval by the FISC with respect to who, what, where, or why the government is conducting its monitoring activity. Instead, the FISC issues mass acquisition orders after reviewing only the general procedures that will govern the government's surveillance program; the question of who to monitor, for how long, and for what purpose is left entirely to executive branch officers, and the only oversight of the government's *implementation* of its FAA authority is conducted by the executive branch itself. The FISC's review of the government's programmatic procedures that will govern vacuum cleaner-like surveillance – both for compliance with the statute and the Constitution – is completely divorced from any individualized interception. The FISC's review of the procedures is nothing more than an abstract assessment of the general rules that will govern a surveillance program implemented entirely by the executive branch.

In this respect, mass acquisition orders issued by the FISC are quite different than traditional search warrants or FISA orders authorizing surveillance of particular targets after a judicial determination of probable cause and a judicial assessment of the limits imposed on the particular monitoring activity. *See supra* at I.C.iii. Whereas the question whether a court should issue a traditional search warrant may be a proper case or controversy, what the FISC does under the FAA bears no resemblance to that Article III function. Cases in which courts have rejected Article III case or controversy challenges with respect to *traditional* FISA warrants are instructive. As Judge Sifton wrote in *Megahey*: "Applications for electronic surveillance submitted to FISC pursuant to FISA involve concrete questions respecting the application of the Act and are in a form such that a judge is capable of acting on them, much as he might otherwise act on an *ex parte* application for a warrant." 553 F. Supp. at 1197 (emphasis added), *aff'd Duggan*, 743 F.2d 59 (2d Cir. 1984); *see also Kevork*, 634 F. Supp. at 1014.

The court's analysis in *Megahey* comports with the views of the Office of the Legal Counsel ("OLC") at the time of FISA's enactment. Prior to FISA's enactment, Congress had sought the OLC's view on whether the FISC's role in issuing traditional FISA warrants would violate the Article III case or controversy requirement. The OLC concluded that Article III was satisfied but stated it was a "difficult question." Key to the OLC's analysis was the fact that the court would be able to exercise legal judgment with respect to applying facts and law to a particular case:

> While the judge's role in assessing the application . . . is limited, we still believe he is able to exercise judgment on matters requiring a legal conclusion. The judge is required under the bill to apply standards of law to the facts of a particular case. For example, he must make certain determinations of probable cause; while his review may be somewhat restricted, his determination will be of the same sort made in other warrant proceedings. In addition, the judge is required to ensure that certain procedural requirements have been satisfied. While this review may be rather routine, it has been considered sufficient in other contexts so long as the

judge may exercise independent judgment.

Memorandum from John M. Harmon, Assistant Att'y Gen., Office of Legal Counsel, to Hon. Edward P. Boland, Chairman, House Permanent Select Comm. on Intelligence (Apr. 18, 1978), in Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence, 95th Cong. 26, 31 (1978) at 28.

As the *Megahey* court and the OLC recognized, a traditional FISC order presents the court with a concrete question about a particular proposed interception. By contrast, a mass acquisition order under the FAA demands a general assessment of whether the government's programmatic minimization and targeting procedures are reasonable – a question asked and answered at the broadest level of generality without reference to particular persons or facilities – is simply not a case or controversy fit for judicial resolution under Article III. The FISC issues an advisory opinion that serves as a fig leaf for executive surveillance that may sweep up the communications of millions of U.S. citizens and residents.

The constitutional flaws of this judicial review scheme are compounded even further by the fact that should the FISC *deny* any application for a mass acquisition order because it finds the government's procedures illegal or unconstitutional, the order is not even binding; it can be disregarded entirely during the pendency of any appeal. Under the statute, the government can initiate an acquisition prior to receiving any judicial authorization (or while its request for authorization is pending). *See* FAA § 702(c)(1)(B) (acquisition can begin only upon submission of a certification to the FISC); FAA § 702(c)(2) (acquisition can begin upon an administrative determination of exigent circumstances). The FISC must issue a ruling on the government's request for a mass acquisition order within 30 days. FAA § 702(i)(B). Should the FISC deny an

order, the government "may continue" any "acquisition affected by" such an order during the pendency of any appeal. FAA § 702(i)(4)(B). This encompasses the period of time between when the FISC denies an acquisition order and when the government's time for appeal lapses, FAA § 702(i)(4)(A), as well as the 60 days the FISA Court of Review has to issue a ruling on the appeal, FAA § 702(i)(4)(C).

A basic principle rooted in both Article III and separation of powers, however, is that judicial decisions are binding on the parties unless they are stayed, modified, or reversed within the judicial process itself. Under our system of divided government, judicial orders cannot be revised by the legislature or ignored by the executive. *See Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 219 (1995) (invalidating scheme allowing for legislative revision of judgments and holding that the judicial power is "to render dispositive judgments," rulings that "decide" cases, "subject to review only by superior courts in the Article III hierarchy"); *Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 113-14 (1948) ("Judgments . . . may not lawfully be revised, overturned or refused faith and credit by another Department of Government"); *Hayburn's Case*, 2 U.S. 408, 410 (1792) (holding "[n]o decision of any court can . . . be liable to a revision, or even suspension, by the legislature itself"). Unenforceable rulings that may be disregarded at will by another branch of government are not judicial decisions at all but rather impermissible advisory opinions. *See Flast v. Cohen*, 392 U.S. 83, 96 (1968) (the "rule against advisory opinions in federal courts" is well-settled); 13 Charles Alan Wright, Arthur R. Miller, and Edward H. Cooper, Fed. Practice & Procedure § 3529.1 (2008) ("The oldest and most consistent thread in the federal law of justiciability is that the federal courts will not give advisory opinions."); 1 Lawrence H. Tribe, American Constitutional Law § 3-9 (3d ed. 2000) (explaining that "article III courts will not give opinions in the nature of advice concerning

legislative or executive action"). FAA orders disapproving acquisitions are denied the dispositive character that is the essential element of the "judicial power." By providing for "judicial review" of general procedures drawn up by the executive branch but excusing the executive from any duty of prompt compliance, the Act violates Article III.[13]

CONCLUSION

For the reasons discussed above, plaintiffs respectfully request that the Court enter summary judgment in their favor.

Respectfully submitted,

JAMEEL JAFFER
MELISSA GOODMAN
L. DANIELLE TULLY
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2583
jjaffer@aclu.org

NEW YORK CIVIL LIBERTIES UNION FOUNDATION, by
CHRISTOPHER DUNN
ARTHUR EISENBERG
New York Civil Liberties Union
125 Broad Street, 19th Floor
New York, NY 10004
(212) 607-3300

CHARLES S. SIMS
THEODORE K. CHENG
MATTHEW J. MORRIS
Proskauer Rose LLP

[13] In addition, by denying the judiciary the power to demand compliance with its orders, the FAA in effect imposes a rule of decision on the courts (mandating a de facto stay) in violation of *United States v. Klein*, 80 U.S. 128 (1871).

1585 Broadway
New York, NY 10036
212-969-3000

September 12, 2008