UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMNESTY INERNATIONAL 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. ARSCHACK; 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 United States, Defendants.	**MEMORANDUM AMICI CURIAE OF THE RUTHERFORD INSTITUTE AND THE BRENNAN CENTER FOR JUSTICE** **IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT & IN OPPOSITION TO DEFENDANTS' CROSS-MOTION FOR SUMMARY JUDGMENT** **Case No. 08-cv-06259 (JGK)** **ECF Case**

LAURA ABEL
Emily Berman
Aziz Huq
THE BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
161 Avenue of the Americas, 12th Floor
New York, NY 10013
(212) 998-6730

December 19, 2008

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other

INTERESTS OF THE AMICI

Amicus the Rutherford Institute is an international civil liberties and human rights organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute specializes in providing legal representation without charge to individuals whose civil liberties are threatened or violated. The Institute also strives to educate the public about constitutional and human rights issues. During its 26-year history, attorneys affiliated with the Institute have represented numerous parties before the U.S. Supreme Court. The Institute has also filed briefs as an amicus of the Court in cases dealing with critical constitutional issues.

The Rutherford Institute believes strongly in an unwavering commitment to our basic and fundamental constitutional framework as the best guarantor of our nation's liberty and security. The Institute is dedicated to both transparency and openness in government, because without accountability in our government officials, our fundamental constitutional and civil liberties are put at jeopardy.

Amicus the Brennan Center for Justice at New York University School of Law ("Brennan Center") is a non-partisan public policy and law institute that focuses on fundamental issues of democracy and justice. Our work ranges from voting rights to redistricting reform, from access to the courts to presidential power in the fight against terrorism. We are concerned with the dangers that national security policy, including the use of new information technologies, poses to privacy and other constitutional liberties. The Brennan Center focuses on preserving the Separation of Powers, which the Framers intended as a bulwark against violations of Americans' freedoms.

Amici submit this brief in support of plaintiffs' opposition to the government's motion to dismiss to aid this Court's consideration of the novel and complex constitutional questions raised by Foreign Intelligence Surveillance Act ("FISA") Amendments Act of 2008, Pub. L. No. 110-261 (2008) ("FAA").

Based on our expertise and scholarship about national security policy and its implications for Americans' constitutional privacy rights, we respectfully urge this Court to deny the government's motion to dismiss and to grant the plaintiffs' motion for summary judgment. The FAA fails to provide adequate protections for U.S. persons' Fourth Amendment rights. Consequently, we urge the court to invalidate the Act.

PRELIMINARY STATEMENT

The FAA dramatically expands governmental authority to seize communications of U.S. persons located inside the United States without a prior judicial warrant. The Government does not dispute that the "broad and unsuspected governmental incursions into conversational privacy" of U.S. persons that the FAA allows "necessitate[s] the application of Fourth Amendment safeguards." *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313 (1972). Rather, the Government contends, *inter alia*, the privacy of U.S. persons are "reasonably protect[ed] … through [the FAA's] requirement of minimization procedures, which, as with targeting procedures, must be approved by the [Foreign Intelligence Surveillance Court]." Def.'s Mem. in Opp'n to Pls.' Mot. for Summ. J. & in Supp. of Def.'s Cross-Mot. for Summ. J. ("Def.'s Br.") at 60; *id.* at 31, 60.

Amici public interest organizations respectfully submit this brief to show how the government errs by relying on the slim reed of minimization procedures as a basis for rejecting plaintiffs' Fourth Amendment claims.[1] The minimization procedures of the FAA on their face fall short of preventing the violation of U.S. citizens' Fourth Amendment rights. And recent history suggests that even when minimization procedures are purportedly in place, external oversight is still necessary to ensure "the security of one's privacy against arbitrary intrusion by the [executive]—which is at the core of the Fourth Amendment [and] is basic to a free society"—is protected. *Berger v. New York*,

[1] Amici curiae agree with Plaintiffs that they have standing to challenge the FAA. Pls.' Reply in Supp. of Pls.' Mot. for Summ. J. & Opp. to Defs.' Cross-Mot. for Summ. J. at 2-15. Plaintiffs also persuasively demonstrate that the surveillance contemplated under the FAA violates the Fourth Amendment's reasonableness requirement by failing to require an *ex ante* judicial determination of individualized suspicion, either through obtaining a traditional warrant on probable cause issued by a neutral magistrate or through some other form of meaningful, pre-surveillance judicial review. Pls.' Mem. in Supp. of Mot. for Summ. J. at 19-31, 33-34.

388 U.S. 41, 53 (1967) (quoting *Wolf v. Colorado*, 338 U.S. 25, 27 (1949)); *see infra* at 19-20. Minimization procedures, in short, cannot cure the constitutional defects at the FAA's heart.

A. Minimization Procedures as Protections for Fourth Amendment Rights

Title 50 defines as "minimization procedures" as:

> specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1).[2] First adopted in the original FISA legislation in 1978, this definition remains unchanged today.

Under this definition, minimization can occur at one of three moments in the course of surveillance. First, there is the *acquisition* stage. At this threshold moment, minimization can be accomplished via protocols about when surveillance should end: "'[W]here a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party' to the communication." *In re Sealed Case*, 310 F.3d 717, 731 (FISA Ct. Rev. 2002) (quoting H. Rep. No. 95-1283, at 55-56 (1978)).

A second option for minimization arises at the *retention* stage, when measures can be taken to destroy information that is acquired but proves unnecessary for "obtaining,

[2] The definition of minimization in the foreign intelligence surveillance context differs from that in the context of domestic criminal surveillance. The Omnibus Crime Control Act ("Title III") provides that every surveillance order must include a provision requiring the surveillance to "be conducted in such a way as to minimize the interception of communication not otherwise subject to interception under this chapter." 18 U.S.C. § 2518(5). Title III has no provision analogous to the retention and dissemination restrictions contained in 50 U.S.C. § 1801(h) because narrowing targeting at the acquisition stage reduces the need for such minimization. By contrast, the FAA limits the acquisition constraints that bind even FISA surveillance.

producing, or disseminating foreign intelligence information." *Id.* (citation omitted) Finally, minimization can be done by restricting *dissemination*. *Id.* The statutory definition of minimization procedures hence includes additional provisions applicable specifically to the retention and dissemination stages:

> procedures that require that nonpublicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; . . . [and] notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

50 U.S.C. § 1801(h)(2), (3). Again, this provision remains unchanged in the law despite the passage of the FAA.

Finally, parallel provisions define and mandate the minimization of material acquired, retained, and disseminated as a result of physical searches. *See* 50 U.S.C. §§ 1821-1829.

B. Minimization Under Traditional FISA[3]

The pivotal feature of the traditional FISA's minimization efforts is the close nexus between any given discrete decision to intercept communications and the tightly tailored and individualized procedures mandated to address the privacy interests of U.S. persons.[4]

[3] Traditional FISA surveillance continues even after the enactment of the FAA. The FISA provisions that existed prior to the FAA's enactment continue to govern foreign intelligence surveillance not aimed at targets "reasonably believed to be located outside the United States." 50 U.S.C. § 1881a. The FAA thus supplemented and expanded, rather than replaced, the government's foreign intelligence surveillance authority under FISA.

[4] Amici take no position in this brief with respect to the constitutionality of FISA's surveillance regime. It merely notes that, under traditional FISA, minimization procedures are much more protective of U.S. persons' privacy rights than they are under the FAA.

FISA's definition of minimization procedures contemplates "specific procedures" crafted for each "particular surveillance." 50 U.S.C. § 1801(h)(1); David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 9.3 (2007). Under FISA, the Attorney General adopted standard minimization procedures that could be applied in most cases and then tailored to the particular circumstances of specific surveillances. Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Jobs*, 12 Rutgers L.J. 405, 415-16 (1981); Kris & Wilson, *supra*, at § 9:3. And with respect to the National Security Agency ("NSA"), the template for FISA minimization is contained in United States Signals Intelligence Directive 18 ("USSID 18") at Annex A, Appendix 1 (1993).[5]

Despite the statute's command to minimize acquisition, retention, *and* dissemination, in many FISA cases minimization is implemented largely at the retention and dissemination stages alone. Under the traditional FISA scheme, surveillance is often targeted at one communication device. With any given device, however, it is not always immediately apparent whether all the intercepted information contains foreign intelligence information. Communications might be in a foreign language, code, or might be significant only on later reexamination. *See United States v. Rahman*, 861 F. Supp. 247, 252-53 (S.D.N.Y. 1994). Hence, "in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and

[5] USSID 18 sets out "policies and procedures" meant to ensure that U.S. signals intelligence is conducted "in a manner that safeguards the constitutional rights of U.S. persons." USSID 18 Letter of Promulgation. A declassified version of USSID 18 from 1993 is available online at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm. While a more recent nonpublic version might exist, the government argues that minimization procedures have remained the same and are also constitutionally sufficient to protect the privacy rights of U.S. persons. So the public version of USSID 18 remains relevant to this case.

logging the pertinent communications." *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002); Kris & Wilson, *supra*, at § 9:4.

When the government cannot "avoid acquiring all information . . . reasonable design of the procedures must emphasize the minimization of retention and dissemination." Kris & Wilson, *supra*, at § 9:5 n.1 (citation omitted). But according to the Foreign Intelligence Surveillance Court ("FISC"), standard minimization procedures provide that all acquired information is retained unless it "could not be" foreign intelligence. *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002) (*In re All Matters*), abrogated on other grounds by *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). Under the FISA minimization procedures, therefore, "a substantial amount of information is in fact retained." Kris & Wilson, *supra*, at § 9:5.

Under the FISA minimization rules, non-pertinent information should "be destroyed where feasible." Kris & Wilson, *supra*, at § 9:5 (citations omitted). Alternatively, government officials can decline to "log" particular communications—i.e., to list the time, date, parties, or contacts of the communication. Information not logged is not be indexed in the relevant database, making it "non-retrievable." Kris & Wilson, *supra*, at § 9:5. In sum, "[u]nder FISA . . . every communication is usually recorded but only pertinent communications are retained via logging and indexing." *Id.*

Under traditional FISA, minimization procedures also limit dissemination of nonpublic information that is neither foreign intelligence information nor evidence of a crime to "officials, agencies, or components with responsibilities directly related to the information." Kris & Wilson, *supra*, at § 9:6 (citation omitted). In addition, information

that is not foreign intelligence may not be disseminated at all if it "identifies any United States person" except when that identity is "necessary to understand foreign intelligence information or assess its importance." 50 U.S.C. § 1801(h)(2). Information that is evidence of a crime may be retained and disseminated. § 1801(h)(3).

The traditional FISA framework also requires ongoing judicial scrutiny of the application of minimization procedures. Under FISA, it remains the task of the FISC to ensure that the particular minimization procedures that were crafted and detailed in an application for a FISA surveillance order satisfy "the definition of minimization procedures under section 1801(h)." If the FISC judge issuing the order is not satisfied, she can modify the government's proposed minimization procedures. § 1804(a)(4), (5). Congress intended that "'[i]f [the court] is not convinced that [the minimization procedures] will be effective, the application should be denied or the procedures modified.'" Schwartz, *supra*, at 439 (quoting S. Rep. No. 95-701, at 53 (1978)). In addition the court's order must "direct that the minimization procedures be followed." 50 U.S.C. § 1805(c)(2)(A). Once a surveillance order is issued, the FISC is also authorized on a continuing basis to "assess compliance with the minimization procedures." § 1805(d)(3).

When FISA permits surveillance without prior judicial approval—which it does only in very narrowly constrained circumstances—minimization requirements are more stringent. Electronic surveillance can be conducted absent a court order when it is targeted at communications between or among foreign powers and "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party." 50 U.S.C. § 1802(a)(1). If

the communications of U.S. persons are acquired by such surveillance, however, minimization procedures demand that "no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours." § 1801(h)(4). Traditional FISA thus recognizes that especially protective minimization procedures are needed when warrantless surveillance might target even an incidental quantity of U.S. persons' communications.

In short, while traditional FISA acquires and retains a substantial amount of U.S. persons' communications, it works in tandem with minimization procedures to protect U.S. persons' privacy in several ways. First, it dictates that the lion's share of surveillance occurs only *after* a judge has identified cause for the surveillance and has examined the metes and bounds of proposed surveillance to ensure adequate tailoring. *See* Kris & Wilson, *supra*, at §§ 9.1 – 9.2; *see also* 50 U.S.C. § 1804(a)(3)(B) (allowing FISA surveillance only when, *inter alia*, there is probable cause to believe that its target is "a foreign power or an agent of a foreign power"). FISA surveillance that does not require prior court approval is both extremely limited in scope and also subject to heightened minimization procedures. Second, the FISA statute compels a close nexus between the particular surveillance at issue and selected minimization procedures. Finally, it enables ongoing judicial monitoring to ensure that chosen minimization procedures in fact function as intended.

C. Minimization Under the FAA

Unlike traditional FISA, the FAA does not require the government to provide *ex ante* particularized reasons or to specify a single targeted person for conducting surveillance. Instead, it need only certify that any acquisition is "limited to targeting

persons reasonably believed to be located outside the United States." 50 U.S.C. § 1881a(d)(1)(A). The FAA thereby abandons the particularization of searches that both domestic criminal surveillance law and FISA have long demanded, and instead invites *open-ended* surveillance authorizations untethered from any single communication, person, or facility.

Despite the gulf between the surveillance regimes authorized by FISA and the FAA, Congress left changed the statutory definition of minimization procedures applicable to FAA surveillance. § 1881a(e). That is, a statutory command of minimization crafted for a universe of discrete and particularized surveillance authorizations has been extended to a new universe of general warrants.

The FAA also differs radically from FISA's in its judicial supervision arrangements. Like FISA, the FAA requires the FISC to pre-approve minimization procedures. § 1881a(g)(2)(A)(ii). The FISC is tasked with reviewing procedures on their face to ensure that they are consistent with the statutory definition, § 1881a(i)(2)(c), and the Fourth Amendment, § 1881a(i)(3)(A). But the FAA diverges dramatically from the traditional FISA regime by eliminating any judicial scrutiny of whether procedures crafted in the abstract satisfy constitutional demands. The FISC thus considers whether minimization procedures *theoretically* satisfy the statute and the Fourth Amendment, but not whether their implementation *in fact* meets either of these thresholds. *Cf.* 50 U.S.C. § 1805(d)(3) ("[T]he judge may assess compliance with the minimization procedures by reviewing the circumstance under which information concerning United States persons was acquired, retained, or disseminated."); 18 U.S.C. § 2518(6) ("[T]he order may require reports to be made to the judge who issued the order. . . . Such reports shall be

made at such intervals as the judge may require."). Moreover, if the FISC finds the government's proposed minimization procedures deficient, the government may nonetheless carry on surveillance while it appeals that decision. 50 U.S.C. § 1881a(i)(4)(B).

Instead of ongoing judicial supervision of minimization procedures, the FAA falls back on *post hoc* executive review: periodic assessments of compliance by the Attorney General and Director of National Intelligence submitted to the FISC and to congressional oversight committees; and the possibility that the Inspector General of the Department of Justice might review compliance with minimization procedures. § 1881a(l).

It is against this backdrop of ill-fitting, and poorly enforced minimization rules that this case arises, and against which the government seeks to persuade this court that the FAA's minimization requirement—itself *de minimus*—is adequate to secure its constitutionality. It is not.

ARGUMENT

The minimization procedures contemplated by the FAA do not satisfy the Fourth Amendment reasonableness requirement for two reasons. *First*, *post hoc* minimization of U.S. persons' communications can never serve as an adequate substitute for *ex ante* judicial determinations of individualized suspicion. However useful they may be at the margin, minimization procedures are but "[o]ne of the protections thought essential by Congress as a bulwark against unconstitutional governmental intrusion on private conversations." *Scott v. United States*, 436 U.S. 128, 143 (1978) (Brennan, J., dissenting). Alone they provide insufficient protection against unwarranted government intrusion to render surveillance under the FAA "reasonable."

Second, the specific minimization procedures contained in the FAA are on their face inadequate to protect U.S persons' privacy rights. Even if the government is correct that the absence of an *ex ante* finding of individualized suspicion does not render the surveillance constitutionally deficient—a position the main brief effectively refutes—the *ex post* judicial scrutiny envisioned by the FAA cannot render the surveillance permitted by the FAA "reasonable" under the Fourth Amendment.

I. Surveillance Employing the FAA's Minimization Procedures But No *Ex Ante* Judicial Finding of Particularized Suspicion is Per Se Unreasonable

Surveillance under the FAA lacks either a prior judicial warrant requirement or *post hoc* judicial supervision. The government therefore relies almost entirely on the statute's minimization procedures to insulate the statute from constitutional attack. But while minimization procedures are *relevant* to whether particular government surveillance is "reasonable" under the Fourth Amendment, they cannot alone satisfy the Fourth Amendment's reasonableness requirement.

At the threshold, the government insists that the FAA will infringe on Fourth Amendment rights only "incidentally." Def.'s Br. at 34-39. But this is implausible. There is no doubt the FAA will permit the collection of significant numbers of U.S. persons' communications. Strictly foreign-to-foreign communications do not require authorization at all. If the government seeks to collect communications from one non-U.S. person abroad to another, it needs no approval. Authorization under the FAA is necessary only when the Attorney General and the Director of National Intelligence conclude that at least *one* target is "reasonably believed to be located outside the United States" and "prevent[ed when]. . . *all* intended recipients are known . . . to be located in the United States." 50 U.S.C. § 1881a(g), (d)(1) (emphasis added). The FAA hence is

unnecessary if *all* parties to a call are outside the United States, and by law required when one party is in the U.S. *See* Def.'s Br. at 53 n.39. The government's reliance on the apparent extra-territorial focus is thus misplaced. *Id.* at 34-39. A majority of surveillance enabled by the statute inevitably—and by design— will sweep in U.S. persons' communications.

As the government concedes, *id.* at 48—and assuming *arguendo* that FAA surveillance does not require a warrant—foreign intelligence surveillance of U.S. persons' communications, even when otherwise targeted abroad, must be "reasonable" to survive constitutional scrutiny. *In re Terrorist Bombings of U.S. Embassies in E. Afr. (Fourth Amendment Challenges)*, Nos. 01-1535; 01-1550; 01-1553; 01-1571; 05-6149; 05-6704, 2008 WL 4967686, at *1, *12-13 (2d Cir. Nov. 24, 2008) (*In re Terrorist Bombings*)[6] (analyzing the constitutionality of foreign intelligence surveillance abroad under a "reasonableness" standard); *In re Sealed Case*, 310 F.3d at 742-46 (asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment); *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980) (even if there is no warrant required, reasonableness analysis limits the government's foreign intelligence surveillance power of communications intercepted within the U.S.). "To determine whether a search is reasonable under the Fourth Amendment, [a court] examine[s] the 'totality of the circumstances' to balance 'on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *In re Terrorist Bombings*, 2008 WL 4967686, at *13 (citations omitted).

[6] *In re Terrorist Bombings* considered the constitutionality of FISA surveillance of the telephone lines of a U.S. citizen located in Kenya. *In re Terrorist Bombings*, 2008 WL 4967686, at *2. Here, the affected U.S. persons are located in the United States—making their constitutional cases stronger.

Minimization is *one factor* in assessing reasonableness. *Scott*, 436 U.S. at 139-42 (majority op.) (evaluating minimization procedures as part of the analysis whether surveillance was "reasonable" under the Fourth Amendment); *see also In re Sealed Case*, 310 F.3d at 740-42 (holding that FISA's constitutionality rests in part on its requirement that the government use minimization procedures, and submit to continuing FISA court oversight of minimization procedures). But no court has ever held that minimization procedures *alone* can be constitutionally sufficient to sustain a surveillance statute's constitutionality. In asking this court to do so, the government asks it to break untrodden constitutional ground.

Precedent makes abundantly clear that minimization procedures alone cannot adequately meet the reasonableness threshold. Evaluating FISA's constitutionality, federal courts have always considered *all* the checks imposed by FISA to shelter privacy, and often refer with approval to the overall "secure framework" these protections *combine* to create. *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984); *United States v. Cavanaugh*, 807 F.2d 787, 789 (9th Cir. 1987). The Second Circuit thus held that "*court orders and other procedural safeguards* laid out in [FISA] 'are necessary to insure that electronic surveillance by the U.S. Government . . . conforms to the fundamental principles of the fourth amendment.'" *Duggan*, 743 F.2d at 73 (emphasis added) (quoting S. Rep. No. 95-701, at 13 (1978)); *see id.* at 73-74 (finding FISA constitutional based on procedures requiring a judicial finding of probable cause regarding both the target and its location, and minimization procedures); *cf. United States v. Tortorello*, 480 F.2d 764, 773-75 (2d Cir. 1973) (holding Title III surveillance constitutional based on multiple protective procedures whose absence led the Supreme

Court to invalidate surveillance in other cases). Similarly, the Court of Appeals for the Fourth Circuit has cautioned that "FISA's *numerous* safeguards [including minimization,] provide sufficient protection for the rights guaranteed by the Fourth Amendment." *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (emphasis added).

The FISC also has emphasized that minimization forms but one small part of a necessary range of protective procedures that together render foreign intelligence surveillance "reasonable" under the Fourth Amendment. *In re Sealed Case*, 310 F.3d at 740-42 (discussing multiple procedural protections necessary to render FISA constitutional). These cases leave no doubt that minimization procedures—standing alone, as in the FAA—cannot suffice.

II. The FAA's Minimization Procedures Fail to Provide Sufficient Privacy Protections for U.S. Persons to Render the Surveillance Reasonable

Even if minimization was an adequate constitutional substitute for prior judicial determinations of individualized suspicion and the particularized identification of a surveillance target, the FAA's specific minimization procedures fail in practice to vindicate constitutional privacy rights. The FAA's surveillance scheme is qualitatively different than that of traditional FISA, yet the minimization regime developed in the context of individualized searches has been imported without alteration into the FAA statutory scheme. Given the differences in the two regimes, the minimization procedures developed under FISA, whatever their constitutional significance in that context, are insufficient to render the FAA's very different scheme constitutional.

A. FAA Surveillance Significantly Differs from FISA Surveillance

While FAA surveillance may be targeted abroad, it is not a program to capture overseas communications because overseas targets will be engaged in communications

with someone else—often in the United States. The surveillance inevitably sweeps up communications of U.S. persons engaged in international communications. *See supra* at 10-11.

The FAA's spying authorization differs from the FISA's in two further important—and legally significant—ways.

First, the FAA does not require the government to identify with any specificity either the target or the particular communications it aims to intercept. Traditional FISA orders must specify

> the identity, if known, or a description of the targets, . . .the nature and location of each of the facilities or places at which the electronic surveillance will be directed, . . . the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance, . . . [and] the means by which the electronic surveillance will be effected."

50 U.S.C. § 1805(c)(1). By contrast, FAA authorizations require only that targeting procedures are "reasonably designed to" limit targets to "persons reasonably believed to be located outside the United States." § 1881a(d)(1). The government is explicitly exempted from identifying "specific facilities, places, premises, or property at which an acquisition . . . will be directed or conducted." § 1881a(g)(4). Nor need it limit collection to any particular targeted individual or type of communication. The FAA thus marks a dramatic shift from a regime of individualized authorizations to one of "blanket" or "programmatic" warrants. The latter yields interception of, for example, all communications to or from an entire geographic area, or all communications traveling via a certain fiber-optic cable connecting Western Europe with South Asia. *See* James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* 175-96; 203-08 (2008) (describing how communications transit the globe via

fiber-optic cable and how these communications can be intercepted and collected at various transit hubs).

Second, the FAA permits surveillance with no justificatory factual predicate. Under FISA, the government can initiate surveillance of a target *only if* it establishes "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a). Authority to conduct surveillance is carefully limited to targets most likely to yield foreign intelligence. But the FAA requires only that "a significant purpose of the acquisition is to obtain foreign intelligence information." § 1881a(g)(2)(A)(v). The government need not indicate that the target(s) are suspected of any activity harmful to the U.S. *Cf. In re Terrorist Bombings*, 2008 WL 4967686, at *15-17 (finding surveillance reasonable once the government had demonstrated that it *specifically* targeted five telephone numbers suspected of being used by al Qaeda associates).

B. FISA's Minimization Procedures Fail to Work Effectively Under the FAA

These two differences make minimization procedures used under traditional FISA insufficient to protect Fourth Amendment interests under the FAA. In foreign intelligence surveillance operations, little effort is made to minimize collection. Instead, "recording devices capture all communications . . . transmitted over a monitored facility." Kris & Wilson, supra, at § 9:4. Rather than a surveillance narrowly targeted at specific, individualized subjects that is likely to yield information relevant to U.S. national interests, the FAA envisages the capture *en masse* of large volumes of communications without any filtering mechanism to screen out personal, innocent communications with no foreign intelligence value.

While the FAA radically changed the initial showing that the government must make to initiate surveillance, it failed to make any corresponding change to the minimization statute. *See supra* at 8; Def.'s Br. at 52. But the same minimization rules, transplanted into wholly new circumstances, operate differently given the changed nature of the surveillance. Even the traditional FISA regime recognized that heightened protections for U.S. persons' communications are necessary when courts do not provide sufficient scrutiny of targeting decisions. 50 U.S.C. § 1801(h)(4) (increasing stringency of minimization requirements when permitting surveillance with no court order). But the FAA abandons this insight. Rather than augmenting minimization procedures, it leaves them unmodified as the government expands the scope of its nearly indiscriminate surveillance.

Traditional FISA authorizations force a filtering out of *most* non-foreign intelligence-related communications at the outset due to narrow targeting of the surveillance. But only a very small percentage of communications captured under blanket FAA surveillance will comprise foreign intelligence: The ratio of unprotected to protected material collected is thus dramatically different.

As courts have recognized in the domestic criminal surveillance context, minimization procedures can become so "diluted" the attendant surveillance is unconstitutional. *United States v. Figueroa*, 757 F.2d 466, 472 (2d Cir. 1985); *see also Scott*, 436 U.S. at 147-48 (Brennan, J., dissenting) (warning that "unravel[ing] individual threads of statutory protection without regard to their interdependence and to whether the cumulative effect is to rend the fabric of" Congress's efforts to ensure domestic criminal surveillance is conducted in a manner consistent with the Constitution). By expanding

surveillance authority so as to abandon any possible nexus between individualized searches and specific minimization rules, the FAA dilutes beyond repair the minimization function.

The harm wrought by the FAA's broad acquisition is compounded at retention and dissemination stages. Having swept up unknown numbers of communications involving U.S. persons, the government is permitted by the FAA to retain and disseminate any "foreign intelligence information." 50 U.S.C. § 1801(h)(1). "Foreign intelligence information" is, however, defined to encompass not only information about "actual or potential attack or other grave hostile acts . . .; sabotage, international terrorism, or the international proliferation of weapons of mass destruction . . .; or clandestine intelligence activities by an intelligence service" and information about the "national defense or the security of the United States," but also any communications concerning the "conduct of the foreign affairs of the United States." § 1801 (e). This is an extremely broad definition, susceptible of expansive interpretation. Most or all of the professional communications of plaintiff journalists and human rights organizations, for example, would fall squarely into this exception. *See* Compl. at ¶¶ 45-48. Moreover, standard minimization procedures call for the retention of all information unless it "could not be" foreign intelligence information. *In re All Matters*, 218 F. Supp. 2d at 618. Combining the vast initial collection contemplated by the FAA, the extremely permissive retention standard, and the broad foreign-intelligence definition, it is inevitable that large volumes of U.S. persons' communications will remain in government databases.

The minimization procedures on retention and dissemination have more loopholes. Even if information does not meet statutory definition of "foreign

intelligence," it still can be disseminated if the identities of U.S. persons involved are excised. Identifying information need not be purged from files in which the information is stored. 50 U.S.C. § 1801(h)(2). Moreover, if the identifying information is "necessary to understand foreign intelligence information or assess its importance," non-foreign intelligence information can be disseminated with identifying information intact. § 1801(h)(2). And evidence of a crime always can be retained and disseminated. § 1801(h)(3). Again, the threats to privacy posed by these elements of the definition of minimization are significantly more severe under the FAA than they were under FISA because of the different volumes of threshold collection. Many innocent Americans' communications will inevitably be collected under the FAA absent individualized suspicion, retained in government files indefinitely, and disseminated throughout government.

Other elements of the statutory definition of minimization procedures also fail to provide effective safeguards for the FAA regime. The definition of minimization procedures requires that the procedures be "reasonably designed *in light of the purpose and technique of the particular surveillance*, to minimize the acquisition and retention, and prohibit the dissemination" of information concerning U.S. persons. § 1801(h)(1) (emphasis added). But if the "purpose and technique of the particular surveillance" is to engage in mass collection of communications—e.g., those going in or out of the Green Zone in Iraq—then minimization provides no constraint whatsoever. This loose statutory definition thus imposes no meaningful obligation on the government to tailor its minimization to the new FAA context.

Similarly, a FISC determination that procedures are "reasonably designed," § 1801(h)(1), to minimize U.S. persons' information does not guarantee those procedures will achieve their goal. Under the FAA, the FISC must approve minimization procedures when surveillance begins but lacks authority thereafter to monitor the effectiveness or to order modifications to those procedures. *See* § 1881a(e), (g), (i). As the drafters of FISA recognized, ongoing judicial scrutiny is the best—perhaps only—way to ensure that procedures developed in the abstract in fact play their intended privacy-protecting role. Both the traditional FISA and domestic criminal surveillance regimes recognize this fact in providing for continued judicial supervision of minimization procedures—a feature conspicuous by its absence from the FAA. *See* 18 U.S.C. § 2518; 50 U.S.C. § 1805.

Recent evidence confirms that without ongoing judicial supervision, procedures intended to restrict the government's use of surveillance fail. Breaches of such procedures include violations of minimization procedures, Bamford, *supra*, at 1, 108, 129-30, as well as other important restraints on foreign intelligence surveillance, Brian Ross, Vic Walter, & Anna Schecter, *Whistleblower: U.S. Snooped on Tony Blair, Iraqi President*, abcnews.com, Nov. 24, 2008 (reporting U.S. surveillance of the communications of then-British Prime Minister Tony Blair in violation of a long-standing agreement between the U.S. and Britain to refrain from collecting intelligence on one another). "Trust us," is clearly inadequate when it comes to electronic surveillance.

In the immediate aftermath of the 9/11 attacks, then-NSA director Michael Hayden unilaterally (and without White House approval) dropped the FISA-mandated minimization procedures with respect to communications between Afghanistan and the United States. Bamford, *supra*, at 108. And other post-9/11 surveillance efforts—

purportedly targeted only at those with demonstrated ties to al Qaeda, Bamford, *supra*, at 131—imposed no meaningful limits on either the targets selected or the use of acquired information. According to one analyst, the NSA as a result knowingly collected the communications of journalists, employees of nongovernmental organizations such as the Red Cross, and businesspeople. "[E]ven though the intercept operators knew they were eavesdropping on American journalists communicating with other journalists and their families in the U.S., the decision was made to continue listening to, recording, and storing the conversations. 'Basically all rules were thrown out the window.'" *Id.* (quoting Adrienne Kinne); *accord* Brian Ross, Vic Walter, & Anna Schecter, *Inside Account of U.S. Eavesdropping on Americans*, abcnews.com, Oct. 9, 2008 (stating that targets of surveillance were "everyday, average, ordinary Americans who happened to be in the Middle East . . . and happened to be making these phone calls"). Analysts who voiced concerns that what they were being asked to do violated regulations such as USSID 18 were sidelined. Bamford, *supra*, at 131-33. That such contempt for rules and Americans' privacy can develop in carrying out a secret operation illustrates vividly why prior judicial review of targets and ongoing judicial oversight are both necessary to protect Americans' privacy rights.

Nor does the semi-annual reporting to the FISC of the results of the Attorney General and Director of National Intelligence's review of incidents of noncompliance with minimization procedures, see 50 U.S.C. § 1881a(l)(1), the possibility of Inspector General review, § 1881a(l)(2), or annual review by the heads of intelligence community elements, § 1881a(l)(3), substitute for ongoing *judicial* superintendence. The Framers,

after all, installed a separation of powers in the Constitution precisely because they mistrusted internal checks.

The FAA authorizes surveillance operations that wholly lack particularity under minimization procedures that provide scant protection of U.S. persons' communications and that preclude ongoing judicial monitoring, guaranteeing that the universe of protected communications intercepted, retained, and available for dissemination is unreasonably vast. Consequently, U.S. persons' Fourth Amendment rights do not receive sufficient protection under the FAA.

CONCLUSION

For all the foregoing reasons, this Court should deny Defendants' motion to dismiss and proceed to the merits.

Respectfully submitted,

/s/ Laura Abel

LAURA ABEL
Emily Berman
Aziz Huq
THE BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
161 Avenue of the Americas, 12th Floor
New York, NY 10013
(212) 998-6730
Counsel for Amici The Rutherford Institute and the Brennan Center for Justice

December 19, 2008

Counsel for Amici Curiae