09-4112-cv

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

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, SYLVIA ROYCE,

Plaintiffs-Appellants,

—against—

JOHN MCCONNELL, in his official capacity as Director of National Intelligence, KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service, ERIC H. HOLDER, in his official capacity as Attorney General of the United States,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF AMICI CURIAE THE BRENNAN CENTER FOR JUSTICE, THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE CONSTITUTION PROJECT, THE ELECTRONIC FRONTIER FOUNDATION AND THE RUTHERFORD INSTITUTE IN SUPPORT OF PLAINTIFFS-APPELLANTS

BARBARA MOSES
MORVILLO, ABRAMOWITZ, GRAND, IASON, ANELLO & BOHRER, P.C.
565 Fifth Avenue
New York, New York 10017
(212) 856-9600

EMILY BERMAN
ELIZABETH GOITEIN
THE BRENNAN CENTER FOR JUSTICE
161 Avenue of the Americas, 12th Floor
New York, New York 10013
(212) 998-6730

(Counsel continued on inside cover)

SHARON BRADFORD FRANKLIN
Senior Counsel
THE CONSTITUTION PROJECT
1200 18th Street, N.W., Suite 1000
Washington, D.C. 20036
(202) 580-6928

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTIONAL AND STATUTORY MATERIALS

MISCELLANEOUS

INTEREST OF AMICI CURIAE

The Brennan Center for Justice at New York University School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and the limits of executive power in the fight against terrorism. The Brennan Center is concerned with the dangers that our national security policies pose to privacy and other constitutional liberties. A primary focus of the Brennan Center is preserving the separation of powers, which the Framers intended as a bulwark against violations of Americans' freedoms.

The Center for Democracy & Technology is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet and other communications networks. The Center represents the public's interest in an open, decentralized Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Constitution Project is an independent, nonprofit organization that brings together legal and policy experts from across the political spectrum to promote and defend constitutional safeguards. After September 11, 2001, the Project created its bipartisan Liberty and Security Committee, a blue-ribbon committee of prominent Americans, to address the importance of preserving civil liberties as we work to protect our Nation from international terrorism. The

committee develops policy recommendations on such issues as U.S. detention and surveillance policies, and emphasizes the need for all three branches of government to play a role in preserving constitutional rights.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry, government and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF is based in San Francisco, has members all over the United States, and maintains one of the most-linked-to Web sites (http://www.eff.org) in the world.

The Rutherford Institute is an international civil liberties organization founded in 1982 by its President, John W. Whitehead. The Institute provides legal representation without charge to individuals whose civil liberties are threatened or violated, and educates the public about constitutional and human rights issues. The Rutherford Institute is concerned that invasive governmental policies pose an imminent danger to key constitutional guarantees — principally those protected by the Fourth Amendment. For 27 years, attorneys affiliated with the Institute have represented numerous parties before this Court. The Rutherford Institute has also filed amicus curiae briefs in cases dealing with critical constitutional issues arising

from the fight against terrorism. *See, e.g.*, *Munaf v. Geren*, 128 S. Ct. 2207 (2008); *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006); *Rasul v. Bush*, 542 U.S. 466 (2004).

Amici submit this brief, in support of plaintiffs-appellants' appeal from the district court's order below, to underscore the importance of judicial review of the facial validity of the Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261 (2008) ("FAA"). Amici respectfully urge this Court to reverse the lower court's determination that plaintiffs lack standing to challenge the FAA, remand this case to the district court, and direct that court to hear plaintiffs' challenge on the merits.

SUMMARY OF ARGUMENT

Throughout our nation's history, the federal courts have proved essential to policing the constitutional boundaries of congressional enactments and executive action. When the political branches have trenched on constitutionally protected individual rights through improper electronic surveillance, the courts have not hesitated to invalidate those actions, jealously guarding Americans' privacy rights, guaranteed by the Fourth Amendment, and expressive rights, guaranteed by the First. Americans rely upon this ongoing oversight to ensure that our government, in exercising its obligation to defend the national interest, preserves the liberties that make that national interest worth defending.

The district court effectively excluded the federal courts from serving this critical oversight role in holding that plaintiffs "lack Article III standing to bring this constitutional challenge" because they could not prove that their own calls or emails were targeted for interception or acquired by the government. *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633, 658 (S.D.N.Y. 2009). Plaintiffs established below that their telephone calls and emails fall squarely within the class of communications that the FAA permits the government to "acquire" without a warrant, and that they have undertaken costly and burdensome measures to protect the privacy of their communications. If these undisputed facts are not sufficient to establish standing, the facial validity of the FAA is effectively immunized from meaningful judicial review, *see* Pls.-Appellants' Br. 50-54, and so, by implication, is the validity of virtually any surveillance program designed to collect foreign intelligence.

Plaintiffs persuasively show that the district court erred in dismissing this action on standing grounds. Amici submit this brief to draw this Court's attention to the very real dangers inherent in eliminating judicial review of laws governing secret surveillance.

As Part I demonstrates, the history of unchecked warrantless electronic surveillance by the government is a history of abuse. Time and again, in the absence of meaningful, judicially enforced *ex ante* legal boundaries or *ex post*

accountability, the nation's intelligence agencies have intruded upon the First and Fourth Amendment rights of law-abiding Americans. Indeed, Congress enacted the Foreign Intelligence Surveillance Act, Pub. L. 95-511, 92 Stat. 1783 (1978) ("FISA"), precisely to curb such abuses, after it was revealed that secret surveillance ostensibly designed to gather "foreign intelligence" during the Cold War had in fact been used to eavesdrop on and harass Americans – including journalists, activists, and even 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).

Noting the risk of abuse, the Supreme Court has recognized that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." *Berger v. New York*, 388 U.S. 41, 63 (1967). This warning is no less true now than it was three decades ago, when the pattern of abuse that led to FISA's enactment was revealed. In the aftermath of 9/11, the executive branch conducted a range of secret surveillance activities, such as the Terrorist Surveillance Program ("TSP"), that were unauthorized under FISA and quite possibly unconstitutional. More recently, "overcollection" of communications by the National Security Agency ("NSA") under the FAA already has been widely reported, on a scale that may dwarf even the government's most

avid collection efforts during the Cold War. *See, e.g.*, Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 16, 2009, at A1 (hereinafter "*Wiretaps Exceeded Law*") (quoting intelligence officials describing the problem as "significant and systemic").[1] At bottom, these activities have been enabled by either the evasion (in the case of the TSP and related activities) or the absence (in the case of the FAA) of effective judicial oversight.

Recognizing the tendency of the intelligence community to err on the side of excess if left unchecked, FISA generally prohibited electronic surveillance of communications involving U.S. persons except pursuant to carefully calibrated statutory protections, enforced through judicial oversight. As this brief demonstrates in Part II, however, the FAA dramatically weakens the judiciary's role in enforcing any limits on the government's power to engage in electronic surveillance of Americans' international communications, even as it vastly expands this power.

The district court's decision must be analyzed against this backdrop. Because the FAA itself eliminates meaningful oversight by the Foreign Intelligence Surveillance Court ("FISC") of the day-to-day application of the statute, and because the FISC has held that it has no authority to review the constitutionality of the FAA on its face, *see In re Proceedings Required by § 702(i)*

[1] Available at: http://www.nytimes/2009/4/16/us/16nsa/html (last visited December 18, 2009).

of the FISA Amendments Act of 2008, No. Misc. 08-01, slip. op. at 10 (FISA Ct. Aug. 27, 2008), challenges like the case at bar provide the only effective avenue for the federal courts to exercise their most critical constitutional function: to "say what the law is." *Marbury v. Madison*, 1 Cranch 137, 177, 2 L. Ed. 60 (1803). The district court's approach to standing virtually guarantees that no court will ever conduct such oversight. The decision is therefore not only erroneous, *see* Pls.-Appellants' Br. 22-50, but also threatens to abdicate the courts' historical role as the guardian of Americans' civil liberties against abuses of power by the other branches of government.

ARGUMENT

I. In the Absence of Sufficient Judicial Oversight Over Executive Surveillance Authority, that Authority Is Prone to Abuse

The fundamental nature of the rights provided by the First and Fourth Amendments, and the courts' vital role in protecting those rights, are beyond question. "[T]he security of one's privacy against arbitrary intrusion by the [government] – which is at the core of the Fourth Amendment – is basic to a free society." *Berger*, 388 U.S. at 53 (quoting *Wolf v. Colorado*, 338 U.S. 25, 27 (1949)). Similarly, the right of free speech, guaranteed by the First Amendment, is "among the most fundamental personal rights and liberties which are secured to all persons" by the Constitution. *Thornhill v. Alabama*, 310 U.S. 88, 95 (1940). It is the role of the courts to protect such fundamental individual rights against

infringement by the political branches. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 577 (1992) ("'Congress established courts to adjudicate cases and controversies as to claims of infringement of individual rights whether by unlawful action of private persons or by the exertion of unauthorized administrative power.'") (quoting *Stark v. Wickard*, 321 U.S. 288, 309-310 (1944)); *Mistretta v. United States*, 488 U.S. 361, 380 (1989) (reaffirming "the central judgment of the Framers of the Constitution that, within our political scheme, the separation of governmental powers into three coordinate branches is essential to the preservation of liberty"). Under our constitutional system of separated powers, the federal courts thus have "the duty to review the constitutionality of congressional enactments." *United States v. Munoz-Flores*, 495 U.S. 385, 391 (1990).

Nor can concerns that our national security is at stake prevent the courts from considering the constitutionality of a statute. "The laws and Constitution are designed to survive, and remain in force, in extraordinary times. Liberty and security can be reconciled; and in our system they are reconciled within the framework of the law." *Boumediene v. Bush*, 128 S. Ct. 2229, 2277 (2008); s*ee also Dennis v. United States*, 341 U.S. 494, 520 (1951) ("[E]ven the all-embracing power and duty of [national] self-preservation are not absolute. Like the war power . . . it is subject to applicable constitutional limitations. Our Constitution has no provision lifting restrictions upon governmental authority during periods of

emergency.") (internal citation omitted).

If anything, ensuring a meaningful role for the courts becomes even more important where, as here, the authority claimed by the government includes wiretapping – long recognized as one of the most dangerous "threats to liberty." *Berger*, 388 U.S. at 63. Time and again, the courts' role as the protector of "'constitutional rights and liberties of individual citizens and minority groups against oppressive or discriminatory government action,'" *Raines v. Byrd*, 521 U.S. 811, 829 (1997) (quoting *United States v. Richardson*, 418 U.S. 166, 192 (1974) (Powell, J., concurring)), has proved essential to the preservation of fundamental rights in the surveillance context. *See, e.g., Berger*, 388 U.S. at 55-61 (invalidating New York's wiretapping statute as violative of the Fourth Amendment); *Katz v. United States*, 389 U.S. 347, 357 (1967) (holding unconstitutional under the Fourth Amendment any wiretap "conducted outside the judicial process, without prior approval by judge or magistrate"); *United States v. U.S. Dist. Ct. for the E. Dist. of Mich. (Keith)*, 407 U.S. 297, 320-21(1972) (holding unconstitutional electronic surveillance for domestic security purposes absent a warrant).

Conversely, in those situations where meaningful judicial oversight has been absent, executives agencies empowered to spy on Americans have tended to abuse that power. From the 1930s through the 1970s, Democratic and Republican administrations alike wiretapped and bugged American citizens without any

judicial authorization. *See* Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755, at 12 (1976) (hereinafter "Church Committee Book II"). Initially, the surveillance was aimed at potential agents of totalitarian powers. *Id*. at 21. Over time, however – based on imprecise targeting rules such as seeking out "subversive activities" – there was a "steady increase in the government's capability and willingness to pry into, and even disrupt, the political activities and personal lives of people." *Id.* The focus of surveillance efforts thus shifted to political dissidents and civil rights organizations "without regard for the consequences to American liberties." *Id*. at 22.

Examples of the improper surveillance that took place during the Cold War in the absence of sufficient judicial oversight are legion. For instance, as part of a secret FBI program known as COINTELPRO (for "Counter Intelligence Program"), the NAACP was investigated for more than 25 years, theoretically to determine whether it "had connections with" the Communist Party. Church Committee Book II at 8, 232. The government used electronic surveillance (among other methods) to collect information about NAACP lobbying and advocacy efforts, and the FBI's extensive reports on the NAACP were shared with military intelligence. *Id*. at 81 n.350. These activities continued despite a report

from the very first year of the investigation indicating that the NAACP had a "strong tendency" to "steer clear of Communist activities." *Id*. at 8.

Perhaps most notoriously, the FBI targeted Dr. Martin Luther King, Jr., in an effort to "neutralize" him as a civil rights leader. Church Committee Book II at 11 (internal quotation marks omitted). The FBI used "nearly every intelligence-gathering technique at [its] disposal," including electronic surveillance, to obtain information about the "private activities of Dr. King and his advisors" in order to "completely discredit" them. *Id*. (internal quotation marks and citation omitted). For example, the FBI mailed to Dr. King a recording from microphones hidden in his hotel rooms, made in an effort to destroy Dr. King's marriage. *Id*.

Other groups and individuals who posed no threat to national security were subject to surveillance under COINTELPRO as well. In addition to civil rights groups like the Southern Christian Leadership Conference, the Congress on Racial Equality, the Student Nonviolent Coordinating Committee, and the Urban League, Church Committee Book II at 105, 167, members of the women's liberation movement, conservative Christian groups, and anti-war student groups like Students for a Democratic Society also were subject to warrantless surveillance. *Id*. at 7, 105.

COINTELPRO was not the only massive government surveillance program conducted during this period. Other such programs included "Operation

Shamrock," under which the NSA conducted blanket surveillance of all cables coming into and going out of the United States. By the 1960s, when paper telegrams gave way to computer discs containing the messages, NSA employees visited cooperative telecommunications companies to "secretly collect the discs . . . during the midnight shift, copy them, and then take the copies to [NSA headquarters at] Fort Meade." James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* 168 (2008). In addition, from the 1960s through 1973, the NSA intercepted and disseminated the international communications of "selected American citizens and groups on the basis of lists of names supplied by other Government agencies," including individuals and groups involved in the anti-war and civil rights movements. Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans (Book III), S. Rep. No. 94-755, at 739 (1976) (hereinafter "Church Committee Book III"). The U.S. Army operated its own surveillance program, under which it assembled files on nearly 100,000 Americans. Church Committee Book II at 174.

Thwarting communist subversion was the purported justification for most of this surveillance. *See* Mark Tushnet, *Making Civil Rights Law: Thurgood Marshall and the Supreme Court*, 1931-1961 295 (1994). Nonetheless, as the scope of surveillance grew, the intelligence agencies' activities became "purely

political." Church Committee Book II at 118, 225. People were targeted for surveillance "on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power." *Id*. at 5. As the Church Committee noted, the imprecision of labels such as "subversive activities," "foreign intelligence," and "national security" enabled surveillance programs, originally designed to protect the nation's security, to expand to include improper surveillance of American citizens "who posed no criminal or national security threat to the country." *Id*. at 205 (internal quotation marks omitted). The Committee concluded, starkly, that unchecked surveillance activity inevitably "exceed[s] the restraints on the exercise of governmental power which are imposed by our Country's Constitution, laws, and traditions." *Id*. at 2.

Recent years have borne out this conclusion. Within days after September 11, 2001, Michael Hayden, then the Director of National Security, simply dropped FISA-mandated minimization rules with respect to communications between the U.S. and Afghanistan. *See* Bamford, *supra*, at 108. The following month, "the President authorized the NSA to undertake a number of new, highly classified intelligence activities," including what became known as the Terrorist Surveillance Program. Offices of the Inspectors General of Dep't of Defense, Dep't of Justice, Central Intelligence Agency, Nat'l Security Agency, & Office of the Director of Nat'l Intelligence, *Unclassified Report on the President's Surveillance Program*,

Report No. 2009-00133-AS, at 5-6 (July 10, 2009) (hereinafter "*Unclassified Report*").[2] The existence of the President's authorizations, and the warrantless wiretapping conducted pursuant thereto, remained secret until late 2005, when, in response to press reports, the President stated that he had authorized interceptions of electronic communications where there was a "reasonable basis to conclude that one party to the communication" was a member or agent of al-Qaeda or an al-Qaeda-affiliated group. *Id*. Rather than seek authorization from the FISC for these intercepts, the White House took the position that FISA "cannot restrict the President's ability to engage in warrantless searches that protect the national security." *Id*. at 11.

The legality of the TSP remains doubtful at best. *See* Eric Lichtblau & James Risen, *U.S. Wiretapping of Limited Value, Officials Report*, N.Y. Times, July 11, 2009, at A1 (noting "fierce debate" about the legality of the TSP when it was revealed in 2005).[3] Moreover, despite the President's assurances, it now appears that the government's warrantless intercepts were not limited to communications to or from individuals suspected of terrorist ties. *See* Bamford, *supra*, at 129-34 (NSA intercept operators eavesdropped and recorded the

[2] Available at: http://www.justice.gov/oig/special/s0907.pdf (last visited December 18, 2009).

[3] Available at: http://www.nytimes.com/2009/07/11/us/11nsa.html (last visited December 18, 2009).

conversations of humanitarian aid workers, journalists, and American troops calling home from Iraq); *Countdown: Did U.S. Spy on Journalists?* (MSNBC television broadcast January 21, 2009) (interview of Russell Tice, former NSA analyst, stating that the NSA specifically identified communications to and from American news organizations and "the collection on those organizations was 24/7")[4]; Brian Ross, Vic Walter & Anna Schecter, *Inside Account of U.S. Eavesdropping on Americans* (ABC News Oct. 9, 2008) (quoting Adrienne Kinne, an Army Reserve linguist assigned to the NSA, explaining that she was asked to monitor "everyday, average, ordinary Americans who happened to be in the Middle East, in our area of intercept," including U.S. military officers, journalists and aid workers).[5]

These post-9/11 transgressions highlight the importance of judicial review that is available in practice as well as in name (a point that has particular resonance in the case at bar). At the time the TSP and related surveillance activities were undertaken, both *ex ante* and *ex post* judicial review theoretically were available under FISA. However, the government evaded *ex ante* review by ignoring its

---

[4] Available at: http://www.msnbc.msn.com/id/28794766/ (last visited December 21, 2009).

[5] Available, together with ABC's related *Nightline* story, at: http://abcnews.go.com/Blotter/story?id=5987804&page=1 (last visited December 18, 2009).

statutory obligations to obtain particularized orders from the FISC. Further, while *ex post* review should serve as a backstop in such cases, the government thus far has managed to stymie any efforts at obtaining such review. Accordingly, several years after the TSP and related activities came to light, the courts have yet to rule on the critical question of whether these activities – many aspects of which now have been incorporated into the FAA – violated FISA and/or the Constitution of the United States.

The most recent example of surveillance excesses in the absence of sufficient judicial oversight grows out of the FAA itself. As detailed in Part II, *infra*, that statute virtually eliminates any judicial role in overseeing the implementation of surveillance with respect to Americans' international communications. It is therefore not surprising that, despite the unprecedented authority granted by the statute, the government already has exceeded that authority: government officials themselves acknowledge that the NSA, while purportedly acting under the authority granted by the FAA to collect international communications, has in fact overcollected the "domestic communications of Americans." *See Wiretaps Exceeded Law, supra* (reporting that the NSA has difficulty distinguishing between communications inside the United States and those overseas, which "led the agency to inadvertently 'target' groups of Americans and collect their domestic communications without proper court

authority"); James Risen and Eric Lichtblau, *E-Mail Surveillance Renews Concerns in Congress*, N.Y. Times, June 16, 2009, at A1 (hereinafter "*E-mail Surveillance*") (reporting that the NSA is facing "renewed scrutiny over the extent of its domestic surveillance program, with critics in Congress saying its recent intercepts of the private telephone calls and e-mail messages of Americans are broader than previously acknowledged").[6] That such excesses continue to occur illustrates the pressing need for the availability of some form of effective judicial review of government surveillance activities.

The harm caused by "overcollection" of Americans' private communications is neither theoretical nor trivial. The Fourth Amendment is violated "at the time of an unreasonable government intrusion," regardless of how the unlawfully seized communication is later used. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990). Moreover, government officials empowered to conduct surveillance with insufficient oversight "may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Keith*, 407 U.S. at 317. During the Cold War, intelligence agencies routinely misused information gleaned through surveillance to "neutralize the actions" of Americans engaged in core political speech and advocacy. Church Committee Book II at 3. Even the threat of such targeting can exert a powerful

[6] Available at: http://www.nytimes.com/2009/06/17/us/17nsa.html (last visited December 18, 2009).

chilling effect on the exercise of First Amendment freedoms, flying in the face of the Supreme Court's admonition that "the price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power." *Keith*, 407 U.S. at 314.

In short, electronic surveillance involving the communications of U.S. persons touches on – and presents a unique danger to – core First and Fourth Amendment rights. Judicial oversight is critical to preserving those rights, and when it has been absent or insufficient, the predictable result has been abuses and surveillance outside the bounds of the law. The importance of a robust role for the courts in reviewing the legality of executive branch surveillance activities has thus been demonstrated throughout this nation's history and cannot be overstated.

II. If the District Court Decision Stands, There Will Be No Meaningful Judicial Oversight of Executive Surveillance Under the FAA.

Recognizing the threats posed by unchecked electronic surveillance, the Church Committee warned that if "new and tighter controls" were not established, our "intelligence agencies threaten to undermine our democratic society and fundamentally alter its nature." Church Committee Book II at 1. Heeding this warning, Congress passed FISA to embody those "new and tighter controls" – and, critically, to subject those controls to judicial scrutiny.

In its original form, FISA required the government to apply for and receive an individualized and particularized order from the FISC before initiating

surveillance. 50 U.S.C. §§ 1804-1805. The statute required the FISC's order to specify the individual target of the surveillance and the facilities or places to be monitored, and such an order could issue only if the government established probable cause that the target of the surveillance was a foreign power or an agent of a foreign power. *Id*. FISA also gave the FISC the authority to monitor the government's compliance with its orders, to prevent (among other things) the "overcollection" of communications to and from non-targeted Americans, and to ensure that the government takes appropriate steps to minimize the incidental acquisition, dissemination, and use of information about U.S. persons. *Id*. § 1805(e)(3).

Supporters and detractors alike recognize that the FAA significantly weakens these longstanding limits on government wiretapping of communications to and from U.S. citizens and lawful residents. *See, e.g.*, Siobhan Gorman, *Deal Set on Domestic Spy Powers*, Wall St. J., June 20, 2008, at A1 (FAA is "the most sweeping rewrite of U.S. domestic-spying powers in three decades, ensuring that much of the controversial surveillance operation created by President Bush in secret will outlast his administration")[7]; *Compromising the Constitution*, N.Y. Times, July 8, 2008, at A20 (FAA will "needlessly expand the government's ability to spy on Americans and ensure that the country never learns the full extent

[7] Available at: http://online.wsj.com/article/SB121388542478988553.html (last visited December 18, 2009).

of President Bush's unlawful wiretapping").[8] Indeed, according to five federal Inspectors General, the FAA gives the government "even broader authority to intercept international communications" than did the secret authorizations that President Bush signed during the pendency of the TSP, discussed in Part I, *supra*. *Unclassified Report*, *supra*, at 31.

Plaintiffs' brief aptly details the FAA's vast expansion of the government's surveillance authority. Pls.-Appellants' Br. 8-12. At the same time this authority has been expanded, the role of the judiciary in overseeing it has been curtailed dramatically – a point that plaintiffs mention, *see id.* at 12-13, but that bears elaboration. The role of the judiciary has been minimized in four primary ways that exacerbate significantly the statute's potential to intrude on constitutionally protected rights.

First, for electronic surveillance involving wire communications into or out of the United States, the FAA gives the FISC no role in approving the particular "target[s]" of the proposed surveillance, the "facilities" at which the surveillance will be directed, or the "means" by which the surveillance will be effected. *Compare* 50 U.S.C. § 1805(c)(1) *with id*. §§ 1881a(d)(1), 1881a(g)(4). Under the FAA, the government need only certify that its procedures are "reasonably designed" to limit the "target[s]" of the surveillance to "persons reasonably

[8] Available at: http://www.nytimes.com/2008/07/08/opinion/08tue1.html (last visited December 18, 2009).

believed to be located outside the United States." 50 U.S.C. § 1881a(d)(1)(A).[9] The FAA thus abandons the requirement, present in both FISA and domestic criminal law, *see id*. § 1805(c)(1); 18 U.S.C. § 2518(4), and seemingly compelled by the Fourth Amendment, U.S. Const. amend. IV (requiring warrants "particularly describing the place to be searched, and the persons or things to be seized"), of a particularized court order.

Second, the FAA eliminates the requirement that the FISC find "probable cause" that the targets of surveillance are "foreign power[s]" or "agent[s] of a foreign power." 50 U.S.C. § 1805(a)(2)(A). Instead, the government need only certify that a "significant purpose" of the surveillance is to obtain "foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v).[10] The court's *ex ante*

[9] The FAA for the first time permits warrantless surveillance, on a mass scale, where one end of a wire communication is *known* to be in the United States, or where one or more participants to that communication are *known* to be Americans. The only wire communications that the government is not permitted to intercept under the FAA are those that take place wholly within the United States, or wholly among United States citizens or lawful permanent residents. 50 U.S.C. § 1881a(g)(2)(A)(i)(II). Thus, although wiretaps under the FAA must "target" non-U.S. persons outside of the U.S., *see id*. § 1881a, the communications thereby acquired are the telephone calls, emails, instant messages, fax transmissions, and other wire communications sent to or received from those non-U.S. persons *by Americans, in America*. As the government acknowledged below, the "constitutionally protected privacy interests implicated by the statute are those of the U.S. persons whose communications are collected as an incident to surveillance targeted at others." Def.'s Mem. in Opp'n to Pls.' Mot. For Summ. J. at 53 n.39.

[10] "Foreign intelligence information" is defined broadly to include, *inter alia*, any information that relates to "the national defense or security of the United States" or "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2).

role is thus reduced from evaluating the merits of the government's probable cause showing to verifying that the government has "certified" to the necessary factors. It comes as no surprise, given this exceedingly low standard, that in 2008 the FISC approved over 99.95% of the surveillance applications placed before it by the government.[11]

Third, the FAA removes the FISC's authority to monitor minimization procedures – the procedures that the government must put in place to minimize the "incidental" acquisition, retention, or dissemination of "nonpublicly available information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1). Under the FAA, as under FISA, the government must present its proposed "minimization" procedures to the FISC for approval. 50 U.S.C. § 1881a(g)(2)(A)(ii). But while the original FISA authorizes the FISC to assess both the facial sufficiency of the procedures and whether the government has in fact complied with them, *see* 50 U.S.C. § 1805(d)(3), the FAA permits the FISC to review minimization procedures only prospectively and in the abstract. *Id.* § 1881a(i). No judicial officer is empowered to determine whether such procedures,

[11] During calendar year 2008, the government reported that it made 2,082 applications to the FISC for authority to conduct electronic surveillance and/or physical searches, and that the FISC approved 2,081 of them. The FAA was enacted in July of 2008. *See* Letter from Assistant Attorney General Ronald Weich to the Hon. Harry Reid, May 14, 2009, available at http://www.justice.gov/nsd/foia/reading_room/2008fisa-ltr.pdf (last visited December 18, 2009).

as actually implemented, satisfy either the statute or the Constitution. Similarly, although the FISC must verify that the government's proposed targeting procedures are reasonably designed to target people abroad, the FAA limits the FISC's ability to review the implementation of those targeting procedures, so the FISC has no means of ensuring that the government's surveillance activities *actually* target those persons whom it is statutorily authorized to target. *Id*.

In place of an independent judicial review, the FAA calls upon the executive branch itself to conduct a semi-annual assessment of its own compliance with targeting and minimization procedures and guidelines, and to submit that assessment to certain Congressional committees and to the FISC. 50 U.S.C. § 1881a(*l*). Even if the executive were to self-report significant statutory or constitutional violations, however, the FISC could not rescind or modify earlier surveillance authorizations. At best, the government offered below, the FISC could "disapprove such procedures in future § 1881 proceedings." Defs.' Mem. in Opp'n to Pls.' Mot. for Summ. J. 52-53.[12]

[12] In addition to the semi-annual review furnished to the FISC, the FAA requires the Inspectors General of the Justice Department and the various intelligence agencies to conduct another, more pointed review, this one disclosing the number of surveillance targets later determined to be in the United States, as well as the number of disseminated intelligence reports improperly revealing the identities of U.S persons. 50 U.S.C. § 1881a(*l*)(2). This report, however, goes only to the Attorney General, the Director of National Intelligence, and certain Congressional Committees – not the FISC. *Id.*

Fourth, in the highly unusual event that the FISC rejects an FAA surveillance application,[13] the government is empowered to ignore that ruling – and keep the unauthorized wiretap in place – not only during any appeal to the Court of Review, but also during any rehearing *en banc*. 50 U.S.C. § 1881a(i)(4)(B). In short, the FAA does not merely permit the government to eavesdrop on Americans with no particularized warrant, no probable cause, and no ongoing judicial review of the effectiveness of its minimization procedures; it purports to permit such eavesdropping – potentially for months – even if the FISC expressly rules that it is unlawful. Moreover, even if the appeals process ultimately confirms the FISC's original judgment, no court can prohibit the government from using or disseminating the information collected, without court authorization, in the interim.

These changes wrought by the FAA not only raise serious questions about the statute's constitutionality[14]; they render the availability of judicial review in

---

[13] As noted above, *supra* n.11, the odds that the FISC will reject a government surveillance application are approximately 2081 to 1.

[14] Indeed, the very safeguards present in FISA – but not in the FAA – were central to earlier judicial determinations of FISA's constitutionality. *See United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (holding 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'" (quoting S. Rep. No. 95-701, at 13 (1978)); *see also United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (explaining that "FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment").

cases like the one at bar all the more important. As described above, the FAA essentially eliminates meaningful judicial oversight of the statute's day-to-day application. Further, the FISC has held that the "narrowly circumscribed" judicial review function allocated to it does not include "a facial review of the constitutionality of the statute." *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, *supra*, slip. op. at 3, 10 (internal quotation marks omitted). Accordingly, challenges like the one brought by plaintiffs represent the only effective avenue for courts to review the legality of electronic surveillance that sweeps in the communications of law-abiding U.S. persons.[15]

Under the theory of standing advanced by the government and accepted by the district court, however, virtually no one can bring suit to challenge the FAA's constitutionality because the very secrecy the statute enshrines prevents the many Americans whose communications have been acquired from proving that such acquisition has taken place.[16] The decision below, if permitted to stand, would

---

[15] In theory, the constitutionality of the FAA could be challenged by a criminal defendant notified by the government that evidence in the case derived from FISA surveillance. Plaintiffs explain why this limited opportunity for review is wholly insufficient to protect the rights of other Americans whose communications are acquired in the course of surveillance. *See* Pl.-Appellants' Br. at 52-54.

[16] It is difficult to estimate how many Americans have been "incidentally" surveilled under the FAA. The *New York Times* reported in June, quoting unnamed intelligence officials, that "[t]he NSA is believed to have gone beyond legal boundaries designed to protect Americans in about 8 to 10 separate court orders issued by the [FISC]. . . . Because each court order could single out hundreds or even thousands of phone numbers or e-mail addresses, the number of

thus render the constitutionality of the FAA – and indeed, the electronic surveillance activities of the executive branch – largely immune from judicial review. Such a result opens the door to the very same types of abuse and excess described in Part I, some of which we already are beginning to see, in the form of ongoing and (under the district court's decision) effectively unreviewable "overcollection" admitted by government officials.

Thirty-one years ago, in enacting FISA, Congress recognized that a lack of judicially enforceable standards for conducting electronic surveillance had led to widespread abuses that jeopardized Americans' First and Fourth Amendment rights. In enacting the FAA, which both loosens the standards that FISA imposed and decimates the role of the judiciary in overseeing compliance with those standards, Congress seems to have forgotten that lesson. And in dismissing plaintiffs' claims for lack of standing, the district court compounded Congress's error by insulating the FAA from meaningful judicial review. In so doing, it ceded the judicial branch's rightful place as the arbiter – and defender – of our fundamental constitutional rights.

---

individual communications that were improperly collected could number in the millions." *E-Mail Surveillance*, *supra*, at A1. These 8 to 10 court orders, of course, account only for the communications that the government itself characterizes as "improperly" collected. As noted above, *supra* n.11, the FISC approved 2,081 government requests for electronic surveillance and/or physical searches in 2008 alone.

CONCLUSION

This Court should reverse the decision below and remand the case for further proceedings.

Respectfully submitted,

BARBARA MOSES
MORVILLO, ABRAMOWITZ, GRAND,
IASON, ANELLO & BOHRER, P.C.

/s/ Barbara Moses

565 Fifth Avenue
New York, NY 10017
(212) 856-9600

EMILY BERMAN
ELIZABETH GOITEIN
THE BRENNAN CENTER FOR JUSTICE
161 Avenue of the Americas, 12th Floor
New York, NY 10013
(212) 998-6730

SHARON BRADFORD FRANKLIN
SENIOR COUNSEL
THE CONSTITUTION PROJECT
1200 18th Street, N.W.
Washington, DC 20036
(202) 580-6920

Date: December 23, 2009

Certificate of Compliance with Rule 32(a)

1. As required by Fed. R. App. P. 32(a)(7)(C), I certify that this brief is proportionally spaced and contains 6,123 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). I relied on my word processor, Microsoft Office Word 2003, to obtain this count.

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Microsoft Office Word 2003 in Times New Roman Style, 14 point font.

I certify that the foregoing information is true and correct to the best of my knowledge and belief.

Respectfully submitted,

/s/ Barbara Moses

Barbara Moses

Date: December 23, 2009

CERTIFICATE OF SERVICE

2009-4112-cv Amnesty International v. McConnell

I hereby certify that two copies of this Brief of Amici Curiae The Brennan Center for Justice, The Center for Democracy & Technology, The Constitution Project, The Electronic Frontier Foundation and the Rutherford Institute in Support of Plaintiffs-Appellants were sent by federal express next business day delivery to:

Jameel Jaffer
Melissa Goodman
American Civil Liberties
Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

Attorneys for Plaintiffs-Appellants

Douglas Letter
Civil Division, U.S. Dept. of Justice
950 Pennsylvania Avenue, N.W.,
Room 7513
Washington, D.C. 20530
(202) 514-2000

Attorneys for Defendant-Appellee

I also certify that the original and nine copies were also shipped via hand delivery to:

Clerk of Court
United States Court of Appeals, Second Circuit
United States Courthouse
500 Pearl Street, 3rd floor
New York, New York 10007
(212) 857-8576

on this 23rd day of December 2009.

Notary Public:

/s/ Jacqueline Gordon

Sworn to me this

December 23, 2009

JACQUELINE GORDON
Notary Public, State of New York
No. 01GO6149165
Qualified in Kings County
Commission Expires July 3, 2010

/s/ Raceel Pascall

RACEEL PASCALL
Record Press, Inc.
229 West 36th Street, 8th Floor
New York, New York 10018
(212) 619-4949

ANTI-VIRUS CERTIFICATION

Case Name: Amnesty International v. McConnell

Docket Number: 09-4112-cv

I, Raceel Pascall, hereby certify that the Amicus Brief submitted in PDF form as an e-mail attachment to **civilcases@ca2.uscourts.gov** in the above referenced case, was scanned using CA Software Anti-Virus Release 8.3.02 (with updated virus definition file as of 12/23/2009) and found to be VIRUS FREE.

/s/ Raceel Pascall
Raceel Pascall
Record Press, Inc.

Dated: December 23, 2009