No. 11-1025

In the

Supreme Court of the United States

JAMES R. CLAPPER, JR., DIRECTOR OF NATIONAL INTELLIGENCE, ET AL.,
Petitioners,
v.
AMNESTY INTERNATIONAL USA, ET AL.,
Respondents.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF OF FORMER CHURCH COMMITTEE MEMBERS AND STAFF AS *AMICI CURIAE* SUPPORTING RESPONDENTS AND AFFIRMANCE*

***See inside for list of amici**

EMILY BERMAN
Brooklyn Law School
250 Joraelmon Street
Brooklyn, NY 11201

JONATHAN HAFETZ
BARBARA MOSES
Seton Hall University School of Law
Center for Social Justice
833 McCarter Highway
Newark, NJ 07102
(973) 642-8700

SIDNEY S. ROSDEITCHER
Counsel of Record
THOMAS B. SULLIVAN
AUSTIN THOMPSON
Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019-6064
(212) 373-3000
srosdeitcher@paulweiss.com

September 24, 2012

LIST OF AMICI

Frederick D. Baron

Sen. Gary Hart (Ret.)

Dr. Loch K. Johnson

Hon. Paul Michel (Ret.)

Vice President Walter Mondale

Frederick A.O. Schwarz, Jr.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTORY MATERIALS

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

Amici were members or staff of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee" or "Committee"), formed in 1975 in response to decades of unethical and illegal conduct by United States intelligence agencies. The Church Committee's investigation led to the enactment of the Foreign Intelligence Surveillance Act, which contained a number of important safeguards against abuse of surveillance powers. *Amici* have an interest in ensuring that the lessons they learned during the Committee's investigation are not forgotten, including the need for judicial safeguards to protect American citizens and legal residents from violations of their First and Fourth Amendment rights.

Amicus Frederick D. Baron served as counsel on the Church Committee staff. As special assistant to the Attorney General of the United States (1977-79) with responsibility for foreign intelligence and counterintelligence matters, he was involved with drafting and legislative coordination of the Foreign Intelligence Surveillance Act of 1978. He later served as Associate Deputy Attorney General and

---

[1] This brief *amici curiae* is filed with the consent of all parties. Counsel for *Amici* affirm, pursuant to Supreme Court Rule 37.6, that no counsel for any party authored this brief in whole or in part, and that no party, counsel for any party, or any other person other than *Amici* and their counsel made a monetary contribution intended to fund the preparation or submission of this brief.

Director of the Executive Office for National Security of the Department of Justice (1995-1996); and as assistant United States attorney for the District of Columbia (1980-82).

Amicus Gary Hart, a United States Senator from Colorado from 1975 through 1987, was a member of the Church Committee. He served as a charter member of the Senate Intelligence Oversight Committee and was a member of the Senate Armed Services Committee. He was co-chair of the United States Commission on National Security for the 21st Century from 1998 through 2001 and currently serves as Chair of the Department of Defense's Threat Reduction Advisory Committee.

Amicus Loch K. Johnson served as the staff assistant or "designee" to Senator Church throughout the Church Committee inquiry. He subsequently served as staff director of the Oversight Subcommittee on the House Permanent Select Committee on Intelligence (1977-1980) and assistant to Chairman Les Aspin of the Aspin-Brown Commission of Intelligence (1995-1996). He is the author of a book about the Church Committee, entitled *A Season of Inquiry* (1987), and is currently senior editor of the international journal *Intelligence and National Security*. He is the Regents Professor of International Affairs at the University of Georgia.

Amicus Paul Michel was an assistant counsel on the Church Committee staff following service as a Watergate special prosecutor. Now retired, he was a judge and, from 2005 onward, Chief Judge, of the United States Court of Appeals for the Federal Circuit between 1988 and 2010, and by 2005

appointment of the Chief Justice, a member of the Executive Committee of the Judicial Conference of the United States, the governing body of the judiciary.

Amicus Walter Mondale, Vice President of the United States from 1977 through 1981 and a United States Senator from Minnesota from 1964 through 1976, was a member of the Church Committee and served as chairman of the subcommittee charged with drafting the Committee's final report on domestic intelligence activities. As Vice President, he was instrumental in facilitating the drafting and passage of the Foreign Intelligence Surveillance Act.

Amicus Frederick A.O. Schwarz, Jr. served as Chief Counsel to the Church Committee. After his work for the Committee, while back at his law firm, he worked as a part-time consultant for Vice President Mondale on issues such as the drafting of the Foreign Intelligence Surveillance Act. He is now Chief Counsel of the Brennan Center for Justice at New York University School of Law, 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. He is the co-author of *Unchecked and Unbalanced: Presidential Power in a Time of Terror*.

SUMMARY OF ARGUMENT

Amici submit this brief in support of Respondents and urge affirmance of the decision of the United States Court of Appeals for the Second Circuit, which found that Respondents have standing

to challenge the constitutionality of Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. § 1881a *et seq.*), ("FAA"). As the Court of Appeals found, Respondents have a reasonable fear that they will be electronically surveilled and have taken expensive steps, many of which are demanded by their ethical and professional responsibilities, to protect the privacy of their communications.

In this brief, *Amici* show that important constitutional questions would escape judicial review if the Court were to find that these Respondents lacked standing. Respondents challenge the FAA because it allows intelligence agencies to conduct surveillance without the judicial safeguards that Congress, based on the findings of the Church Committee, had considered essential to protect Americans from unlawful and unconstitutional executive abuses. Because the government treats as secret the identity of persons surveilled, if the Court determines that these Respondents do not have standing to bring this challenge, it is unlikely that any plaintiff in the future would have standing to bring such a challenge. As a result, the important constitutional questions raised by the FAA would escape judicial review entirely and the judiciary would be deprived of its role as a check against executive or legislative violations of constitutional rights.

Formed in 1975 in the wake of widespread abuses of authority by intelligence agencies, the Church Committee conducted an extensive

investigation of American surveillance operations. The Committee found that intelligence agencies, operating without sufficient oversight or monitoring, repeatedly ran roughshod over Americans' First and Fourth Amendment rights. From the 1930s through the 1970s, Democratic and Republican administrations alike wiretapped and bugged the homes and offices of American citizens without any judicial authorization. Moreover, surveillance purportedly motivated by national security concerns became politically driven.

The Church Committee concluded that without meaningful judicial review and monitoring of surveillance operations, surveillance can exceed constitutional and other legal restraints. In 1978, Congress agreed and enacted the Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-1811) ("FISA"), to, among other things, provide judicial safeguards to protect Americans against the abuses found by the Church Committee. In particular, FISA required *ex ante* judicial review of applications for particularized surveillance orders and authorized *ex post* judicial monitoring of the government's compliance with the limits imposed by statute and by judicial orders.[2]

---

[2] Because the FAA enables the government to completely circumvent FISA's pre-FAA requirements where the government claims to be targeting a non-U.S. person outside the United States, this brief generally uses the past tense in referring to FISA. Outside the area covered by the FAA, FISA's pre-FAA requirements continue to apply.

For almost thirty years, FISA empowered the Foreign Intelligence Surveillance Court ("FISC"), a special court created by the Act, to prevent intelligence agencies from violating the rights of American citizens or using surveillance for political purposes, while permitting those agencies to obtain information needed to protect the United States. However, in the wake of the September 11, 2001 terrorist attacks, FISA's critical safeguards were first disregarded and then, with the passage of the FAA in 2008, effectively abandoned.

While ostensibly leaving FISA's structure intact, the FAA enacted "additional" procedures to authorize surveillance of non-United States persons outside of the United States, including their communications with American citizens in the United States. These procedures enable the government to circumvent entirely the original FISA protections deemed essential to the protection of Americans' basic rights. Notably, some of the most serious abuses discovered by the Church Committee involved the warrantless surveillance of American citizens under the pretext of targeting foreigners.

FISA required particularized and detailed applications to the FISC identifying specific, individual targets and facilities to be surveilled and permitted surveillance only upon a finding of probable cause for the belief that the targets were foreign powers or their agents and that they were using the targeted facilities. Under the FAA's new procedures, however, these limits have been discarded, allowing the executive to bypass FISA's requirements and engage in wholesale, blanket

surveillance without identifying any individual targets or facilities or requiring any showing of probable cause. Judicial review consists only of confirmation that the executive's application contains certain certifications and a determination that the surveillance program's targeting procedures and minimization procedures—procedures to minimize unnecessary collection, retention, and dissemination of collateral communications of American citizens and legal permanent residents—meet statutory and Fourth Amendment requirements.

Further, where FISA empowered the FISC to monitor authorized surveillance operations and enforce the law when the government overstepped applicable limits, the FAA removes this monitoring role, giving courts no authority to stop even blatant overreaching. Instead, it leaves monitoring of compliance with the permitted scope of authorized surveillance operations and minimization procedures essentially to self-regulation by the executive branch, despite the findings of the Church Committee that such self-regulation proved inadequate to prevent abuse.

The judicial safeguards originally enacted by FISA are even more necessary today than they were in 1978, given the expansion of executive surveillance activities, the evolution in communications technology, and the pressures on the executive to conduct surveillance to prevent terrorist attacks. As this Court has recognized, it is in precisely such times that adequate judicial safeguards are most needed as a check against

unconstitutional and other unlawful executive conduct. Yet the FAA now immunizes surveillance of Americans' communications into and out of the United States from meaningful judicial review.

Respondents' claims in this lawsuit thus raise questions as to whether electronic surveillance conducted without the safeguards enacted in response to the Church Committee's findings violate the First and Fourth Amendments. Denying Respondents standing to raise these important questions would effectively insulate the FAA from judicial review. *Amici* submit that such a result would subvert the judiciary's role as "guardians" of the Bill of Rights and as an "impenetrable bulwark" against abuses of power by the other branches of the government. See 1 Annals of Cong. 439 (remarks of James Madison in presenting the Bill of Rights to Congress).

ARGUMENT

I. FISA'S JUDICIAL SAFEGUARDS REFLECTED THE CHURCH COMMITTEE'S FINDINGS THAT ADEQUATE JUDICIAL REVIEW OF INDIVIDUAL SURVEILLANCE ACTIVITIES IS ESSENTIAL TO PROTECT CIVIL LIBERTIES

Without judicial oversight and monitoring, even the best-intentioned members of the United States intelligence community are virtually certain to exceed the proper boundaries of surveillance operations. As this Court recognized forty years ago, those charged with conducting such operations

"should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *United States* v. *U.S. District Court* (*Keith*), 407 U.S. 297, 317 (1972).

Keith held that the Fourth Amendment requires the government to obtain a judicial warrant in advance of conducting electronic surveillance for domestic security purposes. *Id.* at 324. The case did not present, and the Court left open, the question whether such a requirement also applied to surveillance of a foreign power. *See id.* at 322 n.20.

In 1975, the Senate formed the Church Committee, among other things, to address that gap and to investigate allegations of surveillance abuses more generally. *See* Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755 (1976), at v ("Church Committee Book II"). The Committee found a host of government misdeeds and recommended a lengthy series of changes to better ensure that Americans' privacy, expressive, and associational rights were protected. Among these recommendations were provisions, later enacted as part of FISA, requiring judicial oversight of intelligence operations—both before specific individual surveillance activities were initiated and while they were ongoing—to make sure

those operations were conducted within proper limits.

The Committee adopted its findings and recommendations on a bipartisan basis. Despite the Democrats' large Senate majority, the Committee membership was almost evenly divided: six Democrats and five Republicans. Senator John Tower, the senior Republican, was designated the Committee's Vice Chair, and he presided over Committee meetings when the Chairman, Democratic Senator Frank Church, was absent.

There was bipartisan support for the Book II Report on "Intelligence Activities and the Rights of Americans," which focused on non-military intelligence abuses and their impact on American citizens' rights. Three members, however—Senators Tower, Baker and Goldwater—issued separate statements disagreeing with various aspects of the report. But Senators Tower and Baker agreed with the extensive findings of intelligence abuses documented in the report and both agreed with the requirement for an advance judicial warrant for electronic surveillance. Senator Tower specifically emphasized support for "issuance of a judicial warrant as a condition precedent to electronic surveillance," a measure which "enjoys bi-partisan support in Congress." Senator Tower, Church Committee Book II at 371. Similarly, Senator Baker also expressed his "wholehearted[] support" for a bill requiring a warrant, noting "[t]he abuses of electronic surveillance of the past clearly dictate a need for a system of judicial warrant approval" and that the proposed new system "needs consolidated bi-

partisan support because it represents a significant advance from existing practice." *Id.* at 384.

A bipartisan spirit also characterized FISA's enactment. In the final debate over FISA in the Senate, for example, Senator Jake Garn, the Republican manager of the bill and Vice Chair of the Intelligence Committee, explained:

> [FISA's] sponsorship represents a unique bipartisan collaboration in the interests of national security. . . . This is not a liberal bill. It is not a conservative bill. It is neither a Democratic nor a Republican bill. The tasks of balancing cherished constitutional liberties with the increasingly threatened national security needs is too important to be left to partisanship." 124 Cong. Rec. 10888-89 (1978).

FISA was enacted by the Senate by a vote of 95-1 and in the House by a vote of 226-176. This was a resounding endorsement of the provisions for judicial oversight that were a centerpiece of FISA.

Such judicial oversight has been abandoned by the FAA.

A. Before the Passage of FISA, United States Intelligence Agencies Routinely Engaged in Surveillance That Violated the Rights of American Citizens

The Church Committee investigated the

activities of various United States agencies, including the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, the Department of Defense, and the National Security Council, from 1936 through 1976. Church Committee Book II at v-vii, 21. Looking back as far as the administration of Franklin Roosevelt, the Committee found that "intelligence excesses, at home and abroad have been found in every administration." *Id*. at viii. Many presidential administrations collaborated with intelligence agencies to break the law and overextend intelligence operations. *See id.* at v, viii.

The Committee found a pattern of intelligence investigations with vague or imprecisely defined mandates, providing intelligence officials enormous discretion with which to choose their surveillance targets. This broad discretion enabled surveillance of individuals and organizations that presented little or no threat to national security. Often, the targets of wiretapping were chosen based solely on domestic political considerations.

In one of the most notorious examples, the FBI targeted Dr. Martin Luther King, Jr., in an effort to "neutralize" him as a civil rights leader. *Id.* at 11 (internal quotation marks omitted). The FBI used "nearly every intelligence 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 in an effort to destroy Dr. King's marriage. *Id.* In another example, the FBI claimed to justify collecting extensive data on the nonviolent Southern Christian Leadership Conference and its members by labeling the organization a Black Nationalist "Hate Group." *Id.* at 213.

Between 1960 and 1972, the FBI, without seeking judicial approval and based on little or no individualized grounds of suspicion, subjected nearly thirty American citizens to electronic surveillance of their communications in an effort to determine the sources of leaks of classified information. Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans (Book III), S. Rep. No. 94-755 (1976), at 321, 327 ("Church Committee Book III"). The choice of surveillance targets was predicated on attenuated suspicion or mere speculation: for instance, one subject was chosen because of his frequent contact with the White House and National Security Council and his attendance at the same church as a journalist who had written a story revealing information about the President's communications. *Id.* at 326. At least seven of the targets were journalists. *Id.* at 327. Not only were no warrants sought, but at least ten of the wiretaps were initiated without the prior written approval of the Attorney General, in violation of then-current agency policy. *Id.* While the wiretaps allowed the FBI to compile a significant amount of personal and political information about the targets, nothing in the Bureau's records indicated "that the wiretaps succeeded in identifying a single person who had leaked national security information." *Id.* at 327.

Information on Americans that was collected in these programs was often wholly irrelevant to the stated purpose of the surveillance order, but it was nonetheless recorded and then disseminated to senior administration officials. This had disturbing implications for separation of powers principles. *See* Church Committee Book II at 161-3. For example, as part of an investigation into "possibly unlawful attempts of representatives of a foreign country to influence congressional sugar quota legislation," a bug was planted in the hotel room of the chairman of the House Agriculture Committee. *Id.* at 200. The Church Committee found that while the "investigation was apparently initiated because of the Government's concern about future relations with the foreign country involved and the possibility of bribery, it [was] clear that the Kennedy Administration was politically interested in the outcome of the sugar quota legislation as well" and obtained "a great deal of potentially useful political information" from this and other surveillance. *Id.* at 200-01.

B. Before the Passage of FISA, Intelligence Agencies Engaged in Warrantless Surveillance of American Citizens under the Pretext of Targeting Foreigners

The Church Committee also found that intelligence agencies expanded international surveillance programs into the domestic sphere, and as a result they often collected information on American citizens and activist groups while describing their surveillance as "foreign." *See*

Church Committee Book II at 104-05.

Of particular relevance here, the Committee determined that in some instances electronic surveillance of foreigners actually had the "primary purpose of intercepting the communications of a particular American citizen with that target" as a way of circumventing "the generally more stringent requirements for surveillances of Americans." Church Committee Book III at 312-13. In at least one instance, the FBI "instituted an electronic surveillance of a foreign target for the *express* purpose of intercepting telephone conversations of an American citizen." Church Committee Book II at 120 (emphasis added).

NSA surveillance programs purportedly designed to target foreigners also swept up "countless" pieces of correspondence "between Americans in the United States and American or foreign parties abroad." *Id*. at 169. Indeed, the NSA defined foreign communications as any communication "where one terminal is outside the United States," opening the door to surveillance of terminals at the other end of the communication in the United States used by American citizens. *Id*. at 104. As a result, "for many years," the NSA intercepted the communications of American citizens without a warrant or any form of judicial review. *Id*.

For example, Operation SHAMROCK, an NSA program initially intended to review the telegrams of foreign targets, expanded to become the "largest governmental interception program affecting Americans." Church Committee Book III at 740. All of the major telegraph companies agreed to allow the

NSA access to all of their incoming and outgoing international telegrams, "including millions of the private communications of Americans." Church Committee Book II at 104. The CIA initiated similar programs to intercept cables and mail entering the United States. *Id.* at 58. In addition, because the CIA could use wiretaps and bugs to listen to *all* communications of their targets, American citizens with whom the foreign targets spoke were also overheard by intelligence agents. Church Committee Book III at 312.

Americans' fundamental rights were further compromised when the CIA and NSA shared information on American citizens that they had collected in their investigations of "foreign" targets with the FBI. *See* Church Committee Book II at 59. For example, in the 1950s, the CIA began supplying the FBI with information it had collected about American citizens, particularly letters "professing 'pro-Communist sympathies'" and information about U.S. peace groups going to Russia. *Id.* at 59. Government officials outside the intelligence community also made requests—which the NSA honored—for specific people, including American citizens, to be targeted for surveillance. *Id.* at 161-62. In one instance, in response to "the specific request of the Bureau of Narcotics and Dangerous Drugs," the NSA monitored thousands of telephone conversations on a telecommunications pipeline between New York City and South America. *Id.* at 162.

C. The Church Committee Found That a Lack of Judicial and Congressional Oversight Allowed These Abuses to Occur

The Church Committee concluded that this unethical and illegal conduct had occurred—and continued for decades—because intelligence agencies lacked "appropriate restraints, controls, and prohibitions on intelligence collection." Church Committee Book II at 171. As a result, "distinctions between legitimate targets of investigations and innocent citizens were forgotten" and "the Government's actions were never examined for their effects on the constitutional rights of Americans." *Id.*

The Committee identified three characteristics of United States intelligence that, unchecked, had led to violations of the rights of American citizens: (1) excessive concentration of power in the executive, which "contained the seeds of abuse"; (2) excessive secrecy that shielded "constitutional, legal and moral problems from the scrutiny of all three branches of government [and] from the American people themselves"; and (3) a general sense of lawlessness that pervaded the intelligence field, causing government officials to use national-security rationalizations as a pretext to evade statutory and constitutional limits on non-security related surveillance. *Id.* at 292. The result was a "vacuum cleaner" approach to intelligence gathering that included massive overreaches and clear violations of both statutory law and the Bill of Rights. *Id.* at 165.

In response to the violations unearthed in their investigation—and to address the underlying

causes of those violations—the Church Committee called for strong, permanent statutory restraints and oversight from "all branches of Government." *Id.* at 289. Such restraints, the Committee reasoned, were necessary to prevent intelligence agencies from repeating past wrongdoing. *Id.* The Committee concluded that absent "new and tighter controls" designed to reduce the discretion of intelligence agencies, intelligence practices "threaten[ed] to undermine our democratic society and fundamentally alter its nature." *Id.* at 1.

Moreover, the Committee predicted that as the Government's technological capabilities "relentlessly increase[d]," the potential for abuse would grow. *Id* at 289. Therefore, it urged Congress to fashion restraints that could not only cure past problems but also "anticipate and prevent the future misuse of technology." *Id.* These measures, it concluded, would prove particularly necessary in periods of heightened threats to national security. *Id.* The Committee warned that "in time of crisis, the Government will exercise its power . . . to the fullest extent." *Id.* The resulting "crescendo of improper intelligence activity" could be prevented only by cabining executive power before such a time of crisis. *See id.*

II. CONGRESS ENACTED FISA'S JUDICIAL SAFEGUARDS AS ESSENTIAL PROTECTIONS AGAINST THE SURVEILLANCE ABUSES FOUND BY THE CHURCH COMMITTEE TO INFRINGE THE CONSTITUTIONAL RIGHTS OF AMERICAN CITIZENS

The Church Committee determined that active oversight from the judicial branch was the appropriate means to guard against inappropriate surveillance of innocent citizens. Church Committee Book II at 309. Thus, it concluded, "there should be no electronic surveillance within the United States which is not subject to a judicial warrant procedure." *Id.* at 325. The Committee, therefore, recommended requiring intelligence agencies to obtain judicial approval to monitor communications to, from, or about Americans. *See, e.g.*, *id.* at 308-309.

These recommendations were enacted into law as part of FISA. Reflecting the congressional consensus that electronic surveillance undertaken to collect intelligence for foreign intelligence purposes should require judicial approval, FISA set forth a comprehensive procedure through which, with limited exceptions, officials had to obtain a court order before engaging in any surveillance of communications to or from Americans located in the United States. 50 U.S.C. § 1804. As Senator Birch Bayh explained during the Senate floor debate on FISA, the Act was intended to "bring an end to the practice of electronic surveillance by the executive branch without a court order in the United States. It establishes standards for issuing court orders that

reconcile the interests of personal privacy and national security in a way that is fully consistent with the fundamental principles of the fourth amendment and due process of law." 124 Cong. Rec. 10889-90; *see also Foreign Intelligence Surveillance Act: Hearing on H.R. 7308 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 94th Cong. 28, 29 (1976) (explanation of former Deputy Solicitor General Philip Lacovara that FISA's requirement of judicial involvement was necessary both because "the courts, from the earliest time, have been regarded as the bulwarks of liberty against executive excesses," and because executive branch officials would exercise greater self-restraint when forced "to think through the decision that they're making and to put it down on paper and to have to justify it to someone else").

One of the most significant components of FISA's scheme was the creation of the FISC, a special court that served as a check on executive surveillance activities. The government had to apply to the FISC for permission to conduct foreign intelligence surveillance in the United States, including surveillance of communications with American citizens into and out of the United States. 50 U.S.C. §§ 1803, 1804.

Under FISA's procedures, a federal officer seeking authorization to conduct electronic surveillance was required to make a detailed application in writing under oath to a judge of the FISC seeking permission to surveil a specific target. The target of the surveillance must have been either a foreign power or an agent of a foreign power, and

the application was required to identify the specific facilities or places used or about to be used by the foreign power or agent to which surveillance would be directed. *Id.* § 1804(a)(3).

Each application was required to include, *inter alia*, a detailed statement of the facts and circumstances providing: (1) the identity or a description of the specific target of the surveillance and the facilities to be surveilled; (2) the justification for the belief that the target was a foreign power or a foreign power's agent and that the power or agent was using or about to use the targeted facilities or places; (3) proposed minimization procedures; (4) the nature of the information sought and the type of communications or activities to be surveilled; (5) the means to effect surveillance, including whether physical entry was required; (6) the facts of all previous applications; and (7) the period of time for which the surveillance would be maintained. *Id.* § 1804(a)(1)-(9).

In reviewing an application, the FISC judge was required to make an independent determination regarding its sufficiency on a number of grounds. The judge was required to assess whether there was *probable cause* to believe that both the target of the electronic surveillance was a foreign power or its agent and that they were using or about to use each of the facilities or places at which the surveillance was directed. *Id.* § 1805(a). In making the probable cause determination, the judge was to look to "past activities of the target, as well as facts and circumstances relating to current or future activities of the target." *Id.* § 1805(b). If the judge found that

there was not probable cause, she could not authorize the requested surveillance. *Id.* § 1805(a).

The Act also required the judge to evaluate the application's plan for minimization procedures to limit the agency from collecting and retaining collateral information collected on Americans. *Id.* at § 1804(a)(4); S. Rep No. 95-604, at 37-38*, reprinted in* 1978 U.S.C.C.A.N. 3904, 3939.

Not only were FISC judges required to make these independent *ex ante* determinations, but FISA also empowered the judge who authorized the surveillance to "assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated," at or before the end of the period during which surveillance was authorized. 50 U.S.C. § 1805(d)(3).

FISC judges also specified in their orders the permissible duration of the surveillance which, with certain limited exceptions, could be extended only if the government first submitted to the FISC for review and approval a new application containing all of the above details. *Id.* §§ 1805(d)(1), (d)(2).

III. THE FAA RAISES IMPORTANT CONSTITUTIONAL QUESTIONS BECAUSE IT AUTHORIZES MASS SURVEILLANCE THAT INCLUDES COMMUNICATIONS OF AMERICANS LOCATED IN THE UNITED STATES WITHOUT ANY OF FISA'S JUDICIAL SAFEGUARDS

FISA remained the law of the land, with updates, for almost 30 years. However, in the wake of the September 11, 2001 terrorist attacks, the President secretly authorized the NSA to conduct surveillance of communications between Americans and foreign parties without FISC authorization, under the President's claimed wartime powers. *See* Offices of the Inspectors Gen. of the Dep't of Def., Dep't of Justice, Central Intelligence Agency, Nat'l Sec. Agency, & Office of the Dir. of Nat'l Intelligence, *Unclassified Report on the President's Surveillance Program* 1, 11-12, 36 (2009) ("PSP Report"); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1. This surveillance, known as the Terrorist Surveillance Program ("TSP"), was only one part of the still-secret President's Surveillance Program. The TSP itself remained secret until revealed in the press in 2005. *See* PSP Report, *supra*, at 1.

After first disregarding the law, the executive branch then sought to alter it. The Bush Administration worked with Congress to amend FISA three times before the FAA was enacted in 2008. The FAA, while leaving much of FISA intact, creates "Additional Procedures" for authorization of

foreign intelligence surveillance targeting non-United States persons located outside the United States.

These procedures enable the government to circumvent FISA's judicial safeguards, despite the Church Committee's finding that the claim that surveillance was intended to target foreigners was frequently a pretext for unlawful invasions of the privacy of American citizens. *See* pp. 14-16, *supra*.

The FAA abandons FISA's requirement that an individualized order issue after meaningful judicial review of the basis for the government's request. And it circumvents the FISC's power to engage in continued oversight of ongoing surveillance. Instead, the FAA permits the executive branch to initiate a generalized, mass surveillance program for up to one year, encompassing any communications entering or leaving the United States in which one or more unspecified targets are believed to be non-United States persons located outside the United States. In place of the detailed judicial review of the claimed justifications of individual surveillance activities, the FAA limits the FISC to a review that is perfunctory. The FISC does little more than ensure that the government's application recites the required statutory certifications and is designed to meet statutory and constitutional requirements for targeting and minimization procedures. Monitoring of the actual implementation of the minimization procedures is left to the executive branch. 50 U.S.C. § 1881a(a).

Thus, by authorizing mass surveillance and eliminating FISA's judicial safeguards, the FAA

immunizes individual, specific surveillance activities from judicial review.

A. The FAA Allows Mass Surveillance Without Requiring the Detailed, Individualized Showing Considered Necessary to Curb the Abuses of Executive Discretion Found By the Church Committee

One component of reform that the Church Committee advocated was to limit significantly the discretion of intelligence agencies. *See* p. 18, *supra*. Absent such limitations, the Committee concluded, the government came to disregard "distinctions between legitimate targets of investigations and innocent citizens," and the resulting surveillance "threaten[ed] to undermine our democratic society and fundamentally alter its nature." *See id*. One way in which this excessive discretion was addressed was by requiring the government to make specific, individualized, and detailed showings to the FISC before it could obtain a surveillance order. *See* pp. 20-22, *supra*.

As the Second Circuit recognized, however, the FAA replaces FISA's individualized surveillance authorization procedures with a "mass surveillance authorization," *Amnesty Int'l USA* v. *Clapper*, 638 F.3d 118, 124 (2d Cir. 2011), returning to the pre-Church Committee days of relatively unconstrained executive discretion and its concomitant risks to fundamental constitutional rights.

Under its new procedures, the FAA authorizes the Attorney General and the Director of National

Intelligence to apply for an order authorizing them to conduct surveillance "targeting" unspecified foreign persons located outside the United States for a period of up to one year.

In contrast to FISA, the application need not identify or describe the persons or facilities to be surveilled. *Compare* 50 U.S.C. § 1805(c)(1) *with id.* §§ 1881a(d)(1), (g)(4). Nor is the government required to make the showing required by FISA that the target is a foreign power or agent of a foreign power; instead, it must merely certify that "a significant purpose of the acquisition is to obtain foreign intelligence material" and that information will be obtained "from or with the assistance of an electronic communication service provider." *Id.* §§ 1881a(g)(4), (g)(2)(A)(v); *see also id.* § 1801(e)(2).

An FAA application also must comply with a handful of additional requirements. It must attest that adequate targeting and minimization procedures have been approved by the FISC, have been submitted to the FISC, or are being submitted to the FISC with the certification. *Id.* § 1881a(g)(2). It must affirm that the surveillance will not: (1) intentionally target any person known at the time of acquisition to be located in the United States; (2) target a person outside of the United States if the purpose is actually to target a particular, known person reasonably believed to be in the United States; (3) target a United States person known to be outside of the United States; or (4) intentionally acquire any communications whose sender and all intended recipients are known at the time of acquisition to be in the United States. The

certifications, however, do not prohibit surveillance of communications between the foreign targets and United States persons located in the United States.

The application also must state that the surveillance shall be conducted in a manner consistent with the Fourth Amendment of the United States. *Id.* §§ 1881a(b), (g)(2).

None of the FAA's requirements, however, adequately substitutes for the detailed information that was required by FISA and that allowed the FISC to ensure that there was probable cause for government surveillance aimed at individualized, specified targets and facilities.

B. The FAA Does Not Give the FISC Jurisdiction to Review in Advance Specific, Individual Surveillance Activities Involving Communications with American Citizens

In *Keith*, this Court wrote that "[p]rior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." 407 U.S. at 318 (citation omitted). The Church Committee agreed, recognizing that requiring government officials to go before a judge and seek approval was the surest way to guard against abuses. *See* Church Committee Book II at 325. This principle was adopted into law in FISA. *See* 124 Cong. Rec. 10887 ("It is the courts, not the executive, that would ultimately rule on whether the surveillance should occur." (Statement of Sen. Kennedy)). Unlike FISA, the FAA does not require

the government to establish or the FISC to determine that probable cause exists in advance of specific, individualized surveillance of identified targets and facilities. The FAA provides jurisdiction only for an abstract, *a priori* examination of a plan to monitor unknown persons using unknown surveillance facilities.

Under the FAA, the FISC is only granted jurisdiction to (1) determine whether the certification submitted has all the required elements; (2) determine whether the targeting procedures are reasonably designed to ensure that the acquisition is limited to targeting persons reasonably believed to be located outside of the United States and 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; and (3) ensure that the targeting and minimization procedures meet the statutory requirements and Fourth Amendment. 50 U.S.C. § 1881a(i)(2); s*ee id.* § 1881a(i)(3)(A) (stating that the court "shall enter an order approving the certification" if the certification contains the information required by the statute).

Moreover, if the FISC judge finds that the government's certification has failed to include all of the required elements, the government has 30 days to correct any deficiency, *id.* § 1881a(i)(3)(B), and may continue to acquire information during any appeal of a denial of its application, *id.* § 1881(i)(4)(B). Thus, a mass surveillance operation found by the FISC to violate the Fourth Amendment can continue—regardless of the severity of the

violation—until that finding is affirmed by the FISA Court of Review.

C. The FAA Substitutes Executive Self-Regulation for FISA's Authorization of Ongoing Review by the FISC of Compliance With Minimization Procedures

In his letter transmitting the second volume of the Church Committee's findings, Senator Church stated that the Committee's recommendations were "designed to place intelligence activities within the constitutional scheme for controlling government power." Church Committee Book II at iii. FISA's probable cause review by the FISC, discussed above, provided one such check by the judiciary. Another check is meaningful post-authorization monitoring.

The FAA bypasses FISA's provisions empowering FISC to monitor compliance with minimization procedures. Instead, the FAA relies on two self-assessments. First, the Attorney General and Director of National Intelligence are required to conduct a semi-annual review to assess compliance with targeting and minimization procedures and the limitations on targeting of United States persons. *Id.* § 1881a(l)(1). Second, the heads of each intelligence agency conducting an acquisition under the FAA are required to make an annual review "to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition," including, among other things, an accounting of disseminated intelligence reports containing a reference to United States persons, the number of targets later

determined to be located in the United States, and a description of procedures developed to assess the extent to which the acquisitions acquire the communications of United States persons. *Id.* § 1881a(l)(3). While these assessments are submitted to the judges of the FISC and to both houses of Congress's intelligence and judiciary committees, it is far from clear what utility they serve.

As the Second Circuit pointed out in its decision below, though the government claims that FISC judges may disapprove of minimization procedures in the future if they are shown to be ineffective, "the government has not asserted, and the statute does not clearly state, that the FISC may rely on these assessments to revoke earlier surveillance authorizations." *Amnesty Int'l*, 638 F.3d at 125. Moreover, there are no provisions in the FAA that permit the FISC to make its own, independent assessment of whether there has been compliance with the minimization procedures. The reports are also insufficient to allow Congress to monitor or guard against overreaching. In a letter sent to the Director of National Intelligence on July 26, 2012, thirteen senators, including members of both the Intelligence and Judiciary committees, wrote that they were "concerned that Congress and the public do not currently have a full understanding of the impact that [the FAA] has had on the privacy of law-abiding Americans," noting that the intelligence community had been unable "to identify the number of people located inside the United States whose communications may have been reviewed" under the FAA. *See* Letter from Ron Wyden, U.S. Senator, et

al., to James R. Clapper, Jr., Dir. of Nat'l Intelligence (July 26, 2012) at 1, *available at* http://www.wyden.senate.gov/download/letter-to-dni.

Thus, the FAA essentially leaves to the executive the monitoring of its own compliance with minimization procedures. This disregards the Church Committee's findings that such self-regulation was inadequate to prevent abuse. *See* pp. 17-18, *supra*.

* * *

In sum, the FAA disregards entirely the approach taken by Congress in enacting FISA based on lessons learned from the Church Committee. It immunizes from judicial scrutiny actual, specific, individual executive surveillance activities that involve communications with American citizens.

IV. FISA'S JUDICIAL SAFEGUARDS ARE NEEDED NOW MORE THAN EVER TO PROTECT AMERICAN CITIZENS FROM THE KINDS OF UNCONSTITUTIONAL ABUSES FOUND BY THE CHURCH COMMITTEE

The Church Committee recognized that the pressure of foreign or domestic crises can lead to systematic intelligence agency excesses, including "lawless and improper behavior, intervention in the democratic process, [and] overbroad intelligence targeting and collection," if procedures for reporting and review are not established and lines of authority are not clearly drawn. *See* Church Committee Book II at 266; *see* p. 18, *supra*. In the absence of effective

judicial oversight, intelligence agencies have, since the 9/11 crisis, repeatedly infringed the rights of American citizens.

For example, as part of the Bush Administration's Terrorism Surveillance Program, which purportedly was aimed solely at international communications, the NSA nonetheless engaged in warrantless surveillance of purely domestic communications, as a result of what the agency described as "technical glitches." James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. Times, Dec. 20, 2005, at A1.

In 2009, after the passage of the FAA, the press reported that the NSA carried out "significant and systematic" overcollection of domestic communications, due in part to difficulties in distinguishing between intra-American communications and those taking place at least partly overseas. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, April 15, 2009, at A1. The press later reported that the NSA may have gone beyond legal boundaries established by eight to ten separate court orders, meaning that millions of individual communications could have been improperly collected. James Risen & Eric Lichtblau, *Extent of E-mail Surveillance Renews Concerns in Congress*, N.Y. Times, June 17, 2009, at A1.

Some of these incidents seem to be the result of changing technology, illustrating that such changes heighten—not weaken—the importance of providing checks on the government's ability to mass-monitor communications. The Church

Committee recognized that as the government's technological capacity to conduct surveillance increases, so does the potential for abuse. *See* p. 18, *supra*. In the time since the Church Committee made its findings, technology has made surveillance easier while complicating enormously the task of determining which communications can be legally and constitutionally monitored: now, for instance, "a single communication can transit the world even if the two people communicating are only located a few miles apart." *Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intelligence*, 110th Cong., 1st Sess., at 19 (May 1, 2007) (statement of Adm. J. Michael McConnell, Director of Nat'l Intelligence). The potential for error created by this increased technological complexity is compounded by the increasing importance of telecommunications in daily life, as, "[w]ith the explosion of new technologies, including social networking sites, smartphones and other mobile applications. . . . there are . . . many new risks to . . . privacy." *See* 157 Cong. Rec. S3054 (daily ed. May 17, 2011) (statement of Sen. Leahy). Mistakes—and abuses—in electronic surveillance are thus easier and potentially more costly than ever.

This overcollection has likely also resulted, in part, from the enormous pressures that the threat of global terrorism has put on the executive branch. Determined to combat this threat at all costs, both elected and appointed officials can all too easily tolerate abuses of core constitutional rights, including the unjustified surveillance of innocent American citizens and residents. This renders the

need for meaningful judicial safeguards even more urgent, a point the Church Committee explicitly made. *See* p. 18, *supra*. As Justice Kennedy observed: "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*, 553 U.S. 723, 798 (2008); *see also Hamdi* v. *Rumsfeld*, 542 U.S. 507, 532 (2004) (plurality opinion) ("It is during our most challenging and uncertain moments that our Nation's commitment to due process is most severely tested; and it is in those times that we must preserve our commitment at home to the principles for which we fight abroad.").

While the above-described incidents are uniformly troubling, the full extent of FAA surveillance is impossible to determine, given the government's refusal to release—or even allow to be litigated—details of its surveillance activities. *See*, *e.g.*, *ACLU* v. *NSA*, 493 F.3d 644, 653 (6th Cir. 2007) (holding that "plaintiffs do not—and because of the State Secrets Doctrine cannot—produce any evidence" regarding the NSA's conduct of warrantless surveillance under the TSP). And absent any provision for meaningful independent oversight of those activities, the intelligence community will have limited incentives to prevent recurrence of its overcollection errors.

V. IF THESE RESPONDENTS ARE DENIED STANDING, IMPORTANT QUESTIONS CONCERNING THE CONSTITUTIONALITY OF THE FAA'S MASS SURVEILLANCE AUTHORITY ARE LIKELY TO ESCAPE JUDICIAL REVIEW ENTIRELY AND THE COURT'S ROLE IN THE CONSTITUTION'S SYSTEM OF CHECKS AND BALANCES WILL BE UNDERMINED

The central question underlying this case is whether the FAA—which abandons long-standing safeguards and allows wholesale surveillance programs without any judicial oversight of individual, actual surveillance activities—is consistent with the First and Fourth Amendments. The Church Committee recognized that to be consistent with the "fundamental principles of American constitutional government," the government's power to conduct intelligence activities "must be checked and balanced." Church Committee Book II at v. "[T]he preservation of liberty requires the restraint of laws, and not simply the good intentions of men." *Id.*

If these Respondents lack standing, notwithstanding that the nature of their professional responsibilities makes their communications with foreign persons outside the United States particularly likely subjects of surveillance, it is

unlikely that any other plaintiff will have standing.[3] As a result, the FAA procedures that immunize surveillance of such communications from judicial scrutiny will themselves be immunized from judicial review of their constitutionality. The preservation of liberty will be entirely reliant on the good intentions of members of the intelligence community. *See also* Respondents' Brief at 57-58.

Accordingly, while *Amici* recognize that the merits of the constitutional issues raised by Respondents are not before the Court, *Amici* submit that the resolution of the standing question has significant consequences for our constitutional system of separation of powers and checks and balances. Reversing the circuit court's judgment would make it unlikely that these substantial constitutional questions will ever be subject to judicial review. This result would undermine our system of separation of powers by ousting the judiciary from its traditional, constitutionally assigned role as a check on constitutional violations

---

[3] While a criminal defendant would be able to challenge the constitutionality of the FAA if the government attempted to introduce FAA-derived evidence at trial, as far as we can determine, the government has not done so in the four years that the FAA has been in effect. Moreover, to rely on the possibility that the government might do so in the future, would, in effect, mean that whether or when there would be judicial review of the FAA's constitutionality would be dependent on executive discretion. Meanwhile, many Americans might continue to be subjected to surveillance that may be unconstitutional. *Amici* submit that this is inconsistent with the Constitution's system of checks and balances.

by the other branches.

CONCLUSION

For the foregoing reasons, the judgment below should be affirmed.

Respectfully submitted,

EMILY BERMAN
Brooklyn Law School
250 Joraelmon Street
Brooklyn, NY 11201

JONATHAN HAFETZ
BARBARA MOSES
Seton Hall University
School of Law
Center for Social
Justice
833 McCarter Highway
Newark, NJ 07102
(973) 642-8700

SIDNEY S. ROSDEITCHER
Counsel of Record
THOMAS B. SULLIVAN
AUSTIN THOMPSON
Paul, Weiss, Rifkind, Wharton &
Garrison LLP
1285 Avenue of the Americas
New York, NY 10019-6064
(212) 373-3000
srosdeitcher@paulweiss.com

Counsel for Amici Curiae

September 24, 2012