THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

REPORT ON THE FISA AMENDMENTS ACT OF 2008

THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE

September 6, 2012

The Constitution Project
1200 18th Street NW
Suite 1000
Washington, DC 20036
202.580.6920 (tel)
202.580.6929 (fax)
info@constitutionproject.org

www.constitutionproject.org

REPORT ON THE FISA AMENDMENTS ACT OF 2008

In an increasingly interconnected modern world, Americans constantly communicate with friends, relatives, colleagues, and business partners overseas by electronic means. Unfortunately, some people also use these international networks for more nefarious purposes, such as to coordinate espionage and plan acts of terror. To collect information vital to national security, the U.S. government legitimately seeks to monitor the electronic communications of those intending to harm the United States. It is critical that any such surveillance program be designed to incorporate strong privacy safeguards to avoid intrusions on Fourth Amendment rights.

The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 to provide a lawful procedure for such monitoring. Under FISA, the Attorney General can request that the Foreign Intelligence Surveillance Court (FISC) issue a sealed order permitting the government to engage in electronic surveillance of a target for the purpose of collecting foreign intelligence information. FISA was designed to accommodate traditional Fourth Amendment standards by limiting such surveillance to investigations of foreign powers and their agents. To obtain a FISA warrant, it is necessary only to show probable cause that a target is an agent of a foreign power—not that a crime has been or is being committed.

FISA has been amended several times since its enactment in 1978. This report focuses on the most significant set of amendments: the FISA Amendments Act of 2008 (FAA). The FAA was enacted following the public disclosure of the National Security Agency's (NSA) warrantless wiretapping programs in December 2005.[1] The Constitution Project's Liberty and Security Committee released several statements expressing our deep concerns with those programs, and concluding that "at least until issuance of the FISA Court orders announced in January 2007, the NSA domestic surveillance program has been operated in violation of FISA."[2] Ultimately, the Administration sought congressional approval for an expanded program of warrantless surveillance of international communications.[3]

The FAA vastly increased the government's powers to conduct surveillance of international communications without individualized judicial review and severely limited the scope of review performed by the FISC when the court's approval is actually required. Under the FAA, the Attorney General and the Director of National Intelligence may jointly authorize a surveillance program intended to gather foreign intelligence information by targeting the international communications of foreign persons located abroad, including those communications to which U.S. persons[4] may be a party. The FAA does not require the government to identify particular targets or give the FISC a rationale for individual targeting

[1] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

[2] The Constitution Project's Liberty and Security Committee, *Statement on the National Security Agency's Domestic Surveillance Program* (2007), http://www.constitutionproject.org/pdf/51.pdf.

[3] The revisions of the FAA were in large part taken from the Protect America Act, Pub. L. 110-55, which expired in 2007. For an analysis of constitutional defects in the Protect America Act, *see* The Constitution Project's Liberty and Security Committee, *Statement on the Protect America Act* (2007), http://www.constitutionproject.org/pdf/Statement%20on%20PAA1.pdf.

[4] The term "U.S. person" refers to both U.S. citizens and legal residents.

decisions. The government need only provide the FISC and Congress with a description of the "targeting" and "minimization" procedures it will employ to reduce the number of U.S. persons whose communications are intercepted and minimize the amount of data which is stored unnecessarily. The Act, which expires on December 31, 2012, is currently pending reauthorization in Congress.

After almost four years of the expanded, programmatic surveillance the FAA allows, almost nothing is publicly known about how the Act has been implemented or about the scope of the surveillance that is being conducted under the Act. What is known, however, raises serious questions about the Act's impact on privacy rights. In fact, in a letter dated July 20, 2012, an official with the Office of the Director of National Intelligence advised Senator Ron Wyden that on at least one occasion, the FISC ruled that "some collection" conducted under the FAA "was unreasonable under the Fourth Amendment."[5]

The undersigned members of The Constitution Project's Liberty and Security Committee believe that the FAA raises significant Fourth Amendment concerns;[6] that the public has not been adequately informed concerning these authorities; and that Congress should address both of these problems before reauthorizing the statute. Especially in the digital age, national security programs must incorporate robust safeguards for constitutional rights and civil liberties. Our concerns, and our recommendations for amendment of the FAA and for future actions by Congress and the Executive Branch, are spelled out and explained below.

I. Foreign Intelligence Surveillance Raises Unique Fourth Amendment Challenges in the Digital Age

The Fourth Amendment requires in most cases that the government obtain a warrant before conducting searches and seizures, and always requires that searches and seizures be conducted in a reasonable manner. Especially in a world where technology provides government the ability to intercept private communications *en masse*, the government's powers of electronic surveillance should be subject to strict limitations and vigilant oversight. As the Supreme Court

---

[5] *See* Ellen Nakashima, *Privacy Rights Violated At Least Once By U.S. Intelligence-Collection Initiative, Official Says*, WASH. POST, July 20, 2012, http://www.washingtonpost.com/world/national-security/us-intelligence-collection-initiative-violated-rights-at-least-once-government-says/2012/07/20/gJQAtJjFzW_story.html; Letter from Kathleen Turner, Office of the Director of National Intelligence, to Sen. Ron Wyden (July 20, 2012), http://www.wired.com/images_blogs/dangerroom/2012/07/2012-07-20-OLA-Ltr-to-Senator-Wyden-ref-Declassification-Request.pdf. In addition, the *New York Times* has reported that since the time of the FAA's enactment the government has intercepted even more private electronic communications than are authorized by the FAA. Erich Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, April 15, 2009, http://www.nytimes.com/2009/04/16/us/16nsa.html?_r=2&pagewanted=all. In June 2009, Representative Rush Holt, then Chairman of the House Select Intelligence Oversight Panel, claimed that "Some actions [were] so flagrant that they can't be accidental." James Risen & Eric Lichtblau, *E-Mail Surveillance Renews Concerns in Congress*, N.Y. TIMES, June 16, 2009, http://www.nytimes.com/2009/06/17/us/17nsa.html?sq=&st=nyt&scp=41&pagewanted=all Documents acquired by the ACLU in June 2010 through a FOIA request suggest that the overcollection problem continued at least through March 2010. *See* ACLU Summary, http://www.aclu.org/files/pdfs/natsec/faafoia20101129/20101129Summary.pdf.

[6] The Second Circuit recently held that plaintiffs had standing to sue in a challenge to the constitutionality of the FAA and the Supreme Court has granted review on the standing question. *See Amnesty Int'l* v. *Clapper*, 638 F.3d 118 (2011), *cert. granted*, 2012 WL 526046. Plaintiffs allege violations of the First and Fourth Amendments.

observed – long before the emergence of the kind of electronic surveillance that is done today – "[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).

A. The Fourth Amendment generally requires that the government obtain a warrant before engaging in electronic surveillance

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

U.S. Const. amend. IV. Warrants must meet three conditions to authorize a lawful search: they must be issued by a neutral, disinterested magistrate; they must be supported by probable cause; and they must specify their targets with particularity. *Dalia* v. *United States*, 441 U.S. 238, 255 (1979). The Warrants Clause was designed to prevent abuses of authority like those common under the British Empire. *See Virginia* v. *Moore*, 128 S. Ct. 1598, 1603 (2008). Warrantless searches are "*per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." *United States* v. *Karo*, 468 U.S. 705, 717 (1984).

In *Katz* v. *United States*, 389 U.S. 347 (1967), the Court established the general rule that government intrusion upon an individual's reasonable expectation of privacy constitutes a search and therefore requires a warrant. The Court held that Americans have a reasonable expectation of privacy in their private communications. Electronic surveillance is therefore "a 'search and seizure' within the meaning of the Fourth Amendment," *Katz*, 389 U.S. at 353. *See, e.g.*, *Dalia*, 441 U.S. at 256 n.18 ("Electronic surveillance undeniably is a Fourth Amendment intrusion requiring a warrant."); *United States* v. *United States District Court*, 407 U.S. 297, 313 (1972) ("[Katz] implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.").[7] Thus, in general, the government needs a warrant before it may acquire electronic communications to which a U.S. person is a party.

B. The Fourth Amendment applies to foreign intelligence surveillance of U.S. persons and individuals located in the United States

Because and to the extent that surveillance under the FAA may intercept the communications of U.S. persons and individuals located in the United States, safeguards are needed to avoid infringement of Fourth Amendment rights.

The Supreme Court has not extended the Fourth Amendment's protections to searches abroad of non-U.S. persons, and so warrantless surveillance of such individuals is lawful under

[7] A majority of the Justices of the Supreme Court recently acknowledged in a case involving GPS tracking that technological advances give the government unprecedented power to conduct electronic surveillance, infringing upon our reasonable expectations of privacy. *See United States* v. *Jones*, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring; writing for four justices); *id*. at 956 (Sotomayor, J. concurring).

current interpretation. *See United States* v. *Verdugo-Urquidez*, 494 U.S. 259 (1990). One of the justifications for enactment of the FAA was to enable the government to intercept communications legally as they transit equipment located in the United States, even though both parties to the communication are non-U.S. persons located in foreign countries. To the extent that the FAA provides legal authority for such interceptions – when the government *knows* that all parties whose communications will be intercepted are non-U.S. persons located abroad – we do not believe the Act raises Fourth Amendment concerns.

Surveillance conducted for foreign intelligence purposes does not enjoy a blanket exemption from Fourth Amendment scrutiny, however. Under the so-called "foreign intelligence exception" supported by some commentators and accepted by the Foreign Intelligence Surveillance Court of Review, a warrant is not required for surveillance that is conducted "to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." *See In re Directives*, 551 F.3d 1004, 1008 (FISA Ct. Rev. 2008). But even if this exception "applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." *Id.* at 1013. In other words, the FAA does not provide an exemption for intrusions upon the privacy of non-targeted U.S. persons and individuals located within the United States.

Surveillance "directed against" foreign powers and their agents may not of course be employed as a subterfuge for surveillance of U.S. persons interacting with these targets, nor a loophole through which the government may collect vast quantities of data on U.S. persons for subsequent review and analysis. Some have argued that the FAA complies with constitutional requirements because the government may intentionally target only foreign persons or organizations located abroad. Under this argument, while the government may not *intentionally* target the communications of U.S. persons or individuals located within the United States under the FAA, it may still gather vast quantities of data about them "incidentally" when they communicate with a foreign surveillance target; this interception would then be justified as incident to an otherwise-lawful warrantless FAA search. The Supreme Court has not yet addressed this application of the "incidental interceptions" doctrine, and so we acknowledge that this area of the law is unclear.

But even if the incidental interceptions doctrine does apply to warrantless surveillance under the FAA, it should not allow the government to collect *and review* vast quantities of private data about non-targeted U.S. persons, by intercepting and saving for later inspection the conversations of *any and all* such persons with whom targets communicate – when there has been no individualized judicial review or even suspicion that the U.S. persons have engaged in unlawful conduct. Current Supreme Court doctrine goes no further than to permit "incidental interception" where there has been a prior court order authorizing surveillance of a specific individual or individuals. *See, e.g., United States* v. *Kahn*, 415 U.S. 143 (1974) (upholding a wire interception order based on probable cause even though it did not identify all potential interceptees). The Court has implied that while an otherwise valid interception is not unlawful simply because the government failed "to identify every individual who could be expected to be

overheard…the *complete absence* of prior judicial authorization would make an intercept unlawful." *United States* v. *Donovan*, 429 U.S. 413, 436 n.24 (1977) (emphasis added).[8]

Even when a search may be performed without a warrant, it must be conducted reasonably. The potentially enormous scope of government surveillance implicates the reasonableness requirement. When analyzing reasonableness, courts balance the governmental interest at stake versus the individual privacy interests the Fourth Amendment is meant to protect. *See Vernonia School District 47J* v. *Acton*, 515 U.S. 646, 652 (1995). Issues of concern include the intrusiveness of the search and the degree to which executive discretion is limited. *See Berger*, 388 U.S. at 58 (comparing broad authority to engage in electronic surveillance to "general warrants" which are repudiated by the Fourth Amendment).

Because of its potential for incidental interception of the private communications of U.S. persons, FAA programmatic surveillance should be subjected to meaningful *ex ante* judicial review.[9] Although it may not be practicable in all instances to meet the particularity requirement of a warrant before conducting foreign intelligence surveillance, the FAA should be amended to require that the FISC conduct a more rigorous review of government certifications for programmatic surveillance to ensure the privacy rights of U.S. persons are not being violated.[10] As explained in more detail below, to further reduce the risk of intercepting communications of U.S. persons and individuals located within the United States, the government should be required to develop and submit to the FISC procedures for determining when an acquisition may be expected to collect communications to or from the United States or involving any U.S. persons. Then, in cases where the planned surveillance may reasonably be expected to intercept communications to or from a person reasonably believed to be in the United States or to be a U.S. person, the government should be required to obtain a FISA warrant under pre-FAA standards.

Where a warrant is not required before *collecting* information on a U.S. person or an individual located in the United States because that person was not the target, then a warrant should be required before the government may *examine* the information that has already been collected in order to seek information on such individuals. In other words, if the government is "incidentally" intercepting communications of U.S. persons and individuals located in the United States, and it later seeks to use its database of intercepted communications to target, investigate or identify these U.S. persons and individuals within the United States, a warrant should be required at that point.

---

[8] Nor should the plain sight rule, which permits an officer to seize items in plain sight while conducting a lawful warrantless search, extend to electronic surveillance. The rule does not apply to this context and expanding the rule in this manner would significantly infringe upon privacy interests.

[9] One scholar has argued that the FISA warrant requirement encourages the government to screen its warrant applications, even if virtually all are approved by the FISC. *See* Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 PUB. INT. L.J. 269, 307 (2009).

[10] Some committee members believe that to comply with the Fourth Amendment, the government should once again be required to obtain individualized probable cause warrants from the FISC before engaging in electronic surveillance of communications to or from the United States for foreign intelligence purposes. However, all of the undersigned committee members agree that at a minimum, Congress should amend the FAA to require more thorough judicial review by the FISC before surveillance may be authorized.

The need for judicial oversight and authorization becomes more urgent as technology enables the interception of far more communications than ever before. As Justice Alito, writing for four members of the Court, recently noted in *Jones*, "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." *United States* v. *Jones*, 132 S. Ct. 945, 959 (2012) (Alito, J., concurring). Electronic surveillance has no practical limitations – certainly none that protect privacy. Instead, it can generate a "precise, comprehensive record…that reflects a wealth of detail" about an individual. *Id.*, 132 S. Ct. at 955 (Sotomayor, J., concurring). The phrase "incidental interceptions" implies a *de minimis* collection of private communications, but programmatic surveillance is capable of scooping up such communications by the terabyte. Thorough judicial oversight should be required to compensate for the elimination of practical barriers to surveillance – and to avoid "alter[ing] the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States* v. *Cuevas–Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

II. The FISA Amendments Act Lacks Critical Fourth Amendment Safeguards

Section 702(a) of the FAA empowers the Attorney General and the Director of National Intelligence to authorize programmatic surveillance targeting foreign persons or organizations located outside the United States.[11] This sweeping grant of power allows the government to conduct surveillance of entire categories of persons for the broad purpose of acquiring "foreign intelligence information." The government may collect electronic communications under such a programmatic grant of authority for up to a year, and may then seek renewal of the certification. The public is not told what this authority actually means in quantitative terms, but the numbers must be staggering.[12]

The FAA contains express limitations on the government's power to acquire communications, but they are not sufficient to ensure that the FAA's sweeping programmatic surveillance comports with the Fourth Amendment. Defenders of the FAA particularly cite Section 702(b)(2), which prohibits "reverse targeting,"[13] as evidence that the law passes muster. While there is some comfort in the provision that the government may not *target* U.S. persons or individuals located within the United States, none of the Section 702(b) limitations prevents the government from sweeping up the communications of U.S. persons and individuals within the United States "incidentally." Moreover, statements by government officials at the time of the FAA's enactment indicate that acquiring communications between foreign targets and Americans was one of the intelligence community's highest priorities.[14] It is untenable to justify

[11] See Appendix for text of 50 U.S.C. § 1881a(a)-(b).

[12] Although we do not know how many of these have been intercepted pursuant to the FAA, the *Washington Post* reported in 2010 that the NSA intercepts 1.7 *billion* e-mails, phone calls, and other types of communications. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print/.

[13] "Reverse targeting" is where the government monitors a foreign target with the intention of actually collecting the communications of a person located in the United States.

[14] Letter from Attorney General Michael B. Mukasey and Director of National Intelligence J.M. McConnell to Senator Harry Reid (Feb. 5, 2008), http://www.justice.gov/archive/ll/docs/letter-ag-to-reid020508.pdf.

such sweeping and indiscriminate interceptions as merely "incidental" to an otherwise lawful search and therefore reasonable under the Fourth Amendment.

The FAA does not require the government to articulate any individualized suspicion regarding its targets, nor does the FAA even mandate that foreign intelligence be the primary purpose of a surveillance program. This compounds the risk that the communications of U.S. persons and individuals located within the United States will be swept up as part of the surveillance. Intelligence officials may target persons without demonstrating to the FISC that they are agents of a foreign power, as was previously required under FISA, and need not even show that a target is engaged in any suspicious acts. To obtain authorization for FAA programmatic surveillance, the government need only assert that a "significant" purpose of the surveillance is to acquire foreign intelligence information, a category so broad as to include virtually any information relevant to foreign relations. This standard also allows the government to intercept communications for other reasons, including collecting evidence for law enforcement. Additionally, persons targeted need only be "reasonably believed to be located outside the United States." If authorities are uncertain where a target is located, they may still engage in surveillance without a warrant.

Under the FAA, the government never has to identify programmatic surveillance targets to the FISC; it is required only to provide the FISC with its targeting and minimization procedures. The government need not reveal the names of its targets, the basis for targeting them, their locations, or the facilities, phone lines, and e-mail addresses subject to interception. Because FISC proceedings are classified, the public has no way of knowing whether the FISC actually receives the information it would need to provide an independent assessment of the targeting procedures, and the very limited review that the FAA requires the FISC to conduct is insufficient to provide effective oversight. When coupled with such broad authority for the government to engage in surveillance, the lack of requirements for meaningful judicial review raises serious constitutional concerns. At a minimum, the Executive Branch should disclose and Congress should require a fuller description of the FISC's procedures. In addition, Congress should amend the FAA to require that such details about targeting procedures be provided to and assessed by the FISC.

The FAA stipulates that surveillance "shall be conducted in a manner consistent with the fourth amendment" § 702(b)(5), but this statutory declaration does not assure that surveillance authorized by the FAA *in fact* complies with the Fourth Amendment. We would applaud interpreting this provision to require meaningful judicial review of programmatic surveillance that may intercept communications to which a U.S. person or individual within the United States is a party, as well as a warrant before the government may review the communications that have already been collected to seek information on specific such persons. However, there is no indication that either the Executive Branch or the FISC has interpreted the FAA narrowly to avoid infringing Fourth Amendment rights, and, as outlined above, other provisions of the FAA authorize surveillance that is constitutionally problematic, such as permitting entirely warrantless collection and review of communications to or from the United States or involving U.S. persons.

A former technical director at the NSA recently commented that "the real plan was to spy on Americans from the very beginning." Kim Zetter, *Former NSA Official Disputes Claims by NSA Chief*, WIRED THREAT LEVEL BLOG, July 29, 2012, http://www.wired.com/threatlevel/2012/07/binney-on-alexander-and-nsa/.

In addition to raising privacy concerns, unless it is appropriately focused on legitimate targets, the bulk surveillance permitted by the FAA is less effective at dealing with threats of terrorism. As other experts have noted, finding evidence of an impending attack amidst millions of innocuous conversations is the proverbial needle in the haystack. Since 9/11, intelligence officials have noted the difficulty of searching through the data that are collected, even using sophisticated data-mining algorithms.[15] Requiring more probing judicial review prior to surveillance, as well as requiring a showing of probable cause before connecting information to a specific U.S. person or individual within the United States, will increase the likelihood that the information reviewed is essential to foreign intelligence.

The FAA should be amended to restore the requirement that foreign intelligence be the primary purpose of any programmatic surveillance, and to require thorough *ex ante* judicial review. The government should be obligated to provide more information to the FISC regarding requested surveillance authorizations, and the Act should specify that the FISC should conduct a more in-depth review than is currently required by statute. Specifically, when submitting its certifications, the government should have to explain the foreign intelligence purpose of its planned surveillance; clearly define the category or categories of individuals to be targeted and the relevance of their communications to the identified intelligence purpose; and provide sufficient information to enable the court to assess the extent of anticipated interceptions of communications of U.S. persons and persons in the United States.

In addition, the government should be required to develop and submit to the FISC procedures for assessing when surveillance may be expected to collect communications to or from the United States or involving U.S. persons. If the application of such a procedure reveals that a proposed surveillance program may reasonably be expected to intercept communications to or from a person reasonably believed to be in the United States or a U.S. person, the FAA should require the government to obtain a FISA warrant under pre-FAA standards. Such requirements would help to ensure the protection of privacy rights guaranteed by the Fourth Amendment. At present, the FAA permits mass programmatic surveillance; allows unlimited interception of communications to which U.S. persons and individuals located within the United States are party as long as they are not the official targets; does not sufficiently require individualized suspicion; and does not provide for meaningful judicial oversight. It should not be reauthorized until these concerns are addressed and adequate safeguards are restored.

---

[15] *See* ERIC LICHTBLAU, BUSH'S LAW : THE REMAKING OF AMERICAN JUSTICE 160 (2009); Lowell Bergman et al., *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, http://www.nytimes.com/2006/01/17/politics/17spy.html?ei=5090&en=f3247cd88fa84898&ex=1295154000&pagewanted=print; A report authored by the National Research Council and sponsored by the Department of Homeland Security found that filtering huge amounts of data for patterns linked to terrorist threats (the "needle in the haystack" problem) is "extremely difficult to achieve." National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, at 2 (2008), http://www.nap.edu/catalog.php?record_id=12452; *see also* The Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* at 10 – 11 (2010), http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.

III. The FISA Amendments Act Should Contain Stronger Safeguards Restricting Government Retention and Use of Private Communications

Not only does the FAA confer unprecedented authority to engage in broadscale warrantless programmatic surveillance, but it also permits the government to maintain a vast – and searchable – database of communications. As noted above, as long as U.S. persons and individuals located within the United States are not directly targeted, the government can scoop up their private conversations without any showing of suspicion and retain this data forever. The FAA in its present form does not inspire confidence that this information has been or will be used only for legitimate foreign intelligence purposes. In fact, the *New York Times* reported in 2009 that the National Security Agency had been "engaged in 'overcollection' of domestic communications of Americans," and attempted to tap the international communications of a congressman without a warrant.[16] The ample possibility for abuse of collected information – or simply unrestricted use – once the information is in the government's possession necessitates strong safeguards for privacy rights. The scope and volume of private communications that are subject to warrantless collection under the FAA poses a real threat to the privacy of U.S. persons and individuals within the United States. The FAA should only be reauthorized if it is amended to incorporate tighter restrictions on the retention, dissemination, and use of communications collected under warrantless programmatic surveillance.

Most importantly, as introduced above, a post-collection warrant should be required before the government may search through its database of intercepted communications for information about specific U.S. persons or individuals located in the United States.[17] The FAA's authorization of programmatic surveillance should not permit the government to circumvent the Fourth Amendment rights of persons whose communications are "incidentally" intercepted. The lawful "incidental" interception of the communications of such persons becomes an unlawful search and seizure if, and when, the government begins to focus in on individuals. At that point, the government is engaged in a search, impinging upon reasonable expectations of privacy,[18] but the FAA contains few restrictions on how and when information may be later reviewed and used. Permitting the government to build a massive database and then search through it at will to uncover private communications creates a loophole that seriously undercuts the FAA's prohibition on targeting U.S. persons and individuals located in the United States. This is particularly concerning given that surveillance may take place over a period of years, allowing the government to assemble a detailed record of a person's private communications without even a *minimum* showing of suspicion, much less probable cause. To properly safeguard Fourth

[16] Lichtblau & Risen, *supra* note 5.

[17] The Constitution Project has advanced similar proposals in the contexts of video surveillance and cybersecurity. *See* The Constitution Project's Liberty and Security Committee, *Guidelines for Video Surveillance* 27-29 (2007), http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf; The Constitution Project's Liberty and Security Committee, *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy* 28 (2012), http://www.constitutionproject.org/pdf/TCPCybersecurityReport.pdf. Senators Mike Lee and Dick Durbin recently proposed an amendment that would require a warrant before searching for data on a specific U.S. person except in emergency circumstances. *See* http://www.judiciary.senate.gov/legislation/upload/HEN12563-Lee-Durbin.pdf; *see also Report on FAA Sunsets Extension Act of 2012*, Senate Select Committee on Intelligence, June 7, 2012, http://intelligence.senate.gov/pdfs112th/112174.pdf (discussing similar amendment by Sens. Wyden and Udall).

[18] As discussed above, the reasonable expectation of privacy analysis is strengthened by the two concurring opinions, totaling five justices, in *United States v. Jones*, 132 S. Ct. 945 (2012).

Amendment rights, the government should be required to obtain a warrant before it may intrude upon individual privacy to such an extent.

Similarly, a warrant should be required before the government can associate communications acquired under the FAA with a specific U.S. person, or review communications known to be to or from the United States. The government presumably uses complex data mining algorithms to filter the immense amounts of data that it collects.[19] False positives could lead to the seizure of Americans' private conversations contained in the database, where there was never any showing of suspicion about the American. The performance of data mining algorithms should be equally subject to review by the FISC. Communications collected under the FAA involving specific U.S. persons or individuals located within the United States should be stored in anonymized formats, and data mining or other analysis should be restricted to such anonymized records. Then, if and when intelligence analysis identifies a particular communication or group of communications as of interest, and there is a need to know the identity of the sender or receiver, the government should be required to obtain a warrant based on probable cause to uncover the identity of such U.S. persons.

Even if Congress does not amend the FAA to require the post-collection warrants discussed above, at a minimum it should require warrants before the incidentally collected communications of U.S. persons can be used by law enforcement agencies to prosecute U.S. persons. Currently, 50 U.S.C. § 1801(h)(3) from pre-FAA FISA permits information to be "retained and disseminated for law enforcement purposes." The unlimited sharing with law enforcement permitted by this provision is troubling given the expanded warrantless collection powers that the FAA now provides to the government. Criminal prosecution is of course an important tool with respect to national security, and the government may legitimately seek to use some collected information for that purpose. *See In re Sealed Case*, 310 F.3d 717, 743 (FISA Ct. Rev. 2002). However, Section 1801(h)(3), appears to allow the prosecution of Americans for offenses *unrelated* to national security using information swept up by the NSA's warrantless programmatic surveillance. Accordingly, at the very least a warrant should be required before information collected under the FAA can be obtained by law enforcement for the purpose of criminal prosecution of a U.S. person. *See Berger* v. *New York*, 388 U.S. 41, 68 (1967) (Douglas, J., concurring) (arguing for the application of the exclusionary rule to evidence gathered via electronic surveillance).

Moreover, if Congress fails to require more exacting *ex ante* judicial review of FAA surveillance, it should amend the Act to enhance the privacy safeguards that apply post-collection. Specifically, the FAA should require stronger procedures for minimization. Under pre-FAA FISA, minimization procedures had to be tailored to individual targets, but the FAA allows the government to set procedures for the *entire program* of surveillance. *Compare* 50 U.S.C. § 1804(a)(5) (requiring a statement of proposed minimization procedures to issue an individual order) *with* FISA Amendments Act, § 702(g)(ii) (requiring that a certification include

[19] *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1659 (2010). For an extended discussion of the implications of data-mining technology and recommendations on incorporating safeguards to protect privacy rights, *see* The Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (2010), http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.

minimization procedures with respect to the program as a whole). Where private information about Americans can be collected without any showing of suspicion, then retained and used even for purposes unrelated to foreign intelligence, there is obviously a greater need for minimization to be effective.

To ensure that minimization procedures are sufficient, the FAA should incorporate more thorough judicial review by the FISC. Currently, the FISC only looks at the procedures themselves, more or less in a vacuum. The FAA should be amended to require that the FISC be given enough information about the success and failures of the government's minimization and targeting procedures to render an independent judgment of their adequacy, and that the FISC play an ongoing role in reviewing and supervising the implementation of these procedures. The FAA should clearly require that prior to re-authorizing a surveillance program, the FISC scrutinize the extent to which minimization has been conducted as well as the actual impact of the surveillance on U.S. persons and individuals located within the United States, and order additional measures if necessary. Robust provisions for post-collection judicial review and independent oversight are crucial, especially if Congress fails to restore requirements for *ex ante* judicial review in the form of a warrant. The Fourth Amendment mandates scrutiny by an impartial judiciary to protect privacy interests from government intrusion; it does not permit the Executive Branch to police itself.

IV. Congress Should Conduct Vigorous Oversight to Ensure that the FAA Does Not Infringe Upon Privacy

In addition to restoring judicial safeguards as outlined above, Congress itself should intensify its oversight of FAA-authorized programmatic surveillance. It should require the Executive Branch to disclose further information about its interpretation of the legal authority provided by the FAA and the scope of surveillance permitted, and to provide a detailed accounting of the actual operation of the program.[20] Congress should only reauthorize the FAA after conducting a thorough review of how the FAA has been implemented since its enactment and then restoring adequate safeguards for privacy rights.

In particular, Congress should require an explanation of how the intelligence community has used its authority under the FAA. Attempts to obtain details regarding how many Americans' communications have been intercepted have generally not been successful. In a letter responding to a request for such information by Senators Ron Wyden and Mark Udall, the Inspector General of the Intelligence Community stated that "an estimate was beyond the capacity" of the NSA.[21] If even an *estimate* is impracticable, then Americans can rightfully be concerned about the scope of this electronic surveillance. To the extent that the NSA is unable to calculate such statistics at present because it simply is not currently tracking such information, then it should be required to develop procedures by which the actual impact on Americans can be estimated.

[20] Thirteen senators recently signed a letter to Director of National Intelligence James Clapper requesting information regarding how many Americans have been intercepted under the FAA, but they have not yet received an answer. Letter from Sen. Mark Udall to Director James Clapper (July 26, 2012), http://www.markudall.senate.gov/?p= press_release&id=2586.

[21] Letter from I. Charles McCullough to Sens. Ron Wyden &Mark Udall (June 15, 2012), at 1, http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.

The FAA should be amended to incorporate reporting requirements that would better inform the public and facilitate meaningful congressional oversight. The Inspector General for the intelligence community should be required to audit FAA-authorized programmatic surveillance programs and issue annual reports to Congress with statistics describing how many Americans have had their communications intercepted – lawfully and unlawfully.[22] This should include aggregate statistics on the average number of communications involving any particular American that have been "incidentally" intercepted, as well as statistics showing the maximum number of such interceptions for any given U.S. person and the number of communications to or from the United States that have been intercepted, to demonstrate the extent to which large quantities of data may be collected on any particular U.S. person even if he or she is not a target. This information should be compiled in a manner which respects the privacy rights of Americans whose communications have been intercepted, by providing aggregate statistics and without identifying any particular individual in the reports. This information will enable Congress to ensure that the Executive Branch stays within lawful limits and that constitutional rights are protected, and to amend the law as needed based upon these reports.

More information should also be provided to the public, although certain information will of course remain classified. An unclassified summary containing aggregate statistics showing how often the government has intercepted the conversations of U.S. persons should be released by the intelligence community's Inspector General. Additionally, significant decisions by the FISC should be released even if in redacted form or, at a minimum, summarized in an unclassified report. Although the specific facts showing the justification for surveillance in particular cases may remain classified, the standards and analysis being applied by the FISC should be made public. Similarly, a hypothetical or redacted certification submitted to the FISC to justify surveillance should be released to illustrate the extent to which statutory requirements are being complied with as well as the meaningfulness of FISC review. Information regarding the administration's minimization and targeting procedures should be released as well, to the extent possible. Releasing such information will provide a valuable check upon violations of privacy rights, and will also improve public confidence in the legitimacy of the federal government's intelligence collection.

V. Conclusion

The FAA permits the government to engage in broad scale surveillance outside traditional Fourth Amendment limits; to retain massive amounts of personal information for far longer than necessary; and to do so in secret with minimal oversight from the other branches of government. The government must of course protect national security, but it also has a responsibility to respect the private communications of Americans. A public, democratic debate should inform Congress's deliberations on the continuing need for the FAA's sweeping grant of

[22] Senators Ron Wyden and Mark Udall proposed a similar amendment, which would require the Inspector General to provide an estimate of how many Americans have been intercepted. *See* Sen. Ron Wyden, Hold Statement for Congressional Record on FISA Amendments Act (June 11, 2012), http://www.scribd.com/doc/96739611/Wyden-Hold-Statement-for-Congressional-Record-on-FISA-Amendments-Act. Representative Sheila Jackson Lee offered an identical amendment during the House Judiciary Committee mark-up of the FAA reauthorization bill. http://judiciary.house.gov/hearings/Markups%202012/PDF/06192012/061912JacksonLee%20Amdt4%20-%20FAILED.pdf.

power. Reducing the term of reauthorization from five to three years is a good idea,[23] but avoiding a thorough, substantive review of the FAA is not. The constitutional threats posed by the FAA require a thorough review by Congress now. We believe that the actions we recommend will ensure both that the government has the authority to gather critical information and that government surveillance stays within legal and constitutional limits.

Accordingly, we, the undersigned members of The Constitution Project's Liberty and Security Committee, recommend:

1. **Increased Judicial Review of Surveillance Authorizations:** The FAA should be amended to require more robust judicial review by the FISC to authorize programmatic surveillance and ensure that it is appropriately focused on foreign intelligence. Specifically:
    (a.) Congress should restore the requirement that foreign intelligence be the primary purpose of the programmatic surveillance.
    (b.) When seeking approval for programmatic surveillance, the government should be required to (1) explain the foreign intelligence purpose of the proposed surveillance, (2) define the scope of planned interceptions, and (3) provide a risk assessment and an estimate of reasonably anticipated interceptions of the communications of U.S. persons and individuals located within the United States. The surveillance should only be permitted after the FISC has thoroughly evaluated these submissions to ensure that surveillance is appropriately designed to acquire foreign intelligence information from legitimate targets without interfering with the privacy rights of U.S. persons and individuals located within the United States.
    (c.) Additionally, the government should be required to develop and submit to the FISC procedures for determining when an acquisition may be expected to collect communications to or from the United States. Then, in cases where the planned surveillance may reasonably be expected to intercept communications to or from a person reasonably believed to be in the United States, the government should be required to obtain a FISA warrant under pre-FAA standards.

2. **Inclusion of Warrant Requirements and Other Safeguards for Post-Collection Use of Information:** The FAA should be amended to require that the government obtain a warrant from the FISC before searching collected communications for information on a specific U.S. person, decrypting the identity of a specific U.S. person party to a conversation, or reviewing communications reasonably believed to be to or from the United States. As required under the pre-FAA version of FISA, the warrant should be based upon a showing of probable cause to believe that the target is an agent of a foreign power or has committed a crime, and that evidence of the crime will be found and must name its target(s) with particularity. Moreover, Congress should ensure that collected information is being properly used for foreign intelligence purposes, including at the very least a requirement that authorities obtain a warrant before using data for law enforcement purposes. Finally, Congress should amend the FAA to require more

[23] The Senate Judiciary Committee adopted an amendment to this effect by unanimous consent. *See* http://www.judiciary.senate.gov/legislation/upload/HEN12571-Leahy-Sub.pdf.

stringent procedures for minimization, including periodic, ongoing FISC review of the implementation and efficacy of such procedures.

3. **Increased Reporting and Oversight:** More information about the intelligence community's use of the FAA should be provided to Congress and the public. Before reauthorizing the FAA, Congress should demand and review detailed information regarding the operation of the FAA surveillance program to date, including the extent and scope of interceptions of the communications of U.S. persons and individuals located within the United States. Further, the Inspector General of the Intelligence Community should be required to audit these surveillance programs and issue annual reports to Congress regarding how government surveillance has been conducted. In particular, these reports should include: statistics regarding how many U.S. persons' communications have been intercepted by the government; aggregate statistics on the number of intercepted communications in total, and the number of intercepted communications to or from the United States or involving any U.S. person; an analysis of the performance of the government's targeting and minimization procedures; and an explanation of how collected information has been used, including the number of times the information has been used for law enforcement rather than foreign intelligence purposes. These reports should also be provided in an unclassified form released to the public. Additionally, as much as practicable, more information on the FAA should be released to the public, including important decisions by the FISC and Foreign Intelligence Surveillance Court of Review, redacted as necessary.

Appendix

The Current FISA Amendments Act, 50 U.S.C. § 1881a(a)-(b)

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) Limitations

An acquisition authorized under subsection (a)–

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire 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

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

MEMBERS OF THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE
Endorsing the Report on the FISA Amendments Act of 2008*

CO-CHAIRS:

David Cole, Professor of Law, Georgetown University Law Center

David A. Keene, former Chairman, American Conservative Union

MEMBERS:

Stephen Abraham, Lieutenant Colonel (USAR, Ret.); Law Offices of Stephen E. Abraham

Bob Barr, former Member of Congress (R-Ga.); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy, the American Conservative Union; Chairman, Patriots to Restore Checks and Balances; practicing attorney

David E. Birenbaum, Of Counsel, Fried, Frank, Harris, Shriver & Jacobson LLP; Senior Scholar, Woodrow Wilson International Center for Scholars; U.S. Ambassador to the U.N. for U.N. Management and Reform, 1994-96

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

Eugene R. Fidell, Senior Research Scholar in Law and Florence Rogatz Visiting Lecturer in Law, Yale Law School

Michael German, Special Agent, Federal Bureau of Investigation, 1988-2004; former Adjunct Professor, National Defense University School for National Security Executive Education

Philip Giraldi, Contributing Editor for *The American Conservative Magazine*, antiwar.com, and *Campaign for Liberty*; Executive Director, Council for the National Interest; former operations officer specializing in counter-terrorism, Central Intelligence Agency, 1975-1992; United States Army Intelligence

Asa Hutchinson, Senior Partner, Asa Hutchinson Law Group; Undersecretary, Department of Homeland Security, 2003-2005; Administrator, Drug Enforcement Administration, 2001-2003; Member of Congress (R-Ark.), 1997-2001; United States Attorney, Western District of Arkansas, 1982-1985

David Lawrence Jr., President, Early Childhood Initiative Foundation; Education and Community Leadership Scholar, University of Miami's School of Education and Human Development; Member, Governor's Children's Cabinet; retired publisher of *The Miami Herald*

Mary O. McCarthy, Consultant, Freedom of Information and Privacy Act; Associate Deputy Inspector General, Investigations, Central Intelligence Agency, 2005-2006; Visiting Fellow, Center for Strategic and International Studies, 2002-2004; Senior Policy Planner, Directorate of Science and Technology, Central Intelligence Agency, 2001-2002; Senior Director, Special

Assistant to the President, National Security Council, 1998-2001; Director for Intelligence Programs, National Security Council, 1996-1998; National Intelligence Officer for Warning, (Deputy 1991-1994) 1991-1996

James E. McPherson, Rear Admiral USN (Ret.); Executive Director, National Association of Attorneys General; Judge Advocate General of the Navy, 2004-2006; Deputy Judge Advocate General of the Navy, 2002-2004; Active Duty, United States Navy, Judge Advocate General's Corps, 1981-2006; former General Counsel for the Department of Defense Counterintelligence Field Activity

Paul R. Pillar, Visiting Professor and Director of Studies, Security Studies Program, Georgetown University; intelligence officer (positions included Deputy Chief of DCI Counterterrorist Center, National Intelligence Officer for the Near East and South Asia, and Executive Assistant to the Director of Central Intelligence), Central Intelligence Agency and National Intelligence Council, 1977-2005

James Robertson, Neutral Arbitrator and Mediator, JAMS; U.S. District Judge for the District of Columbia, 1994-2010; Judge, Foreign Intelligence Surveillance Court, 1994-2005

Earl Silbert, Partner, DLA Piper; United States Attorney, District of Columbia, 1974-1979; former Watergate Prosecutor

Neal R. Sonnett, member, American Bar Association (ABA) Board of Governors; past Chair, ABA Task Force on Treatment of Enemy Combatants and Task Force on Domestic Surveillance in the Fight Against Terrorism; past Chair, ABA Criminal Justice Section; former Assistant United States Attorney and Chief of the Criminal Division for the Southern District of Florida

Geoffrey R. Stone, Edward H. Levi Distinguished Service Professor, University of Chicago; former Provost, University of Chicago, 1993-2002

Colby Vokey, Lieutenant Colonel USMC (Ret.); Attorney, Fitzpatrick Hagood Smith & Uhl LLP; Lieutenant Colonel, U.S. Marine Corps, 1987-2008; lead counsel for Guantanamo detainee Omar Khadr at Military Commissions, 2005-2007

Don Wallace, Chairman, International Law Institute; Professor Emeritus and Adjunct Professor, Georgetown Law

John W. Whitehead, President, The Rutherford Institute

Lawrence B. Wilkerson, Colonel, U.S. Army (Ret.); Adjunct Professor of Government and Public Policy at the College of William and Mary; Chief of Staff to Secretary of State Colin L. Powell, 2002-2005

THE CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel, Rule of Law Program

* Affiliations are listed for identification purposes only