UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, - against - AGRON HASBAJRAMI, *Defendant*.	11 Cr. 623 (JG)

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS

Patrick Toomey
Jameel Jaffer
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Amici Curiae

Hanni Fakhoury
Mark Rumold
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
hanni@eff.org

Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF *AMICI CURIAE*

Amicus curiae American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil rights laws. Since its founding in 1920, the ACLU has appeared before the federal courts as direct counsel and as *amicus curiae* in many cases involving the Fourth Amendment, including cases concerning foreign-intelligence surveillance. For example, the ACLU represented the plaintiffs in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), and it currently serves as direct counsel in *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo.), and *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (appeal pending).

Amicus curiae Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization working to protect innovation, free speech, and privacy in the online world. With more than 22,000 dues-paying members nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. EFF has participated, either directly or as *amicus*, in FISA cases, including *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011); *First Unitarian Church of Los Angeles v. NSA*, No. 13-cv-03287 (N.D. Cal. filed July 16, 2013); *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 671 F.3d 881 (9th Cir. 2011); and *Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d 845 (9th Cir. 2012) (amicus).

INTRODUCTION

In this criminal prosecution, the government has indicated that it intends to introduce evidence obtained or derived from surveillance conducted under the FISA Amendments Act of 2008 ("FAA"). *Amici* submit this brief to provide the Court with information about the scope of the law and the manner in which the law has been implemented. The brief makes three points. First, the FAA represents a stark departure from the traditional FISA regime, which governed foreign-intelligence surveillance in the United States from 1978 until the FAA's enactment in 2008. As originally enacted, FISA permitted the government to conduct surveillance of foreign powers and their agents based on individualized judicial authorization; the FAA, by contrast, permits the government to monitor Americans' communications without individualized judicial approval and without reference to whether the targets of the surveillance are foreign powers or foreign agents. Second, the government has implemented the FAA broadly, relying on the law to justify the collection of huge volumes of Americans' communications. Third, because FAA surveillance is both warrantless and unreasonable under the Fourth Amendment, it is unconstitutional. The government has reasonable alternatives that would permit it to collect foreign intelligence while protecting the privacy of Americans' communications.

Amici thank the Court for the opportunity to submit this brief and will make themselves available for argument should the Court conclude that *amici*'s participation would be helpful.

BACKGROUND

A. The Foreign Intelligence Surveillance Act of 1978

In 1975, Congress established a committee, chaired by Senator Frank Church, to investigate allegations of "substantial wrongdoing" by the intelligence agencies in their conduct of surveillance. Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II), S. Rep. No. 94-755, at v (1976) ("Church Report").

The committee discovered that, over the course of four decades, the intelligence agencies had "violated specific statutory prohibitions," "infringed the constitutional rights of American citizens," and "intentionally disregarded" legal limitations on surveillance in the name of "national security." *Id.* at 137. Of particular concern to the committee was that the agencies had "pursued a 'vacuum cleaner' approach to intelligence collection," in some cases intercepting Americans' communications under the pretext of targeting foreigners. *Id.* at 165. To ensure proper judicial involvement in the protection of Americans' communications, the committee recommended that all surveillance of communications "to, from, or about an American without his consent" be subject to a judicial warrant procedure. *Id.* at 309.

In 1978, largely in response to the Church Report, Congress enacted FISA to regulate surveillance conducted for foreign-intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny applications for surveillance orders in certain foreign-intelligence investigations. *See* 50 U.S.C. § 1803(a).

As originally enacted, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. *See id.* §§ 1805, 1809(a)(1). To obtain a traditional FISA order, the government is required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facilities to be monitored. *See id.* § 1804(a). The FISC may issue such an order only if it finds that, among other things, there is "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," and "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2)(A)–(B).

B. The Warrantless Wiretapping Program

On October 4, 2001, President George W. Bush secretly authorized the NSA to engage in

warrantless electronic surveillance inside the United States. After *The New York Times* exposed the program and a federal district court ruled that the program was unconstitutional, *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), the government stated that the program would not be reauthorized in its then-existing form. The government ultimately sought legislative amendments to FISA that granted authorities beyond what FISA had allowed for three decades.

C. The FISA Amendments Act of 2008

The legislative amendments sought by the Bush administration were embodied in the FAA, which was signed into law on July 10, 2008.[1] The FAA substantially revised the FISA regime and authorized the acquisition without individualized suspicion of a wide swath of communications, including U.S. persons' international communications, from companies inside the United States. Like surveillance under FISA, FAA surveillance takes place on U.S. soil. But the authority granted by the FAA is altogether different from, and far more sweeping than, the authority that the government has traditionally exercised under FISA. The FAA's implications for U.S. persons' constitutional rights are correspondingly far-reaching.

The FAA allows the government to conduct warrantless surveillance of international communications entering or leaving the United States, including communications sent or received by U.S. persons. It does this by permitting the government to intercept communications when at least one party to a phone call or email is a foreigner located abroad. In particular, the FAA permits the Attorney General and DNI to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Importantly, this surveillance is not limited to counterterrorism targets. Rather, "foreign intelligence information" is defined

[1] On August 5, 2007, Congress passed a predecessor statute, the Protect America Act ("PAA"), Pub. L. No. 110-55, 121 Stat. 552 (2007), whose authorities expired in February 2008.

extremely broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* § 1801(e).

No court ever approves the targets of this surveillance. Instead, the FISC approves only the general procedures the government proposes to use in carrying out its surveillance and, based on those procedures alone, the FISC issues a so-called "mass-acquisition order." *See id.* § 1881a(i). Before obtaining such an order, the government must provide to the FISC a written certification attesting that the FISC has approved, or that the government has submitted to the FISC for approval, both "targeting procedures" and "minimization procedures." *Id.* § 1881a(d)–(g). The targeting procedures must be "reasonably designed" to ensure the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id.* § 1881a(g)(2)(A)(I); *see Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144–45 (2013).

A crucial difference between the FAA and traditional FISA is that the FAA authorizes surveillance not predicated on probable cause or individualized suspicion. When the government makes an FAA application to the FISC, it simply asks the court to approve the overall targeting and minimization procedures that will guide the government's surveillance for the following year. The government need not demonstrate to the FISC that its surveillance targets are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, the FAA permits the government to target *any* foreigner located outside the United States in order to obtain foreign-intelligence information.[2]

[2] *See* David S. Kris & J. Douglas Wilson, 1 *National Security Investigations and Prosecutions* § 17.3, 602 (2d ed. 2012) ("For non–U.S. person targets, there is no probable-cause requirement; the only thing that matters is []the government's reasonable belief about[] the target's location.").

As noted, the FAA does not require the government to identify its surveillance targets to the FISC at all, or even to identify the specific "facilities, places, premises, or property at which" its surveillance will be directed. 50 U.S.C. § 1881a(g)(4). This means that the government can "direct surveillance . . . at various facilities without obtaining a separate authorization for each one." Kris & Wilson § 17.3, 602. The government may even direct its surveillance at "gateway" switches, through which flow the communications of millions of people, rather than at individual telephone lines or email addresses. *Id.* § 16.12, 577.

By dispensing with FISA's principal limitations, the FAA exposes every international communication—that is, every communication between an individual in the United States and a non-American abroad—to potential surveillance. Indeed, in the government's view, the FAA allows it to conduct the kind of vacuum-cleaner–style surveillance that the Church Committee found so disturbing. And, as discussed below, the NSA is using the statute to do precisely this.

To the extent the statute provides safeguards for U.S. persons, the safeguards take the form of "minimization procedures." 50 U.S.C. §§ 1881a(e), 1801(h)(1). The statute's minimization requirement is supposed to protect against the collection, retention, and dissemination of communications that may be intercepted "incidentally" or "inadvertently." However, the statute does not prescribe specific minimization procedures and it does not give the FISC authority to supervise compliance with those procedures. Most significantly, it includes an exception that allows the government to retain communications—including those of U.S. persons—if the government concludes that they may contain any information broadly considered "foreign intelligence." *Id.* In other words, the statute is designed to allow the government not just to collect but to retain, review, and use U.S. persons' international communications.

The FISC's oversight role in authorizing and supervising FAA surveillance is "narrowly

circumscribed." *In re Proceedings Required by § 702(i) of the FAA*, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008). Unlike the judiciary's traditional Fourth Amendment role—as a gatekeeper for particular acts of surveillance—the FISC simply approves vague parameters under which the government is free to conduct surveillance for up to one year. The role that the FISC plays under the FAA bears no resemblance to the role it traditionally played under FISA.[3]

D. The Government's Implementation of the FISA Amendments Act

The government has implemented the FAA broadly, relying on the statute to sweep up—and store for later use—huge volumes of Americans' communications.[4] The government has reported that in 2013 it monitored the communications of 89,138 targets under a single mass-acquisition order issued by the FISC.[5] In 2011, FAA surveillance resulted in the collection of more than 250 million communications, a number that has likely grown significantly as the number of NSA targets has ballooned.[6] Every time a U.S. person communicates with any one of those targets—targets that may include journalists, academics, and human rights researchers—the government can collect that communication. The government has refused to count, or even estimate, how many U.S. persons' communications it collects under the FAA, but by all indications that number is substantial.[7]

---

[3] *See, e.g.*, Hearing of the Privacy and Civil Liberties Oversight Bd. ("PCLOB") at 31:27–32:28 (July 9, 2013), http://cs.pn/177IpII (statement of former FISC judge James Robertson).

[4] *See, e.g.*, Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014, http://wapo.st/1xyyGZF.

[5] ODNI, Statistical Transparency Report at 2 (June 26, 2014), http://1.usa.gov/1lVG5xI. The total number of targeted accounts is, in reality, significantly higher because where multiple accounts are used by the same target, the government counts those accounts—or "selectors"—as a single target. *See id.* at 3.

[6] *See [Redacted]*, 2011 WL 10945618, at *9–*10 (FISC Oct. 3, 2011); Glenn Greenwald, *No Place to Hide* 111 (2014), http://bit.ly/1g5vgsv (NSA Slide, *Unique Selectors Tasked to PRISM*).

[7] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, http://wapo.st/1kdYqVb ("Even when the system works just as advertised, with no American singled out for targeting, the NSA routinely

By design, the targeting and minimization rules that supposedly protect the privacy of U.S. persons are weak and riddled with exceptions.[8] Those rules give the government broad latitude to review, analyze, use, and disseminate the communications it collects, including searching that data for information about Americans in unrelated criminal investigations.[9] Even domestic communications obtained in violation of the targeting rules may be reviewed and retained under a variety of circumstances. *See* 2011 Minimization Procedures at 8.[10]

Public disclosures indicate that the government conducts two types of surveillance under the FAA: PRISM surveillance and Upstream surveillance. These methods are described in documents released by the Director of National Intelligence, in decisions issued by the FISC, and in a recent report by the Privacy and Civil Liberties Oversight Board.[11] The government has not disclosed which specific program or programs it relied upon in this case.

1. PRISM Surveillance

In what is known as PRISM surveillance, the government obtains stored and real-time communications directly from online service providers like Google, Yahoo, Facebook, and Microsoft.[12] The government identifies the user accounts it wishes to monitor—for example,

---

collects a great deal of American content."); PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* at 87 (2014), http://bit.ly/1pJz0EA ("PCLOB Report").

[8] The government has officially disclosed a version of the minimization procedures it uses to implement the FAA. *Minimization Procedures* (Oct. 31, 2011), http://1.usa.gov/1e2JsAv ("2011 Minimization Procedures"). *The Guardian* has published a copy of the FAA targeting procedures approved by the FISC in 2009. *See Procedures Used by the NSA for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States* (July 28, 2009), http://bit.ly/1rf78HV ("2009 Targeting Procedures"); *see also [Redacted]*, 2011 WL 10945618, at *6–*7, *13–*16.

[9] *See* PCLOB Report at 59; Ellen Nakashima, *NSA Searched Americans' Communications Without a Warrant, Intelligence Director Says*, Wash. Post, Apr. 1, 2014, http://wapo.st/1mJ9cpl.

[10] FISC opinions make clear that the government has violated its own rules repeatedly, including in the months prior to Mr. Hasbajrami's arrest. *See, e.g.*, *[Redacted]*, 2011 WL 10945618, at *2–*9.

[11] *See, e.g.*, PCLOB Report at 33–41; *[Redacted]*, 2011 WL 10945618.

[12] *See* PCLOB Report at 33–34; *[Redacted]*, 2011 WL 10945618, at *9 & n.24; *NSA Prism Slides*, Guardian, Nov. 1, 2013, http://bit.ly/1qmj46r.

particular Yahoo email addresses—and then collects from the provider all communications to or from those accounts, including any and all communications with U.S. persons. As of April 2013, the NSA was monitoring at least 117,675 targeted accounts via PRISM.[13] In order to facilitate the surveillance of PRISM targets, providers "were essentially asked to erect . . . locked mailbox[es]" containing user communications and to "give the government the key[s]."[14]

2. Upstream Surveillance

The second collection method, known as Upstream surveillance, operates very differently from PRISM. Upstream surveillance involves the NSA copying and searching entire streams of internet traffic as that data flows across fiber-optic networks inside the United States. The NSA apparently copies "most e-mails and other text-based communications that cross the border."[15] Upstream surveillance can be understood as encompassing the following stages:

- **Stage 1: Copying**. The NSA creates a copy of *all* traffic flowing across certain circuits on the "internet backbone," including circuits maintained by Verizon and AT&T.[16] That stream of data includes, among other things, email, internet-messaging communications, web-browsing content, search-engine queries, and internet voice and video calls.
- **Stage 2: Filtering**. After the stream of data is copied, the NSA attempts to filter and eliminate wholly domestic communications. This filtering is only partially successful, however. As the FISC has stated, the NSA is unable to eliminate a significant number of wholly domestic communications, which therefore remain in the filtered stream of data.[17]

---

[13] *See NSA Slides Explain the PRISM Data Collection Program*, Wash. Post., July 10, 2013, http://wapo.st/158arbO.

[14] Claire Cain Miller, *Tech Companies Concede to Surveillance Program*, N.Y. Times, June 7, 2013, http://nyti.ms/1FlRcGv; *see* PCLOB Report at 33–34.

[15] Charlie Savage, *NSA Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1cez5ZK; *see generally* PCLOB Report at 35–41.

[16] *See* Siobhan Gorman & Jennifer Valentino DeVries, *New Details Show Broader NSA Surveillance Reach*, Wall St. J., Aug. 20, 2013, http://on.wsj.com/1usTArY (reporting that Verizon has installed intercepts to facilitate this surveillance in "the largest U.S. metropolitan areas"); PCLOB Report at 36–37.

[17] *[Redacted]*, 2011 WL 10945618, at *11–*12; *see also* PCLOB Report at 38 & n.140. For instance, a wholly domestic communication sent from one person in the United States to another may follow a path that takes the message outside the country while in transit, unbeknownst to either the sender or recipient. *See* President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* at 183 (Dec. 12, 2013), http://1.usa.gov/1be3wsO ("PRG Report").

- **Stage 3: Content Querying**. Once it has filtered out some purely domestic communications, the NSA queries the full contents of all the remaining communications, looking for any instance of its search terms. The search terms, known as "selectors," may include email addresses, phone numbers, domain names, and other identifiers the government believes to be associated with its foreign-intelligence targets.[18]
- **Stage 4: Retention and Use**. The copying and querying process described above produces tens of millions of search-term "hits" each year.[19] The NSA deposits all of those communications into its databases, where they are stored for future review, use, and dissemination, including in aid of criminal investigations.

Critically, under Upstream, the NSA's searches are not limited to communications sent or received by its targets. Rather, the NSA also engages in what is called "about" surveillance—*i.e.*, the NSA systematically examines the full text of every message in the filtered stream of data for *any* reference to a targeted selector. In this way, the NSA searches for and collects messages that are merely about its targets. The PCLOB has suggested that "about" surveillance is simply a technical byproduct of collecting communications that are to and from targets, *see* PCLOB Report at 38, but NSA documents indicate that the agency pursues this data in its own right.[20]

ARGUMENT

I. Surveillance conducted under the FAA violates the Fourth Amendment.

The FAA gives the government nearly unfettered access to U.S. persons' international communications. Whereas FISA authorizes the government to conduct relatively narrow surveillance of foreign agents and foreign powers, the FAA permits the government to monitor any international communication so long as the target of its surveillance is a foreigner abroad and a significant purpose of its surveillance is to acquire foreign-intelligence information. The statute violates the warrant clause because it allows the government to monitor U.S. persons'

[18] *See* PCLOB Report at 37–38.

[19] *[Redacted]*, 2011 WL 10945618, at *10 & n.26.

[20] *See* 2009 Targeting Procedures at 1 (discussing "cases where NSA seeks to acquire communications about the target that are not to or from the target"); *[Redacted]*, 2011 WL 10945618, at *5.

international communications without obtaining judicial approval based upon probable cause, and without describing the communications to be obtained with particularity. It also violates the reasonableness requirement. The Supreme Court has emphasized that a surveillance statute is reasonable only if it is precise and discriminate. The FAA is neither of these things.

A. American citizens and residents have a protected privacy interest in their international communications.

U.S. persons have a constitutionally protected privacy interest in the content of their emails and telephone calls. *Katz v. United States*, 389 U.S. 347, 353 (1967); *see also United States v. U.S. District Court (Keith)*, 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."); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The Fourth Amendment's protection extends not just to domestic communications but to international ones as well. *See, e.g.*, *United States v. Ramsey*, 431 U.S. 606, 616–20 (1977).[21]

B. The FAA permits surveillance of Americans' international communications in violation of the warrant requirement.

The Fourth Amendment requires that search warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Supreme Court has interpreted these words to require three things: (1) that any warrant be issued by a neutral, disinterested magistrate; (2) that those

[21] In defending the FAA, the government has claimed that "the privacy interests of U.S. persons in international communications are significantly diminished, if not completely eliminated, when those communications have been transmitted to or obtained from non-U.S. persons located outside the United States." Gov't Unclassified Mem. at 35, *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo. May 9, 2014) (ECF No. 559) ("Gov't Muhtorov Br."). But that argument contradicts the position the government has taken before the FISC, where it has conceded that Americans have a privacy interest in the same kinds of communications that it collects under the FAA. *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B*, No. 105B(g): 07-01, at 55–56 & n.56 (FISC Apr. 25, 2008), http://bit.ly/1vE3Lgt.

seeking the warrant demonstrate to the magistrate there is probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense; and (3) that any warrant particularly describe the things to be seized as well as the place to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979).

The FAA authorizes the executive branch to conduct electronic surveillance without complying with any of these three requirements; accordingly, the statute is presumptively unconstitutional. *See Katz*, 389 U.S. at 357 (warrantless searches and seizures are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions"); *Chimel v. California*, 395 U.S. 752, 768 (1969).[22]

First, the FAA fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Katz*, 389 U.S. at 357 (internal quotation marks omitted). While the government may not initiate an acquisition under the FAA without first applying for a mass-acquisition order from the FISC (or obtaining such an order within seven days of initiating the acquisition), the FISC's role is solely to review general procedures relating to targeting and minimization. Every decision relevant to the surveillance of specific targets is made by executive-branch employees and never presented to the FISC. Indeed, nothing in the FAA requires the government even to inform the FISC who its surveillance targets are, which facilities are to be monitored, or how many U.S. persons are likely to be implicated by the acquisition. The Fourth Amendment reflects a judgment that "[t]he right of privacy [is] too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of

[22] For the reasons set forth in this brief, the FAA violates the Fourth Amendment both on its face and as implemented. Upstream surveillance illustrates the severity of these warrantless intrusions: because it involves the bulk copying and scanning of internet traffic, Upstream surveillance effects both a mass "seizure" and "search" of non-target communications under the Fourth Amendment. *See* Pls.' Mot. for Partial Summary Judgment, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. July 25, 2014) (ECF No. 261).

criminals." *McDonald v. United States*, 335 U.S. 451, 455–56 (1948). But that is precisely what the FAA does: it entrusts to the unreviewed discretion of the executive branch decisions that affect the privacy rights of countless U.S. persons.

Second, the FAA fails to condition government surveillance on the existence of probable cause. It permits the government to conduct acquisitions without proving to a court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. *Compare* 18 U.S.C. § 2518(3) (Title III); 50 U.S.C. § 1805(a)(2) (FISA). It permits the government to conduct acquisitions without even making an administrative determination that its targets fall into any of these categories.

Third, the FAA fails to restrict the government's surveillance authority to matters described with particularity. The requirement of particularity "is especially great in the case of eavesdropping," as eavesdropping inevitably results in the interception of intimate conversations that are unrelated to the investigation. *Berger v. New York*, 388 U.S. 41, 56 (1967). Unlike Title III and FISA, however, the FAA does not require the government to identify to any court the individuals to be monitored. It does not require the government to identify the facilities, telephone lines, email addresses, places, or premises at which its surveillance will be directed. It does not limit the kinds of communications the government can acquire, beyond requiring that a programmatic purpose of the government's surveillance be to gather foreign intelligence. It does not require the government to identify "the particular conversations to be seized." *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). Nor, finally, does it place any reasonable limit on the duration of mass-acquisition orders. *See generally* 18 U.S.C. § 2518 (Title III); 50 U.S.C. §§ 1804(a), 1805 (FISA). The FAA simply does not ensure that surveillance conducted under the Act "will be carefully tailored." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

C. No exception to the warrant requirement applies.

1. The fact that the government is "targeting" people outside the United States does not render the warrant clause inapplicable when the government intercepts Americans' communications.

In defending the FAA, the government has argued that "incidental capture of a U.S. person's communications during surveillance that lawfully targets non-U.S. persons abroad" does not engage the warrant clause. Gov't Muhtorov Br. at 38.[23] But the rule the government cites—sometimes called the "incidental overhear" rule—has no application here.

First, the surveillance of Americans' communications under the FAA is not merely "incidental." Intelligence officials who advocated passage of the FAA—and the Protect America Act before it—indicated that their principal aim was to give the government broader authority to monitor Americans' international communications.[24] One cannot reasonably say that the surveillance of Americans' communications under the FAA is "incidental" when permitting such surveillance was the purpose of the Act. Nor can one reasonably say that the surveillance of Americans' international communications is "incidental" when the FAA allows large-scale collection and retention of those communications.[25] While the FAA prohibits "reverse targeting," the prohibition is narrow—it applies only if the surveillance targets a "particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2). Outside that narrow prohibition, the statute allows the government to conduct surveillance to collect Americans' international communications. And that is precisely how the government uses the statute: it has

[23] *See also* Gov't Unclassified Resp. at 28–31, *United States v. Mohamud*, No. 10-cr-00475 (D. Or. May 3, 2014) (ECF No. 509).

[24] *See, e.g.*, *FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. at 9 (2006), http://1.usa.gov/1kbgHm3 (statement of NSA Director Michael Hayden) (stating, with respect to the FAA's predecessor statute, that certain communications "with one end . . . in the United States" are the ones "that are most important to us").

[25] *See* PCLOB Report at 82 ("Such 'incidental' collection of communications is not accidental, nor is it inadvertent"); *id.* at 86.

acknowledged not only that it collects and stores Americans' communications, but that it frequently uses search terms associated with U.S. persons to sift through the millions of communications it has acquired without a warrant. *See* PCLOB Report at 59; Letter from Deirdre Walsh, ODNI, to Sen. Ron Wyden (June 27, 2014), http://1.usa.gov/V8lYTo.[26]

Second, the "incidental overhear" cases involve surveillance predicated on warrants—that is, they involved circumstances in which courts had found probable cause regarding the government's targets and had limited with particularity the facilities to be monitored. *See, e.g.*, *United States v. Kahn*, 415 U.S. 143 (1974); *United States v. Figueroa*, 757 F.2d 466 (2d Cir. 1985). The "incidental overhear" rule applies where a court has carefully circumscribed the government's surveillance and limited its intrusion into the privacy of third parties. *See United States v. Donovan*, 429 U.S. 413, 436 n.24 (1977) (holding that while a warrant is not made unconstitutional by "failure 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. Yannotti*, 399 F. Supp. 2d 268, 274 (S.D.N.Y. 2005); *see also* PCLOB Report at 95.

Surveillance conducted under the FAA is not similarly limited. Quite the opposite: the FAA does not require the government to establish probable cause or individualized suspicion of any kind concerning its targets; it does not require the government to identify to any court the facilities it intends to monitor; and it does not require the government to limit which communications it acquires. Surveillance is not particularized, and thus the rule of the "incidental overhear" cases cannot be extended to this context.

[26] The government's retention of these U.S. person communications for later searching—so-called "backdoor searches"—sets this case apart from the FISCR's decision in *In re Directives*, 551 F.3d 1004 (FISCR 2008). In that case, the FISC found it significant that the government was not amassing the database it is concededly amassing here, let alone querying that database for information about Americans. *Id.* at 1015 ("The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary.").

Third, the *volume* of communications intercepted "incidentally" in surveillance under the FAA differs dramatically from the volume of communications intercepted incidentally in surveillance conducted under original FISA or Title III. Unlike original FISA and Title III, the FAA allows the government to monitor individuals without regard to whether those individuals are suspected criminals or foreign agents. PCLOB Report at 116 ("[T]he expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications."). Under the government's theory, the statute even allows the NSA to scan millions of people's communications for information "about" the government's targets. *See* Background § D.2, *supra*. The government's use of the term "incidental" is meant to convey the impression that its collection of Americans' communications under the FAA is a *de minimis* byproduct common to all forms of surveillance. But whereas surveillance under Title III or the original FISA might lead to the incidental collection of a handful of people's communications, surveillance under the FAA invades the privacy of tens of thousands or even millions of people.[27]

The government's effort to stretch the incidental overhear doctrine to cover its dragnet collection of Americans' communications reflects a view that constitutional rules and exceptions designed for an era of individualized surveillance can be applied blindly to broad programs of suspicionless surveillance. This view is wrong.[28] *See Riley v. California*, 134 S. Ct. 2473, 2488

[27] *See [Redacted]*, 2011 WL 10945618, at *27 (observing that "the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial"); *id.* at *26; PRG Report at 149 ("incidental interception is significantly more likely to occur when the interception takes place under section 702 than in other circumstances").

[28] The government has also argued that the border-search and third-party doctrines excuse FAA surveillance from the warrant requirement, but neither argument is supportable. *See* Def. Reply at 17–18, *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo. July 3, 2014) (ECF No. 602).

(2014) ("That is like saying a ride on horseback is materially indistinguishable from a flight to the moon."); *United States v. Jones*, 132 S. Ct. 945, 954 & n.6 (2012) (recognizing that the broad collection of data raises different constitutional questions).[29]

2. If there is a foreign-intelligence exception to the warrant requirement, the exception is not broad enough to render the FAA constitutional.

In other contexts the government has contended, citing the "special needs" doctrine, that surveillance conducted for foreign-intelligence purposes is not subject to the warrant requirement. *See, e.g.*, Gov't Muhtorov Br. at 41–42. This is incorrect. Courts recognize an exception to the warrant requirement only "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring); *see Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987).

The mere fact that the government's surveillance is conducted for foreign-intelligence purposes does not render the warrant and probable cause requirements unworkable. In *Keith*, the Supreme Court expressly rejected the government's argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316–21. The Court's logic applies with equal force to surveillance directed at targets with a foreign nexus—at least when that surveillance sweeps up U.S. persons' communications (as surveillance conducted under the FAA does), and is conducted inside the United States (as surveillance conducted under the FAA is).[30] History shows, too, that the courts are capable of overseeing foreign-intelligence

[29] The district court in *United States v. Mohamud* erred in finding that incidental collection under the FAA does not "differ sufficiently from previous foreign intelligence gathering to distinguish prior case law"—a finding upon which the court based its conclusion that the FAA "does not trigger the warrant clause." *See* No. 3:10-CR-00475, 2014 WL 2866749, at *15 (D. Or. June 24, 2014).

[30] *See also Zweibon v. Mitchell*, 516 F.2d 594, 613–14 (D.C. Cir. 1975) (stating in dicta that "we believe that an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional"); S.

surveillance of U.S. persons' communications: since 1978, the FISC has granted more than 33,000 applications to conduct foreign-intelligence surveillance.[31]

Moreover, even if the foreign-intelligence context may justify an exception to the warrant and probable-cause requirements, that exception is not broad enough to render FAA surveillance constitutional. Courts have approved a modification to the probable-cause requirement when considering individualized surveillance under traditional FISA, as the Second Circuit did in *United States v. Duggan*, 743 F.2d 59, 73–74 (2d Cir. 1984). Yet the Second Circuit has declined to adopt a blanket foreign-intelligence exception to the Fourth Amendment. *See In re Terrorist Bombings*, 552 F.3d 157, 172 (2d Cir. 2008). Indeed, the courts that have recognized a foreign-intelligence exception have defined that exception very narrowly. They excused the government from compliance with the warrant requirement only where the surveillance in question was directed at foreign powers or their agents and predicated on an individualized finding of suspicion. *See, e.g.*, *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002); *Bin Laden*, 126 F. Supp. 2d at 277. They also required that the surveillance be personally approved by the President or Attorney General. *See, e.g.*, *id*.

The Foreign Intelligence Surveillance Court of Review's decision in *In re Directives*, 551 F.3d 1004 (FISCR 2008), only underscores these crucial limitations. That case addressed the constitutionality of surveillance conducted under the PAA, Executive Order 12,333, and certain Defense Department regulations. In its analysis, the FISCR emphasized again and again that, "[c]ollectively, these procedures require a showing of particularity, a meaningful probable cause

---

Rep. No. 95-701 at 15, *reprinted at* 1978 U.S.C.C.A.N. 3973, 3984 (stating that the arguments in favor of prior judicial review "apply with even greater force to foreign counterintelligence surveillance"); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 272, 274 nn.8–9 (S.D.N.Y. 2000).

[31] *See, e.g.*, Foreign Intelligence Surveillance Act Orders 1979–2014, Elec. Privacy Info Ctr., http://bit.ly/LoZqZG.

determination, and a showing of necessity." *Id.* at 1016; *see id.* at 1007, 1013–14. Thus, while the FISCR recognized a foreign-intelligence exception, that exception was narrow:

> [W]e hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance 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.

551 F.3d at 1012 (emphasis added). Indeed, the exception approved by the FISCR was premised on an individualized finding of probable cause certified by the Attorney General himself.

The FAA contains none of these limitations—it would require a foreign-intelligence exception far broader than the one recognized by the FISCR or any other court. Surveillance under the FAA is not directed only at "foreign powers or agents of foreign powers reasonably believed to be located outside the United States," but may be directed at any non-citizen located outside the United States. Nor does the FAA require that surveillance targets be personally approved by the President or the Attorney General; that responsibility has been handed off to dozens of lower-level NSA analysts. In short, no court has ever recognized a foreign-intelligence exception sweeping enough to render constitutional the surveillance at issue here.[32]

D. Surveillance under the FAA violates the Fourth Amendment's reasonableness requirement.

The FAA would be unconstitutional even if the warrant clause were inapplicable because the surveillance the statute authorizes is unreasonable. "The ultimate touchstone of the Fourth Amendment is reasonableness," and the reasonableness requirement applies even where the warrant requirement does not. *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006); *Figueroa*, 757 F.2d at 471–73 (Title III); *Duggan*, 743 F.2d at 73–74 (FISA). Reasonableness is determined by examining the "totality of the circumstances" to "assess[], on the one hand, the degree to

[32] *See* PCLOB Report at 90 n.411 (acknowledging that "it is not necessarily clear that the Section 702 [FAA] program would fall within the *scope* of the foreign-intelligence exception recognized by [earlier] decisions").

which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted).

1. The FAA lacks the indicia of reasonableness that courts routinely rely upon when assessing the legality of electronic surveillance.

In the context of electronic surveillance, reasonableness requires that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions of privacy." *Berger*, 388 U.S. at 58; *see United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973) ("[W]e must look . . . to the totality of the circumstances and the overall impact of the statute to see if it authorizes indiscriminate and irresponsible use of electronic surveillance or if it authorizes a reasonable search under the Fourth Amendment."). Courts that have assessed the lawfulness of electronic surveillance have looked to FISA and Title III as measures of reasonableness. *See, e.g.*, *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986) (video surveillance). While the limitations on foreign-intelligence surveillance may differ in some respects from those applicable to law-enforcement surveillance, *see Keith*, 407 U.S. at 323–24, "the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns," *In re Sealed Case*, 310 F.3d at 737.

By abandoning all the core requirements of the warrant clause—individualized suspicion, prior judicial review, and particularity—the FAA eliminates the primary protections against general surveillance. Whereas both FISA and Title III require the government to identify to a court its targets and the facilities it intends to monitor, the FAA does not. Whereas both FISA and Title III require the government to demonstrate individualized suspicion to a court, the FAA does not. (Indeed, the FAA does not require even an administrative finding of individualized suspicion.) And, whereas both FISA and Title III impose strict limitations on the nature of the

communications that the government may monitor and the duration of its surveillance, the FAA does not. The FAA's failure to include these basic safeguards is fatal, because these are the very safeguards that the courts have cited in upholding the constitutionality of both FISA and Title III. *See, e.g.*, *Duggan*, 743 F.2d at 73 (FISA); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (FISA); *In re Sealed Case*, 310 F.3d at 739–40 (FISA); *United States v. Falvey*, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (FISA); *United States v. Tortorello*, 480 F.2d 764, 773–74 (2d Cir. 1973) (Title III).

The consequence of the FAA's failure to include any of these limitations is that the government may target essentially any foreigner for surveillance—and may thereby collect the phone calls, emails, and text messages of all U.S. persons communicating with those foreigners. The government has acknowledged that it targeted 89,138 such individuals or groups in 2013. *See* note 5, *supra*. The scope of this surveillance is a radical departure from both Title III, where the government's targets must be criminal suspects, *see* 18 U.S.C. § 2518(1), (3), and FISA, where the surveillance targets must be agents of a foreign power, *see* 50 U.S.C. § 1804(3). The FAA's sweeping authorization ensures that the communications of countless innocent U.S. persons will be monitored.

2. The government's targeting and minimization procedures fail to make FAA surveillance reasonable, and instead exacerbate the statute's defects.

The targeting and minimization procedures used by the government magnify the statute's flaws by allowing the government to collect, retain, and disseminate U.S. persons' international communications in vast quantity in the course of surveillance directed at foreign targets. For example, the targeting procedures allow the government to search literally every communication going into or out of the United States for information "about" the NSA's targets, so long as the NSA uses "an Internet Protocol filter to ensure that" one of the parties to the communication "is

located overseas."[33] Those same procedures also reveal that the factors NSA analysts consider when determining whether a particular email address or phone number will be used to communicate foreign-intelligence information are incredibly broad—broad enough to make essentially any foreign person a viable target. *See* 2009 Targeting Procedures at 4–5.

For all those U.S. persons who communicate with the tens of thousands foreigners monitored under the FAA, the sole safeguard is the requirement that the government "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1); *see* 50 U.S.C. § 1881a(e). But the minimization procedures, too, fail to provide meaningful protection:

- Rather than requiring the government to segregate or destroy any U.S.-person communications acquired without a warrant, the procedures explicitly permit the NSA to retain and disseminate U.S. persons' international communications if "necessary to understand foreign intelligence information or assess its importance," or for almost a dozen other reasons. 2011 Minimization Procedures § 6(a)(2), 6(b).
- The procedures permit the government to retain wholly domestic communications acquired through the inadvertent targeting of U.S. persons if the government determines that the communications contain "significant foreign intelligence information" or "evidence of a crime." *Id.* § 5(1)–(2).
- The procedures permit the government to retain—for up to five years—even those U.S.-person communications that do not contain foreign intelligence or evidence of a crime. *Id.* § 3(b)(1), 3(c)(1).
- While the procedures ostensibly require the government to destroy—or "minimize"—U.S.-person communications that do not meet one of the enumerated criteria upon recognition, *id.* § 3(c), that requirement has little or no force in practice.[34]

The minimization procedures also permit the government to conduct so-called "backdoor searches," in which the government later searches its repository of FAA-collected

[33] 2009 Targeting Procedures at 1–2; *see also* Savage, *supra* note 15.

[34] For example, *The Washington Post* has reported that the NSA's "policy is to hold on to 'incidentally' collected U.S. content, even if it does not appear to contain foreign intelligence." Gellman et al., *supra* note 4; *see also id.* (reporting that "the NSA does not generally attempt to remove irrelevant personal content, because it is difficult for one analyst to know what might become relevant to another.")

communications specifically for information about U.S. citizens and residents—like Mr. Hasbajrami—including for evidence of criminal activity. *See* PCLOB Report at 59; 2011 Minimization Procedures § 3(b)(6).[35] These kinds of queries are an end-run around the Fourth Amendment, because they convert sweeping warrantless surveillance directed at foreigners into a tool for investigating Americans in ordinary criminal investigations. The President's Review Group has recommended prohibiting the practice of backdoor searches, concluding that the practice violates the "full protection of [Americans'] privacy," *see* PRG Report at 149, 145–50; and, in June 2014, the House of Representatives voted to prohibit such searches.[36]

The FAA's targeting and minimization requirements—in permitting nearly unfettered surveillance of U.S. persons' international communications—bear little resemblance to the procedures in place under Title III and FISA. *See, e.g.*, *In re Sealed Case*, 310 F.3d at 740–41 (stating that courts have found FISA's minimization requirements to be "constitutionally significant"); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *Duggan*, 743 F.2d at 74; *United States v. Turner*, 528 F.2d 143, 156 (9th Cir. 1975) (finding Title III constitutional because "measures [must] be adopted to reduce the extent of . . . interception [of irrelevant or innocent communications] to a practical minimum"); *Figueroa*, 757 F.2d at 471.

Title III requires the government to conduct surveillance "in such a way as to minimize the interception of" innocent and irrelevant conversations, 18 U.S.C. § 2518(5), and strictly limits the use and dissemination of material obtained under the statute, *see* 18 U.S.C. § 2517. FISA similarly requires the government to minimize the acquisition, retention, and dissemination

[35] Warrantless backdoor searches were once prohibited by the government's minimization procedures, but the prohibition was lifted in 2011. *See* Ellen Nakashima, *Obama Administration Had Restrictions on NSA Reversed in 2011*, Wash. Post, Sept. 7, 2013, http://wapo.st/1hP9FWm.

[36] *See* Charlie Savage, *House Votes to Curb NSA Scrutiny of Americans' Communications*, N.Y. Times, June 20, 2014, http://nyti.ms/1vh2zti.

of non-publicly available information concerning U.S. persons. *See* 50 U.S.C. § 1801(h). It requires that each order authorizing surveillance of a particular target contain specific minimization procedures that will govern that particular surveillance. *See* 50 U.S.C. § 1804(a)(4); 50 U.S.C. § 1805(a)(3); 50 U.S.C. § 1805(c)(2)(A). FISA also provides the FISC with authority to oversee the government's minimization on an individualized basis during the course of the actual surveillance. *See* 50 U.S.C. § 1805(d)(3); *see also* 18 U.S.C. § 2518(6). Thus, under FISA, minimization is applied to every individual surveillance target, and, equally important, minimization is judicially supervised during the course of the surveillance. *See* Kris & Wilson § 9:1–2. Neither is true of FAA surveillance.

The FAA's meager minimization provisions are especially problematic because the FAA does not provide for individualized judicial review at the acquisition stage. Under FISA and Title III, minimization operates as a second-level protection against the acquisition, retention, and dissemination of information relating to U.S. persons. The first level of protection comes from the requirement of individualized judicial authorization for each specific surveillance target. *Cf. Scott v. United States*, 436 U.S. 128, 130–31 (1978) ("'The scheme of the Fourth Amendment becomes meaningful only when it is assured that at some point the conduct of those charged with enforcing the laws can be subjected to the more detached, neutral scrutiny of a judge who must evaluate the reasonableness of a particular search or seizure in light of the particular circumstances.'" (quoting *Terry v. Ohio*, 392 U.S. 1 (1968))); *United States v. James*, 494 F.2d 1007, 1021 (D.C. Cir. 1974) ("The most striking feature of Title III is its reliance upon a judicial officer to supervise wiretap operations. Close scrutiny by a federal or state judge during all phases of the intercept, from the authorization through reporting and inventory, enhances the protection of individual rights." (quotation marks omitted)); *Cavanagh*, 807 F.2d at 790.

Under the FAA, by contrast, there is no first-level protection, because the statute does not call for individualized judicial authorization of specific surveillance targets (or, for that matter, of specific facilities to be monitored). Unlike FISA and Title III, the FAA permits dragnet surveillance of Americans' international telephone calls and emails. In this context, minimization requirements should be at least as stringent as they are in the context of FISA surveillance of facilities used exclusively by foreign powers or their agents. *See* 50 U.S.C. § 1801(h)(4).

3. The government has reasonable alternatives that would allow it to collect foreign intelligence while protecting Americans' international communications from warrantless invasions.

The government has reasonable alternatives at its disposal. Compliance with the warrant clause requires at least two things: that the government avoid warrantless acquisition of Americans' international communications where it is reasonably possible to do so, and that it avoid warrantless review of Americans' communications when it collects them inadvertently or incidentally. There is no practical reason why these limitations—which have the effect of requiring a warrant *only* for Americans' communications—could not be imposed here.[37]

Indeed, a number of reform proposals would permit the government to continue collecting foreign-to-foreign communications while providing additional protections for communications involving U.S. persons. During the debate that preceded the passage of the FAA, then-Senator Barack Obama co-sponsored an amendment that would have codified these limitations by prohibiting the government from (1) acquiring a communication without a warrant

[37] The NSA could easily implement these limitations. The government already filters out Americans' wholly *domestic* communications using addressing information, like US-based IP addresses, and other technical methods. *See* PCLOB Report at 38. The government could apply similar filters to exclude Americans' international communications. It could also exclude from its collection any communications sent or received by accounts, addresses, or identifiers that it separately has reason to believe are associated with U.S. persons. The NSA apparently maintains a list of such accounts, addresses, and identifiers to prevent targeting errors; there is no reason that it could not do the same to protect Americans' privacy more fully. 2009 Targeting Procedures at 3.

if it knew "before or at the time of acquisition that the communication [was] to or from a person reasonably believed to be located in the United States," and (2) accessing Americans' communications collected under the FAA without a warrant. *See* S.A. 3979, 110th Cong. (2008). More recently, the President's Review Group concluded that a warrant requirement should be imposed, and the House of Representatives passed a bill that would impose one. *See* PRG Report at 28–29; H.R. 4870, 113th Cong. § 8127 (2014).

The government has argued that complying with the warrant requirement would be unworkable because "imposition of a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection." Gov't Muhtorov Br. at 39. But this is a red herring. The Fourth Amendment does not require the government to obtain prior judicial authorization for surveillance of foreign targets merely because those foreign targets might, at some unknown point, communicate with U.S. persons. Rather, the Fourth Amendment requires the government to take reasonable steps to avoid the warrantless interception, retention, and use of Americans' communications. FAA surveillance lacks even basic protections that would prevent these warrantless intrusions—as a consequence, it is unreasonable.

CONCLUSION

For the foregoing reasons, the FAA violates the Fourth Amendment on its face and as implemented, and thus the government's surveillance of Mr. Hasbajrami was unconstitutional. *Amici* thank the Court again for the opportunity to submit this brief and will make themselves available for argument should the Court conclude that *amici*'s participation would be helpful.

Dated: December 5, 2014
New York, New York

Respectfully submitted,

/s/ Patrick Toomey
Patrick Toomey

Jameel Jaffer
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Amici Curiae

Hanni Fakhoury
Mark Rumold
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993

Of Counsel