NO. 14-30217

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

MOHAMED OSMAN MOHAMUD,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the District of Oregon
Case No. 3:10-cr-00475-KI-1
Honorable Garr M. King, Senior District Judge

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF OREGON, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT

Counsel for Amici Curiae
Patrick Toomey
Jameel Jaffer
Alex Abdo
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
jjaffer@aclu.org
aabdo@aclu.org

Of Counsel
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
mark@eff.org
andrew@eff.org

Of Counsel
Mathew W. dos Santos
AMERICAN CIVIL LIBERTIES UNION OF OREGON FOUNDATION
P.O. Box 40585
Portland, OR 97240
Phone: (503) 227-6928
MdosSantos@aclu-or.org

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, *amici curiae* state that no party to this brief is a publicly held corporation, issues stock, or has a parent corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Constitutional Provisions

Legislative Materials

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The 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. The ACLU has appeared before the federal courts in many cases involving the Fourth Amendment, including cases concerning foreign-intelligence surveillance. The ACLU represented the plaintiffs in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), and is currently counsel in *Wikimedia v. NSA*, No. 15-cv-00662 (D. Md.), and *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo.).

The American Civil Liberties Union of Oregon ("ACLU of Oregon") is a nonprofit, nonpartisan organization with over 10,000 members dedicated to the principles embodied in the Bill of Rights. The ACLU of Oregon has appeared as *amicus curiae* in cases involving the Fourth Amendment and foreign-intelligence gathering, including *Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010), and *United States v. Battle*, 2007 WL 3341740 (D. Or. Nov. 9, 2007).

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization working to protect innovation, free speech, and privacy in the

[1] No party or party's counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than *amici*, their members, and their counsel contributed money to fund the preparation or submission of this brief. All parties consent to the filing of this brief.

online world. With nearly 22,000 members, EFF represents the interests of technology users in court cases and 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.); and *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 671 F.3d 881 (9th Cir. 2011).

INTRODUCTION

In this criminal prosecution, the government notified the defendant—belatedly, after trial—that it relied on 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 this law and the manner in which it 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' international 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.

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 federal intelligence agencies. 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 decades, the intelligence agencies had "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 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. FISA generally required the government to obtain an individualized order from the newly created Foreign Intelligence Surveillance Court ("FISC") before conducting electronic

surveillance on U.S. soil. *See* 50 U.S.C. §§ 1805, 1809(a)(1). To obtain a traditional FISA order, the government was required to demonstrate "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," and that "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 subsequently 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 ultimately embodied in the FAA. 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 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 the communication is a foreigner located abroad. In particular, the FAA permits the Attorney General and Director of National Intelligence to authorize "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 or to counterterrorism purposes. The targets may be any foreigner abroad, and "foreign intelligence information" is defined extremely broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* 50 U.S.C. § 1801(e).

No court ever approves the targets of this surveillance. Instead, the FISC's role consists principally of reviewing the general procedures the government uses in carrying out its surveillance: the "targeting" and "minimization" procedures. *See id.* § 1881a(i), (d)–(g). These procedures govern who may be targeted for

surveillance by executive-branch employees and how communications are to be handled once intercepted.

A crucial difference between the FAA and traditional FISA is that the FAA authorizes surveillance *without* probable cause or individualized suspicion. The government need not demonstrate 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. Similarly, the FAA does not require the government to identify the specific "facilities, places, premises, or property at which" its surveillance will be directed. 50 U.S.C. § 1881a(g)(4). The government may even direct its surveillance at "gateway" switches, which carry the communications of millions of people, rather than at individual telephone lines or email accounts.[2] As a result, a single FISC order authorizing FAA surveillance may result in the acquisition of the communications of thousands of individuals for up to a year at a time.

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-

[2] David S. Kris & J. Douglas Wilson, 1 *National Security Investigations and Prosecutions* § 16.12, 577 (2d ed. 2012).

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 minimization requirement is supposed to protect against the collection, retention, and dissemination of Americans' communications that are intercepted "incidentally" or "inadvertently." Significantly, however, this provision 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.

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.[3] The government reported that in 2014 it monitored the communications of 92,707 targets under a single order issued by the FISC.[4] In 2011, FAA surveillance

[3] *See* 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.

[4] ODNI, 2014 Statistical Transparency Report at 1 (Apr. 22, 2015), http://1.usa.gov/1JFUMll.

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.[5] 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.[6]

The targeting and minimization rules that supposedly protect the privacy of U.S. persons are weak and riddled with exceptions. These rules give the government broad latitude to review, use, and disseminate the communications it collects, including searching that data for information about Americans in unrelated criminal investigations.[7]

---

[5] *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*).

[6] *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 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/1FJat9g ("PCLOB Report").

[7] The government has officially disclosed the minimization procedures the NSA used to implement the FAA in 2011. *Minimization Procedures Used by the NSA* (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

Official disclosures indicate that the government conducts two types of surveillance under the FAA: "PRISM" surveillance and "Upstream" surveillance.[8] The government has refused to identify which it relied upon in this prosecution.

1. PRISM Surveillance

PRISM surveillance involves the acquisition of stored and real-time communications directly from U.S. companies like Google, Facebook, and Microsoft.[9] The government identifies the user accounts it wishes to monitor—for example, particular Microsoft 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.[10]

2. Upstream Surveillance

Upstream surveillance operates very differently. It involves the NSA copying and searching entire streams of internet traffic as that data flows across

---

FISC in 2009. *See Procedures Used by the NSA for Targeting* (July 28, 2009), http://bit.ly/1rf78HV ("2009 Targeting Procedures").

[8] *See* PCLOB Report 33–41.

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

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

major networks inside the United States.[11] The NSA reportedly copies "most e-mails and other text-based communications that cross the border."[12] Upstream surveillance can be understood as encompassing the following processes, some of which are implemented by telecommunications providers at the NSA's direction:

- **Copying**. Using surveillance devices installed at key access points, the NSA makes a copy of substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. The copied traffic includes emails, web-browsing content, and search-engine queries.

- **Filtering**. The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, while preserving international communications. The filtering is only partially successful, however—subjecting a substantial number of wholly domestic communications to warrantless surveillance.[13]

- **Content Review**. The NSA reviews the copied communications—including their full content—for instances of its search terms.[14] The search terms, called "selectors," include email addresses, phone numbers, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets.

- **Retention and Use**. The NSA retains all communications that contain selectors associated with its targets, as well as those bundled with them in transit—totaling tens of millions of communications each

[11] *See* Siobhan Gorman & Jennifer Valentino-DeVries, *New Details Show Broader NSA Surveillance Reach*, Wall St. J., Aug. 20, 2013, http://on.wsj.com/1usTArY; *see generally* PCLOB Report 35–41.

[12] Charlie Savage, *NSA Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1cez5ZK.

[13] *See [Redacted]*, 2011 WL 10945618, at *11–12; PCLOB Report 38.

[14] *See* PCLOB Report 37–39.

> year.[15] NSA analysts may read, query, and data-mine these communications with few restrictions, and they may share the results of those efforts with the FBI, including in aid of criminal investigations.

Critically, Upstream surveillance is not limited to communications sent or received by the NSA's targets. Rather, the NSA also engages in what is called "about" surveillance—that is, the NSA examines essentially *everyone's* communications to determine whether they contain the NSA's search terms.[16] Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets; nor does it later purge those communications.

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 spy on foreign agents and foreign powers, the FAA permits monitoring of 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

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

[16] *See* PCLOB Report 37, 111 n.476; 2009 Targeting Procedures 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.

the government to monitor U.S. persons' 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.

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. *See Katz v. United States*, 389 U.S. 347, 353 (1967); *United States v. U.S. District Court ("Keith")*, 407 U.S. 297, 313 (1972); *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).

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 the government demonstrate probable cause to believe that the evidence sought will aid in a particular apprehension or conviction; and (3) that any warrant particularly describe the things to be seized and the places 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).[17]

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 (quotation marks omitted). While the government may not conduct surveillance under the FAA without seeking an order from the FISC, 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 solely by executive-branch employees. The Fourth Amendment reflects a judgment that "[t]he right of privacy

[17] For the reasons set forth in this brief, the FAA violates the Fourth Amendment both on its face and as implemented. Indeed, Upstream surveillance—which involves the bulk seizing and searching of internet traffic—illustrates just how broadly the statute has been implemented.

[is] too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of 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 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, or places at which its surveillance will be directed. Nor, finally, does it

require the government to identify "the particular conversations to be seized." *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). 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 upholding the FAA, the district court found that incidental collection of a U.S. person's communications during surveillance targeting non-U.S. persons abroad did not engage the warrant clause at all. Dist. Ct. Op. 26–27 (I:197–98). But the rule the district court cited—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 indicated that their principal aim was to give the government broader authority to monitor Americans' international communications.[18] One cannot reasonably say that the warrantless surveillance of Americans' communications under the FAA is

[18] *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").

"incidental" when permitting such surveillance was both the purpose and the direct result of the Act.[19] Outside a narrow prohibition on the "reverse targeting" of U.S. persons, *see* 50 U.S.C. § 1881a(b)(2), the statute allows the government to collect Americans' international communications. And the government uses it for precisely that: to collect and store Americans' communications, and to routinely search through the millions of communications it collects for information about U.S. persons. *See* PCLOB Report 59.[20]

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 Donovan*,

[19] *See* PCLOB Report 82, 86–87 ("Such 'incidental' collection of communications is not accidental, nor is it inadvertent").

[20] 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 FISCR found it significant that the government was not amassing the database it is concededly amassing here. *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."); *see [Redacted]*, 2011 WL 10945618, at *27 n.67 (distinguishing *In re Directives*).

429 U.S. at 436 n.24 (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); PCLOB Report 95.

Surveillance conducted under the FAA is not similarly limited. Quite the opposite: the FAA does not require the government to establish 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.

Third, the *volume* of communications intercepted "incidentally" under the FAA dwarfs that of communications intercepted incidentally under original FISA or Title III. Indeed, the findings of the President's Review Group, the FISC, and the PCLOB all contradict the district court's opinion on this key point.[21] The scale

[21] *Compare* Dist. Ct. Op. 27 (I:198), *with, e.g.*, President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* at 149 (2013), http://1.usa.gov/1be3wsO ("PRG Report") ("incidental interception is significantly more likely to occur when the interception takes place under section 702 than in other circumstances"); *[Redacted]*, 2011 WL 10945618, at *26–27 (observing that "the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream

of incidental collection is a direct consequence of the FAA's suspicionless targeting standard: "[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." PCLOB Report 116. Under the government's theory, the statute even allows the NSA to review the contents of millions of Americans' communications for information "about" the government's targets using Upstream surveillance. *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 Americans. The district court thus erred as a matter of fact 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." Dist. Ct. Op. 27 (I:198).

---

collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial").

The government's effort to stretch the incidental overhear doctrine to cover its dragnet surveillance of Americans' communications reflects a view that constitutional rules designed for an era of individualized surveillance can be applied blindly to broad programs of suspicionless surveillance. This view is wrong.[22] *See Riley v. California*, 134 S. Ct. 2473, 2488 (2014) (refusing to extend rules for physical searches to digital contents of cell phones); *United States v. Jones*, 132 S. Ct. 945, 954 & n.6 (2012) (recognizing that broad collection of data raises different constitutional questions).

2. If There Is a Foreign-Intelligence Exception to the Warrant Requirement, the Exception Is Not Broad Enough to Render the FAA Constitutional.

The government argues that the warrant requirement does not apply here because FAA surveillance serves a foreign-intelligence purpose and therefore falls within the "special needs" doctrine. *See* Gov't Unclassified Resp. 32–34 (VII:3239–41). 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).

[22] 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 17–18, *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo. July 3, 2014) (ECF No. 602).

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 FAA surveillance does), and is conducted inside the United States (as FAA surveillance is).[23]

Moreover, even if there is a foreign-intelligence exception to the warrant requirement, 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 this Court did in *United States v. Cavanagh*, 807 F.2d 787, 790–91 (9th Cir. 1987). But the courts have defined any exception very narrowly. They excused the government from the ordinary 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.*, *id.*; *United States v. Duka*, 671 F.3d

[23] *See Zweibon v. Mitchell*, 516 F.2d 594, 613–14 (D.C. Cir. 1975); S. Rep. No. 95-701 at 15 (1978), *reprinted in* 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 n.9 (S.D.N.Y. 2000).

329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002); *Bin Laden*, 126 F. Supp. 2d at 277 (S.D.N.Y.). They also required that the surveillance be personally approved by the President or Attorney General. *See, e.g.*, *id.*; *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977).

The Foreign Intelligence Surveillance Court of Review's ("FISCR") 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 Protect America Act, Executive Order 12,333, and Defense Department regulations. In its analysis, the FISCR emphasized that, "[c]ollectively, these procedures require a showing of particularity, a meaningful probable cause 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). Moreover, the exception was premised on a probable-cause determination certified by the Attorney General himself.

The FAA contains none of these limitations. 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," *id.*, but may be directed at any non-citizen outside the United States. Nor does the FAA require that 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. *See* PCLOB Report 90 n.411.

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); *cf. Cavanagh*, 807 F.2d at 789–90 (FISA). Reasonableness is determined by examining the "totality of the circumstances" to "assess[], on the one hand, the degree to 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). 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); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992). While the limitations on foreign-intelligence surveillance may differ in some respects from those applicable to law-enforcement surveillance, "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 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.*, *Cavanagh*, 807 F.2d at 790 (FISA); *In re Sealed Case*, 310 F.3d at 739–40 (FISA); *United States v. Turner*, 528 F.2d 143, 158–59 (9th Cir. 1975) (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 emails and phone calls of all U.S. persons communicating with those foreigners. 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).

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." 2009 Targeting Procedures 1–2. Those same procedures also reveal that the factors NSA analysts consider when determining whether a particular email or telephone account will be used to communicate foreign-intelligence information are incredibly broad—broad enough to make essentially any foreign person a viable target. *See id.* 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 for almost a dozen 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 as long as five years—even those U.S.-person communications that do not contain *any* 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.[24]

The minimization procedures also permit the government to conduct so-called "backdoor searches," in which the government searches its repository of FAA-collected communications specifically for information about U.S. citizens and residents—like Mr. Mohamud—including for evidence of criminal activity. *See* PCLOB Report 59; 2011 Minimization Procedures § 3(b)(6). These kinds of queries are an end-run around the Fourth Amendment, converting sweeping warrantless surveillance directed at foreigners into a tool for investigating Americans in ordinary criminal investigations. *See* Br. of Appellant 197–200. The President's Review Group has recommended prohibiting the practice of backdoor searches, concluding that the practice violates the "full protection of [Americans'] privacy," PRG Report 149, 145–50.

The FAA's targeting and minimization requirements—in permitting nearly unfettered surveillance of U.S. persons' international communications—fall far

[24] 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 3.

short of the protections in place under Title III and FISA. *See, e.g.*, *Turner*, 528 F.2d at 156 (finding Title III constitutional because "measures [must] be adopted to reduce the extent of . . . interception [of irrelevant or innocent communications] to a practical minimum"); *In re Sealed Case*, 310 F.3d at 740–41.

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 id.* § 2517. FISA similarly requires that each order authorizing surveillance of a particular target contain minimization procedures tailored to that particular surveillance, *see* 50 U.S.C. §§ 1805(a)(3), 1805(c)(2)(A), and 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). Thus, under FISA and Title III, minimization is applied to every individual surveillance target, and, equally important, minimization is judicially supervised during the course of the surveillance. *See id.*; 18 U.S.C. § 2518(6). 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. *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 the facilities to be monitored). In this context, minimization requirements should be at least as stringent as they are in the context of those exceptional instances where FISA surveillance is permitted without an individualized court order. *See* 50 U.S.C. §§ 1801(h)(4), § 1802(a) (requiring significantly heightened protections for U.S. persons).

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 one of two things: that the government avoid warrantless *acquisition* of Americans' international communications where it is reasonably possible to do so, or 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.[25]

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 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), 154 Cong. Rec. S607–08 (daily ed. Feb. 4, 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 28–29; H.R. 4870, 113th Cong. § 8127 (2014).

[25] The NSA could readily implement more protective measures. It could adopt more stringent filtering methods to exclude Americans' international communications in the first place wherever possible, similar to its existing efforts to exclude wholly domestic communications and to avoid targeting errors. *See* PCLOB Report 38; 2009 Targeting Procedures 3. At the same time, it could impose far stricter limitations on the querying, accessing, and use of any American communications captured incidentally or inadvertently without a warrant.

The government argued below 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 Unclassified Resp. 30 (VII:3237). 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. The Court should hold that the surveillance of Mr. Mohamud was unconstitutional.

Dated: June 3, 2015

Respectfully submitted,

/s/ Patrick Toomey

Patrick Toomey
Jameel Jaffer
Alex Abdo
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

Of Counsel:
Mathew W. dos Santos
AMERICAN CIVIL LIBERTIES
UNION OF OREGON FOUNDATION
P.O. Box 40585
Portland, OR 97240
Phone: (503) 227-6928
MdosSantos@aclu-or.org

Of Counsel:
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

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amici Curiae* American Civil Liberties Union, American Civil Liberties Union of Oregon, and Electronic Frontier Foundation In Support of Defendant-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,982 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: June 3, 2015

/s/ Patrick Toomey
Patrick Toomey

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on June 3, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: June 3, 2015

/s/ Patrick Toomey
Patrick Toomey

Counsel for Amici Curiae