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
m (.org) 2Mkhahanni@F

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

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*

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

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)

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

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*

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.

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

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-

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

[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.

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 t

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

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 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

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, w

believed to be located outside the United States," *id.*

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.

(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*

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

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]

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

The government argued below that complying with the warrant requirement

Phone: (212) 549

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS