WASHINGTON
LEGISLATIVE OFFICE

May 10, 2016

The Honorable Charles Grassley
Chairman, Senate Judiciary Committee
U.S. Senate
Washington, D.C. 20510

The Honorable Patrick Leahy
Ranking Member, Senate Judiciary Committee
U.S. Senate
Washington, D.C. 20510

CC: Members of the Senate Judiciary Committee

RE: Senate Judiciary Committee's Hearing, "Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties"

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

KARIN JOHANSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

Dear Chairman Grassley, Ranking Member Leahy, and Members of the Committee,

On behalf of the American Civil Liberties Union ("ACLU"[1]), we submit this letter for the record in connection with the Senate Judiciary Committee's hearing, "Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties" to address concerns with Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Since its enactment, the ACLU has strongly opposed Section 702 on the grounds that it authorizes the warrantless surveillance of Americans' communications. Absent meaningful reforms, we believe that Congress should not reauthorize Section 702 when it is set to expire in 2017.

To ensure that Section 702 surveillance complies with the government's obligations under the Constitution and international law, we urge the committee to adopt reforms to Section 702 that would: (1) close the "backdoor search" loophole; (2) prohibit "upstream" surveillance; (3) narrow the permissible purposes for Section 702 surveillance; (4) enhance FISA court oversight; (5) limit retention, use, and dissemination of information; (6) ensure appropriate notice when Section 702 is used in criminal investigations; and (7) enhance transparency. In addition, as part of the debate over Section 702, we urge the committee to consider reforms to electronic surveillance currently undertaken under Executive Order 12333, which implicate the rights of millions of Americans and individuals around the world.

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

1. The "Backdoor Search" Loophole

Although Section 702 prohibits the government from intentionally targeting the communications of U.S. persons, it does not contain language imposing restrictions on querying those communications if they were inadvertently or incidentally collected under Section 702. As a result of an apparent change in the NSA's internal practices in 2011, the NSA has asserted the authority to query databases containing these communications using the names and identifiers of U.S. persons—without ever obtaining a warrant.[2] The NSA, CIA, FBI, and other agencies all conduct these types of queries. Through this so-called "backdoor search" loophole, the government has transformed Section 702—designed to target citizens abroad—into a tool that can be used to conduct surveillance on U.S. citizens and residents. These backdoor searches are particularly concerning given that executive branch procedures allow the government to use Section 702 information in domestic criminal investigations of any kind, and as evidence at trial in cases unrelated to national security, such as kidnapping, human trafficking, or certain transnational crimes.[3]

To address this deficiency, Congress should adopt a requirement that the government obtain a warrant to search the Section 702 database for information about U.S. person. Indeed, there appears to already be broad Congressional support for such a reform. On two separate occasions the House has voted for appropriations amendments that would require a warrant prior to searching the Section 702 database for information concerning U.S. persons.[4] Such a reform is critical to ensure that Section 702 is not used by the government to circumvent the Fourth Amendment's warrant requirement.

2. Upstream Surveillance[5]

The government conducts Upstream surveillance by tapping directly into the Internet "backbone" inside the United States—the network of high-capacity cables and switches that carry the communications of hundreds of millions of Americans and others around the world.[6] With the assistance of providers like Verizon and AT&T, the NSA seizes international communications en masse and searches their full contents for terms related to its thousands of targets. Upstream surveillance is not limited to communications sent or received by the NSA's targets. Instead, the NSA is engaging in what is called "about" surveillance, in which the NSA intercepts vast quantities of internet traffic and examines the contents of essentially everyone's communications to determine whether they mention identifiers associated with the NSA's thousands of targets.[7] Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets (as opposed to those "to" or "from" its targets); nor does it later purge those intercepted communications.

---

[2] *See [Redacted]*, No. [Redacted] (FISC Nov. 6, 2015), http://1.usa.gov/1Vq8tLp.

[3] Robert Litt, Gen. Counsel, Office of the Dir. Of Nat'l Intelligence, Speech at the Brookings Institute: U.S. Intelligence Community Surveillance One Year After President Obama's Address (Feb. 4 2015), *available at* http://www.brookings.edu/~/media/events/2015/02/04-surveillance/20150204_intelligence_surveillance_litt_transcript.pdf.

[4] Sam Sacks, "NSA Backdoor Searches Would End if House Amendment Survives," THE INTERCEPT, June 12, 2015, https://theintercept.com/2015/06/12/house-hopes-provision-close-surveillance-loophole-will-survive-time/.

[5] The ACLU is currently engaging in litigation challenging Upstream surveillance as unconstitutional. Brief for Appellant, Wikimedia Found. v. NSA/Central Sec. Serv, 2016 WL 1426106 (4th Cir. April 2016) (No. 15-2560).

[6] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) https://www.pclob.gov/library/702-Report.pdf. [Hereinafter "PCLOB Report on 702"].

[7] *See* PCLOB Report on 702, *supra* note 6 at 7, 37–38, 111 n.476, 120–22; David Kris, *Trends and Predictions in Foreign Intelligence Surveillance*, 8 J. Nat'l Security L. & Pol'y 18 n.64 (2016), http://bit.ly/1WLjG8C (discussing Upstream surveillance and observing that it is unresolved whether the government should be permitted to "review the contents of an unlimited number of e-mails from unrelated parties in its effort to find information 'about' the target")

As part of its examination of Section 702, we urge the Committee to remedy deficiencies in the current statute that the government improperly relies on to conduct Upstream surveillance, including by clarifying that the statute does not authorize the seizure and search of communications that are neither to nor from the NSA's targets.

3. Scope of Section 702 Surveillance

Section 702 permits surveillance for purposes that extend far beyond national security needs or counterterrorism. Under Section 702, the government is not required to certify that surveillance targets are agents of a foreign power, engaged in criminal activity, or even remotely associated with terrorism. Instead, the government is permitted to target any foreigner if a significant purpose of the surveillance is to collect "foreign intelligence" information—a term defined broadly to cover a wide array of communications. For example, "foreign intelligence" is defined to include information about "foreign affairs,"[8] which could include communications between international organizations and government whistleblowers; diplomats; or even journalists and sources. Such surveillance, due to its very purpose, extends beyond national security and sweeps up the information of individuals who pose no threat to the United States. To address this overbreadth, the Committee should consider reforms to narrow the definition of "foreign intelligence" and limit the scope of Section 702 surveillance.

4. FISC Oversight

Section 702 dramatically diminished FISC oversight of government surveillance. Prior to Section 702, FISA generally foreclosed the government from engaging in electronic surveillance without obtaining an individualized and particularized order from the FISC. The FISC could only issue an order if, among other things, it found that there was probable cause to believe that a specific *target* was a "foreign power" or "agent of a foreign power"—terms defined to include members of foreign terrorist organizations or governments. For surveillance conducted under Section 702, however, the FISC has no role in reviewing the government's individual surveillance targets who, as noted above, may be journalists, academic researchers, human rights advocates, and others who are not even remotely engaged in wrongdoing. Instead, the FISC only has the authority to review the government's targeting and minimization *procedures* to assess whether they comply with the statute, and ensure that the government has certified that their purpose of engaging in the surveillance is to collect "foreign intelligence." The limited role of the FISC in this context raises significant concerns, particularly given that the number of targets has ballooned to over 94,000.[9] As part of its examination of Section 702, we urge the Committee to enact reforms that would enhance FISC review, including enhanced assessment of targeting and minimization.

5. Notice

The government asserts the authority to use information collected under Section 702 in any type of domestic criminal investigation and as evidence at a trial in criminal proceedings that have no nexus to national security.[10] This concerning practice is compounded by the failure of the government to fulfill its obligations to notify individuals if it intends to use information "obtained or derived" from Section 702 in legal or administrative proceedings.[11] Until recently, this notification requirement was only honored in the breach: the Department of Justice did not provide notice of Section 702 surveillance to *any* defendant from 2008 to 2013, and since then it has provided notice in

---

[8] 50 U.S.C. § 1801(e)(2)(B) (2012).

[9] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES (April 30, 2016), *available at* https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf.

[10] *See [Redacted]*, *supra* note 2; Litt, *supra* note 3.

[11] 50 U.S.C. § 1806(c).

only 8 criminal cases.[12] In addition, the Treasury Department's Office of Foreign Assets Control reportedly relies on Section 702-derived information but has never notified those affected in its proceedings.[13]

The Committee should examine how the government is interpreting its current obligation to provide notice where information is "derived" from Section 702, and should adopt reforms that ensure defendants are provided notice in cases where Section 702 information is used directly or indirectly in support of a criminal prosecution. Moreover, because of the government's track-record in this area, the Committee should enact reforms that facilitate effective judicial oversight of the government's notice obligations.

6. Retention, Use, and Dissemination of Information

Section 702 minimization procedures—which govern the use, sharing, and retention of information – fail to adequately protect the rights of U.S. and non-U.S. persons. Under current procedures, the government can retain communications indefinitely if they are encrypted or are found to contain foreign intelligence information.[14] Even for data that does not fall into either of these categories, the default retention period is two years for data acquired through Upstream surveillance, and five years for other Section 702-acquired information. This data can be searched, disseminated to other countries, and used for a wide variety of purposes, including criminal prosecutions. As part of its examination of Section 702, we urge the Committee to enact reforms that appropriately restrict the retention, use, and dissemination of information collected under Section 702.

7. Transparency

The current statute fails to ensure appropriate transparency of Section 702 activities. For example, despite numerous requests from members of Congress,[15] the government has refused to disclose the (1) number of Americans whose information is collected under Section 702, or (2) the number of times the FBI and other agencies search the Section 702 database for information about U.S. persons (i.e. "backdoor searches"). The government has also failed to fully implement PCLOB recommendations that would shed greater light on the number of Americans impacted by Section 702 surveillance.

As part of its examination of Section 702, we urge the Committee to press for release of this information to ensure that Congress has the information necessary to appropriately reform Section 702. In addition, we urge the Committee to enact reforms that would require additional transparency of the government's surveillance activities.

---

[12] *See* Patrick C. Toomey, "Why Aren't Criminal Defendants getting Notice of Section 702 Surveillance—Again?," JUST SECURITY (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/; Charlie Savage, "Warrantless Surveillance in Terror Cases Raises Constitutional Challenge," N.Y.TIMES, April 26, 2016, http://www.nytimes.com/2016/04/27/us/warrantless-surveillance-in-terror-case-raises-constitutional-challenge.html.

[13] Charlie Savage, "Debate Brews Over Disclosing Warrantless Spying," N.Y.TIMES, Sep. 30, 2014, http://mobile.nytimes.com/2014/10/01/us/debate-simmers-over-disclosing-warrantless-spying.html.

[14] *See* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE ACT OF 1978, AS AMENDED (Jan. 8, 2007), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[15] Letter from Rep. John Conyers, Jr., et. al. to the Hon. James Clapper, Dir., Office of the Dir. Of Nat'l Intelligence. (April 22, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

Please contact Legislative Counsel Neema Guliani at nguliani@aclu.org or 202-675-2322 for more information. Please also find attached the following testimony and letters providing additional background information: 1) Testimony of Jameel Jaffer, Deputy Legal Director of the ACLU, to the Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act; 2) Coalition Letter to James R. Clapper, Director of the Office of the Director of National Intelligence Regarding Transparency of Section 702 of the Foreign Intelligence Surveillance Act (including a response letter from ODNI dated Dec. 28, 2015).

Sincerely,

Karin Johanson
Director, Washington Legislative Office

Neema Singh Guliani
Legislative Counsel

Privacy and Civil Liberties Oversight Board
Public Hearing on Section 702 of the FISA Amendments Act
March 19, 2014

Submission of Jameel Jaffer*
Deputy Legal Director
American Civil Liberties Union Foundation

INTRODUCTION

Thank you for the opportunity to provide the board with the ACLU's views concerning Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). The ACLU's view is that Section 702 is unconstitutional. The statute violates the Fourth Amendment because it permits the government to conduct large-scale warrantless surveillance of Americans' international communications—communications in which Americans have a reasonable expectation of privacy.[1] The statute would be unconstitutional even if the warrant clause were inapplicable because the surveillance it authorizes is unreasonable.[2]

The ACLU also believes, based on records released over the past nine months, that the government's implementation of the Act exceeds statutory authority—i.e., that the government is claiming, and exercising, more authority than the statute actually provides. First, while the statute was intended to augment the government's authority to collect international communications, the NSA's targeting and minimization procedures give the government broad authority to collect purely domestic communications as well. Second, while the statute was intended to give the government authority to acquire communications to and from the government's targets, the NSA's procedures also permit the government to acquire communications "about" those targets. And, third, while the statute prohibits so-called "reverse targeting," the NSA's procedures authorize the government to conduct "backdoor" searches of

* I would like to acknowledge the substantial contributions of Alex Abdo, Brett Max Kaufman, Michelle Richardson, and Patrick Toomey—though any errors herein are solely my own.

[1] In this submission, I use "Americans" interchangeably with "U.S. persons," as defined in 50 U.S.C. § 1801(i). I use the phrase "international communications" to refer to communications that either originate or terminate (but not both) inside the United States. I use "FISA Amendments Act," "FAA," and "Section 702" interchangeably.

[2] As discussed below, the statute is also unconstitutional because it imposes a substantial burden on expressive and associational rights but lacks the safeguards that the First Amendment demands.

communications acquired under the FAA using selectors associated with particular, known Americans. Thus, even if the statute itself is lawful, the NSA's implementation of it is not.[3]

ANALYSIS

I. 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.[4] 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."[5] 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.[6] To better protect Americans' privacy, the committee recommended that all surveillance of communications "to, from, or about an American without his consent" be subject to a judicial warrant procedure.[7]

In 1978, largely in response to the Church Report, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny government applications for surveillance orders in certain foreign intelligence investigations.[8] In its current form, FISA regulates, among other things, "electronic surveillance," which is defined to include:

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.[9]

---

[3] This submission focuses solely on the requirements of domestic law. The ACLU intends to file a separate submission analyzing Section 702 under principles of international law.

[4] *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"); *see also* President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 57–63 (Dec. 12, 2013), http://1.usa.gov/1cBct0k ("PRG Report").

[5] Church Report at 137.

[6] *Id*. at 165.

[7] *Id*. at 309.

[8] 50 U.S.C. § 1803.

[9] *Id.* § 1801(f)(2).

Before passage of the FAA, FISA generally foreclosed the government from engaging in "electronic surveillance" without first obtaining individualized and particularized orders from the FISC. To obtain an order, the government was required to submit an application that identified or described the target of the surveillance; explained the government's basis for believing that "the target of the electronic surveillance [was] a foreign power or an agent of a foreign power"; explained the government's basis for believing that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power"; described the procedures the government would use to "minimiz[e]" the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons; described the nature of the foreign intelligence information sought and the type of communications that would be subject to surveillance; and certified that a "significant purpose" of the surveillance was to obtain "foreign intelligence information."[10]

The FISC could issue a traditional FISA order only if it found that there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power,"[11] and that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power."[12]

B. The Warrantless Wiretapping Program and the 2007 FISA Orders

In late 2001, President Bush secretly authorized the NSA to implement a program of warrantless electronic surveillance. The program, which President Bush publicly acknowledged after *The New York Times* reported its existence in December 2005,[13] involved, among other things, the interception of certain emails and telephone calls that originated or terminated inside the United States.[14] The interceptions were not predicated on judicial warrants or any other form of judicial authorization; nor were they predicated on any determination of criminal or foreign intelligence probable cause. Instead, NSA "shift supervisors" initiated surveillance when, in their judgment, there was a "reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[15]

---

[10] *Id.* § 1804(a) (2006).

[11] *Id.* § 1805(a)(2)(A).

[12] *Id.* § 1805(a)(2)(B).

[13] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, http://nyti.ms/1ibX2RM.

[14] *See* Public Declaration of James R. Clapper, Director of National Intelligence ("DNI") ¶ 6, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. Dec. 20, 2013), Doc. 168 ("Clapper *Jewel* Declaration").

[15] Alberto Gonzales, Attorney General, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19. 2005), http://www.fas.org/irp/news/2005/12/ag121905.html; *see also* Offices of Inspectors General of the DOD, DOJ, CIA, NSA & ODNI, Unclassified Report on the President's Surveillance Program 14–16 (2009), https://www.fas.org/irp/eprint/psp.pdf ("PSP IG Report").

A district court enjoined the warrantless wiretapping program on August 17, 2006, holding that it violated FISA, the First and Fourth Amendments, and the principle of separation of powers.[16] On January 17, 2007, then–Attorney General Alberto Gonzales announced that the government would discontinue the program as it was then constituted.[17] He explained that a judge of the FISC had ratified the program and that, as a result, "any electronic surveillance that had been occurring" as part of the program would thereafter be conducted "subject to the approval of the Foreign Intelligence Surveillance Court."[18]

In the spring of 2007, the FISC narrowed the orders it had issued in January of that year.[19] After it did so, the administration pressed Congress for amendments that would permit large-scale warrantless surveillance of Americans' international communications.[20]

C. The FISA Amendments Act of 2008

President Bush signed the FAA into law on July 10, 2008.[21] The statute authorizes the government's large-scale acquisition of U.S. persons' international communications from Internet and telecommunications providers inside the United States. It achieves this result by giving the government sweeping authority to monitor the communications of "targets" located outside the United States and to monitor U.S. persons' communications in the course of that surveillance.

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."[22] Before obtaining an order authorizing surveillance under the Act, the Attorney General and DNI 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, "targeting procedures" and "minimization procedures."[23] The targeting procedures must be "reasonably designed" to ensure that 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."[24] The minimization procedures

---

[16] *See ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated on jurisdictional grounds*, 493 F.3d 644 (6th Cir. 2007).

[17] Letter from Alberto Gonzales, Attorney General, to Senators Patrick Leahy and Arlen Specter 1 (Jan. 17, 2007), http://nyti.ms/1ixrE0M.

[18] *Id.*; *see* PSP IG Report 30–31.

[19] *See* PSP IG Report 30–31; *see also Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013).

[20] *See* PSP IG Report 31.

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

[22] 50 U.S.C. §1881a(a).

[23] *Id.* § 1881a(d)–(g).

[24] *Id.* § 1881a(g)(2)(A)(I).

must meet the requirements of sections 1801(h) and 1821(4), described below.[25] The certification and supporting affidavit must also attest that the Attorney General has adopted "guidelines" to prevent the targeting of known U.S. persons; that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose" of the acquisition is "to obtain foreign intelligence information."[26] The phrase "foreign intelligence information" is defined broadly to include, among other things, information concerning terrorism, national defense, and foreign affairs.[27]

Surveillance conducted under the FAA differs significantly—indeed, radically—from surveillance conducted under traditional FISA. Unlike surveillance under traditional FISA, surveillance under the FAA is not predicated on probable cause or individualized suspicion. The government's targets need not be 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 so long as the programmatic purpose of the surveillance is to acquire "foreign intelligence information."[28]

In addition, the FISC's role in reviewing the government's surveillance activities under the FAA is "narrowly circumscribed."[29] The FISC does not review or approve the government's targeting decisions. Nor does it review or approve the list of "facilities" the government proposes to monitor—to the contrary, the FAA expressly provides that the government need not inform the FISC of the "facilities, places, premises, or property" at which its surveillance will be directed.[30] The FISC reviews only the general procedures that the government proposes to use in carrying out its surveillance.[31] The role that the FISC plays under the FAA bears no resemblance to the role that it has traditionally played under FISA.[32]

Importantly, while the FAA addresses the circumstances in which the government may "target" individuals outside the United States, its effect is to give the government broad authority to monitor *Americans'* international communications. This is by design. In advocating changes to

---

[25] *Id*. § 1881a(g)(2)(A)(ii).

[26] *Id*. § 1881a(g)(2)(A)(iii)–(vii).

[27] *Id*. § 1801(e).

[28] *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.").

[29] *See In re Proceedings Required by § 702(I) of the FISA Amendments Act of 2008*, No. Misc. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008).

[30] 50 U.S.C. § 1881a(g)(4).

[31] *See id*. § 1881a.

[32] *See* Privacy & Civil Liberties Oversight Board, *Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act* at 35 (July 9, 2013) (statement of Hon. James Robertson), http://www.pclob.gov/SiteAssets/9-july-2013/Public%20Workshop%20-%20Full.pdf.

FISA, intelligence officials made clear that their principal aim was to enable broader surveillance of communications between individuals inside the United States and non-Americans abroad.[33]

To the extent the FAA protects Americans' privacy rights, it does so through the requirement that the government adopt "minimization procedures"—procedures that must be "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[34] However, the statute does not prescribe specific minimization procedures and it does not give the FISC the authority to monitor compliance with minimization procedures. Moreover, it includes an exception that expressly allows the government to retain and disseminate communications—including those of U.S. persons—if the government concludes that the communications contain "foreign intelligence information." Again, that term is defined very broadly. The effect of the statute is to allow the government to conduct large-scale monitoring of Americans' international communications for "foreign intelligence information."

II. The FAA violates the Fourth Amendment.

The FAA authorizes warrantless surveillance of Americans' international communications, communications in which Americans have a reasonable expectation of privacy. This warrantless surveillance is not excused by any recognized exception to the warrant requirement. While some courts have recognized an exception to the warrant requirement in the foreign intelligence context, most of these courts did so before Congress enacted FISA in 1978, and the nation's experience with FISA since 1978 has undermined these courts' reasoning. In any event, no court has recognized a foreign intelligence exception broad enough to justify the dragnet surveillance at issue here.

The fact that the Constitution forecloses the government from conducting warrantless surveillance of U.S. persons' international communications does not mean that the Constitution invariably requires the government to obtain probable-cause warrants before conducting surveillance of a legitimate foreign intelligence targets outside the United States. 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 point communicate with U.S. persons. But compliance with the warrant clause requires, at the very least, that the government avoid warrantless acquisition of Americans' international communications where it is reasonably possible to do so. It must make reasonable efforts not to intercept those communications in the first place—for example, it must minimize "acquisition" of those communications. If it nonetheless acquires U.S. persons' communications through warrantless surveillance, it should generally not retain them. If it retains them, it should not access them—"collect" them, in the NSA's terminology—without first seeking a warrant based on probable cause.[35] The mere fact that the government's "targets" are foreigners outside the

[33] *See infra* Section II.C.

[34] 50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

[35] A bill co-sponsored by then-Senator Obama corresponded to these principles. The bill would have prohibited the government from 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

United States cannot render constitutional a program that is designed to allow the government to mine millions of Americans' international communications for foreign intelligence information.

It is important to note that the FAA would be unconstitutional even if the warrant clause did not apply. As discussed in Section II.D, *infra*, the FAA lacks any of the traditional indicia of reasonableness. Indeed, it authorizes the kind of surveillance that led to the adoption of the Fourth Amendment in the first place—generalized surveillance based on general warrants. While the government plainly has a legitimate interest in collecting information about threats to the national security, the Fourth Amendment requires that the government pursue this interest with narrower means.

A. The FAA violates the Fourth Amendment because it permits the government to monitor Americans' communications in violation of the warrant clause.

Americans have a constitutionally protected privacy interest in the content of their telephone calls and emails.[36] This expectation of privacy extends not just to domestic communications but to international communications as well.[37] Because Americans have a constitutionally protected privacy interest in the content of their international communications, the government generally cannot monitor these communications without first obtaining a warrant

---

the United States." *See* S. 3979, 110th Cong. (2008). It would also have generally prohibited the government from accessing Americans' communications collected under Section 702 without a warrant based on probable cause. *Id.*

[36] *United States v. Katz*, 389 U.S. 347, 353 (1967); *see also United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297, 313 (1972) ("*Keith*") ("[*Katz*] implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."); *Alderman v. United States*, 394 U.S. 165, 177 (1969); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *see also* Defs.' Mem. in Opp'n to Pls.' Mot. for Summ. J. 48, *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633 (S.D.N.Y. 2009) (No. 08 Civ. 6259) (not contesting that the Fourth Amendment protects privacy of U.S. persons' international communications).

[37] *See, e.g.*, *United States v. Ramsey*, 431 U.S. 606, 616–20 (1977) (holding that Fourth Amendment was implicated by statute that authorized customs officers to open envelopes and packages sent from outside the United States); *Birnbaum v. United States*, 588 F.2d 319, 325 (2d Cir. 1979); *United States v. Doe*, 472 F.2d 982, 984 (2d Cir. 1973); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000); *see also United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992) (holding that Fourth Amendment is engaged even by *foreign* governments' surveillance of Americans abroad if the U.S. government is sufficiently involved in the surveillance); *United States v. Peterson*, 812 F.2d 486 (9th Cir. 1987) (same); *Berlin Democratic Club v. Rumsfeld*, 410 F. Supp. 144 (D.D.C. 1976) (same).

based on probable cause.[38] Warrantless searches are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[39]

The Supreme Court has interpreted the warrant clause to require three things: first, that any warrant be issued by a neutral, disinterested magistrate; second, that those seeking the warrant demonstrate to the magistrate "probable cause"; and third, that any warrant particularly describe the things to be seized as well as the place to be searched.[40] The requirement of a "neutral, disinterested magistrate" is a requirement that that "the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police."[41] The requirement of probable cause is meant to ensure that "baseless searches shall not proceed."[42] The requirement of particularity, finally, is meant to "limit[] the authorization to search to the specific areas and things for which there is probable cause to search" in order to "ensure[] that the search will be carefully tailored."[43]

The importance of the particularity requirement "is especially great in the case of eavesdropping," because eavesdropping inevitably leads to the interception of intimate

---

[38] *See Dalia v. United States*, 441 U.S. 238, 256 n.18 (1979) ("electronic surveillance undeniably is a Fourth Amendment intrusion requiring a warrant"); *Keith*, 407 U.S. at 313 ("the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitates the application of Fourth Amendment safeguards"); *Katz*, 389 U.S. at 356; *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985) ("even narrowly circumscribed electronic surveillance must have prior judicial sanction"); *United States v. Tortorello*, 480 F.2d 764, 773 (1973).

[39] *United States v. Karo*, 468 U.S. 705, 717 (1984); *see Payton v. New York*, 445 U.S. 573 (1980); *Chimel v. California*, 395 U.S. 752, 768 (1969); *Katz*, 389 U.S. at 357.

[40] *Dalia*, 441 U.S. at 255.

[41] *Katz*, 389 U.S. at 357; *see also Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1972) (stating that a "neutral, disinterested magistrate" must be someone other than an executive officer "engaged in the often competitive enterprise of ferreting out crime"); *Keith*, 407 U.S. at 316–17 ("The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised."); *McDonald v. United States*, 335 U.S. 451, 455–56 (1948) ("The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals.").

[42] *Keith*, 407 U.S. at 316. Probable cause "is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness." *Camara v. Mun. Court of S.F.*, 387 U.S. 523, 534 (1967).

[43] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also United States v. Silberman*, 732 F. Supp. 1057, 1061–62 (1990) ("[T]he particularity clause requires that a statute authorizing a search or seizure must provide some means of limiting the place to be searched in a manner sufficient to protect a person's legitimate right to be free from unreasonable searches and seizures."); *see also United States v. Bianco*, 998 F.2d 1112, 1115 (2d Cir. 1993) (stating that the particularity requirement "prevents a general, exploratory rummaging in a person's belongings" (internal quotation marks omitted)). The particularity requirement is designed to leave nothing "to the discretion of the officer executing the warrant." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976).

conversations that are unrelated to the investigation.[44] In the context of electronic surveillance, the requirement of particularity generally demands that the government identify or describe the person to be surveilled, the facilities to be monitored, and the particular communications to be seized.[45]

The FAA authorizes the executive branch to conduct electronic surveillance without compliance with the warrant clause.

First, the Act fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police."[46] While the government may not initiate an acquisition under section the FAA without first applying for an order from the FISC (or, in an emergency, obtaining such an order within seven days of initiating the acquisition), the FISC's role in this context is limited to reviewing general procedures relating to targeting and minimization. Nothing in the Act requires the government even to inform the court who its surveillance targets are (beyond to say that the targets are outside the United States), what the purpose of its surveillance is (beyond to say that a "significant purpose" of the surveillance is foreign intelligence), or which Americans' privacy is likely to be implicated by the acquisition.[47]

Second, the Act fails to condition government surveillance on the existence of probable cause. The Act permits the government to conduct acquisitions under section 702(a) without proving to a court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism.[48] Indeed, the FAA permits the government to conduct acquisitions without even making an *administrative* determination that its targets fall into any of these categories. Accordingly, the government's surveillance targets may be political activists, victims of human rights abuses, journalists, or researchers. The government's targets may even be entire populations or geographic regions.[49]

---

[44] *Berger v. New York*, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) ("The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations."); *see also Tortorello*, 480 F.2d at 779.

[45] *See United States v. Donovan*, 429 U.S. 413, 427 n.15, 428 (1977).

[46] *Katz*, 389 U.S. at 357.

[47] *Cf.* 18 U.S.C. § 2518(1)(b) (requiring government's application for Title III warrant to include, inter alia, details as to the particular offense that has been committed, a description of the nature and location of facilities to be monitored, a description of the type of communications to be intercepted, and the identity of the individual to be monitored); 50 U.S.C. § 1804(a) (setting out similar requirements for FISA warrants).

[48] *Cf.* 18 U.S.C. § 2518(3) (permitting government to conduct surveillance under Title III only after court makes probable cause determination); 50 U.S.C. § 1805(a)(2) (corresponding provision for FISA).

[49] *See* Letter from Att'y Gen. Michael B. Mukasey and DNI McConnell to Hon. Harry Reid (Feb. 5, 2008), http://1.usa.gov/1kVLzJu (arguing that the intelligence community should not be prevented "from targeting a particular group of buildings or a geographic area abroad").

Again, it is important to recognize that the absence of an individualized suspicion requirement has ramifications for Americans even though the government's ostensible targets are foreign citizens outside the United States. The absence of an individualized suspicion requirement means that the government can conduct large-scale warrantless surveillance of *Americans'* international communications.

Third, the FAA fails to impose any meaningful limit on the scope of surveillance conducted under the Act. Unlike FISA, it does not require the government to identify the individuals to be monitored.[50] It does not require the government to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed.[51] 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.[52] Nor does it require the government to identify "the particular conversations to be seized."[53] Nor, finally, does it place any reasonable limit on the duration of surveillance orders.[54]

B. That surveillance under the FAA is conducted for "foreign intelligence" purposes does not make the warrant clause inapplicable.

The warrant requirement applies not only to surveillance conducted for law enforcement purposes but to surveillance conducted for intelligence purposes as well. In *Keith*, the government argued that the President, acting through the Attorney General, could constitutionally "authorize electronic surveillance in internal security matters without prior judicial approval."[55] In support of its position, the government argued that surveillance conducted for intelligence purposes "should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity"; that courts "have neither the knowledge nor the techniques necessary to determine whether there was probable cause to believe that surveillance was necessary to protect national security"; and that judicial oversight of intelligence surveillance "would create serious potential dangers to the national security and to the lives of informants and agents."[56]

---

[50] *Cf.* 18 U.S.C. § 2518(1)(b)(iv) (requiring Title III application to include "the identity of the person, if known, committing the offense and whose communications are to be intercepted"); 50 U.S.C. § 1804(a)(2) (requiring FISA application to describe "the identity, if known, or a description of the target of the electronic surveillance").

[51] *Cf.* 18 U.S.C. § 2518(1)(b)(ii); 50 U.S.C. § 1804(a)(3)(b).

[52] *Cf.* 50 U.S.C. § 1804(a)(6) (allowing issuance of FISA order only upon certification that a significant purpose of the specific intercept is to obtain foreign intelligence information).

[53] *Donovan*, 429 U.S. at 427 n.15; *cf.* 18 U.S.C. § 2518(1)(b)(iii); 50 U.S.C. § 1804(a)(6).

[54] *Compare* FAA § 702(a) (allowing surveillance programs to continue for up to 1 year), *with* 50 U.S.C. § 1805(d)(1) (providing that surveillance orders issued under FISA are generally limited to 90 or 120 days); 18 U.S.C. § 2518(5) (providing that surveillance orders issued under Title III are limited to 30 days).

[55] 407 U.S. at 299.

[56] *Id*. at 319.

The Court emphatically rejected these arguments. To the government's effort to distinguish intelligence surveillance from law enforcement surveillance, the court wrote that "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[57] To the government's claim that security matters would be "too subtle and complex for judicial evaluation," the Court responded that the judiciary "regularly deal[s] with the most difficult issues of our society" and that there was "no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases."[58] Finally, to the government's contention that the warrant requirement would "fracture the secrecy essential to official intelligence gathering," the Court responded that the judiciary had experience dealing with sensitive and confidential matters and that in any event warrant application proceedings were ordinarily *ex parte*.[59]

Keith involved surveillance conducted for domestic intelligence purposes, but all of the *Keith* Court's reasons for refusing to exempt domestic intelligence surveillance from the warrant requirement apply with equal force to foreign intelligence surveillance as well. First, intelligence surveillance conducted inside the United States presents the same risks to "constitutionally protected privacy of speech" whether the asserted threats are foreign or domestic in origin; both forms of surveillance can be used to "oversee political dissent," and both forms of surveillance could as easily lead to the "indiscriminate wiretapping and bugging of law-abiding citizens" that the *Keith* Court feared.[60] The risks are even greater if, as under the FAA, there is no requirement that the government's surveillance activities be directed at specific foreign agents.[61]

Second, the courts are just as capable of overseeing intelligence surveillance relating to foreign threats as they are of overseeing intelligence surveillance relating to domestic threats. Indeed, for the past 30 years, the courts have been overseeing intelligence surveillance relating to agents of foreign powers because, since its enactment in 1978, FISA has required the government to obtain individualized judicial authorization—based on probable cause that the target is an agent of a foreign power—before conducting foreign intelligence surveillance inside the nation's borders. There is nothing unworkable about FISA's core requirement of judicial authorization. Since 1978, the FISC has granted more than 33,000 surveillance applications

---

[57] *Id*. at 320.

[58] *Id*.; *see also id.* ("If a threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.").

[59] *Id*. at 320–21.

[60] *See Keith*, 407 U.S. at 321; *see also* S. Rep. No. 95-701, *reprinted in* 1978 U.S.C.C.A.N. at 3984 (stating Senate Select Committee on Intelligence's judgment that the arguments in favor of prior judicial review "apply with even greater force to foreign counterintelligence surveillance").

[61] Notably, in *Keith* the government argued that it would be difficult if not impossible to distinguish domestic threats from foreign ones. *See Zweibon v. Mitchell*, 516 F.2d 594, 652 (D.C. Cir. 1975) (en banc) (plurality opinion) (discussing the Solicitor General's brief in *Keith*); *United States v. Hoffman*, 334 F. Supp. 504, 506 (D.D.C. 1971) ("The government contends that foreign and domestic affairs are inextricably intertwined and that any attempt to legally distinguish the impact of foreign affairs from the matters of internal subversive activities is an exercise in futility.").

submitted by the executive branch, and the government has brought dozens of prosecutions based on evidence obtained through FISA.[62]

Finally, the country's experience with FISA also shows that judicial oversight can operate without compromising the secrecy that is necessary in the intelligence context. The FISC meets in secret, rarely publishes its opinions, and generally allows only the government to appear before it.[63] The entire system is organized around the need to preserve the confidentiality of sources and methods. To my knowledge, the executive branch has never suggested that the oversight of the FISC presents a danger to national security. Indeed, in recent months the President and senior intelligence officials have acknowledged that the FISA system is *too* secretive.[64]

In the wake of *Keith*, the D.C. Circuit suggested that a warrant should be required even for foreign intelligence surveillance directed at suspected foreign powers and agents.[65] While other circuit courts recognized a foreign intelligence exception,[66] all of these cases involved surveillance conducted before the enactment of FISA, and FISA seriously undermines their rationale.[67] Equally important, these cases limited the foreign intelligence exception to contexts in which (i) the government's surveillance was directed at a specific foreign agent or foreign power; (ii) the government's primary purpose was to gather foreign intelligence information; and

---

[62] *See, e.g.*, Foreign Intelligence Surveillance Act Orders 1979–2012, Elec. Privacy Info Ctr., https://epic.org/privacy/wiretap/stats/fisa_stats.html; FISA Annual Reports to Congress 1979–2007, Foreign Intelligence Surveillance Act, Fed'n of Am. Scis., http://bit.ly/1cvnUef; *United States v. Sattar*, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (collecting cases).

[63] *See In re Motion for Release of Court Records*, 526 F. Supp. 2d. 484, 488 (FISC 2007) ("Other courts operate primarily in public, with secrecy the exception; the FISC operates primarily in secret, with public access the exception.").

[64] *See* White House, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://1.usa.gov/1itRgM7; Eli Lake, *Spy Chief: We Should've Told You We Track Your Calls*, Daily Beast, Feb. 17, 2014, http://thebea.st/1eMlBRk; *see also Secret Law and the Threat to Democratic and Accountable Government: Hearing Before the Subcomm. on the Constitution of the Senate Judiciary Committee*, 110th Cong. (2008) (testimony of J. William Leonard, Former Director Information Security Oversight Office, and Steven Aftergood, Director, Project on Government Secrecy, Federation of American Scientists).

[65] *Zweibon*, 516 F.2d at 614 (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"); *Berlin Democratic Club*, 410 F. Supp. at 159.

[66] *See., e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 912–15 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 604–05 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973). In *In re Sealed Case*, the Foreign Intelligence Surveillance Court of Review noted that pre-FISA cases had recognized a foreign intelligence exception, but the court did not reach the issue itself. 310 F.3d 717, 742 (FISC Rev. 2002).

[67] *See Bin Laden*, 126 F. Supp. 2d at 272 n.8.

(iii) either the President or Attorney General personally approved the surveillance.[68] The FAA contains none of these limitations.

C. That U.S. persons' communications are collected "incidentally" does not render the warrant clause inapplicable.

The government has argued that the warrant clause is inapplicable because surveillance of Americans' communications under the FAA is "incidental" to surveillance of foreign targets who lack Fourth Amendment rights. This is incorrect. The so-called "incidental overhear" cases hold that where the government has a judicially authorized warrant based on probable cause to monitor specific individuals and facilities, its surveillance is not unlawful merely because it sweeps up the communications of third parties in communication with the target. These cases do not have any application here.

First, the surveillance of Americans' communications under the Act is not "incidental" in any ordinary sense of that word. Intelligence officials who advocated for passage of the FAA (and the Protect America Act before it) indicated that their principal aim was to allow the government broader authority to monitor Americans' international communications.[69] Indeed, when legislators proposed language that would have required the government to obtain probable-cause warrants before accessing Americans' international communications, the White House issued a veto threat.[70] One cannot reasonably say that the surveillance of Americans' communications under the FAA is "incidental" when permitting such surveillance was the very purpose of the Act.

Nor can one reasonably say that the surveillance of Americans' international communications is "incidental" when the Act is *designed* to allow the government to conduct large-scale warrantless surveillance of those communications. While the statute prohibits "reverse targeting," the prohibition is narrow—it applies only if the purpose of the government's surveillance is to target a "*particular, known* person reasonably believed to be in the United States."[71] Outside that narrow prohibition, the statute allows the government to conduct

---

[68] *See Truong*, 629 F.2d at 912; *United States v. Ehrlichman*, 546 F.2d 910, 925 (D.C. Cir. 1976); *Bin Laden*, 126 F. Supp. 2d at 277.

[69] *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 that communications originating or terminating in the United States were those of most importance to the government); *see also* Privacy & Civil Liberties Oversight Board, *Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act* at 109:9–17 (July 9, 2013) (statement of Steven G. Bradbury, Former Principal Deputy Ass't Att'y Gen., DOJ Office of Legal Counsel) (stating that the FAA is "particularly focused on communications in and out of the United States because . . . those are the most important communications").

[70] *See* Letter from Att'y Gen. Michael Mukasey & DNI John M. McConnell to Sen. Harry Reid, at 3–4 (Feb. 5, 2008), http://1.usa.gov/1ihhf9A (asserting that proposed amendment would make it "more difficult to collect intelligence when a foreign terrorist overseas is calling into the United States—which is precisely the communication we generally care most about").

[71] 50 U.S.C. § 1881a(b)(2) (emphasis added).

surveillance in order to collect Americans' international communications. It can target *Al Jazeera* or the *Guardian* in order to monitor their communications with sources in the United States. It can target business executives in order to monitor their communications with American financial institutions. Consistent with the intent of its proponents, the FAA authorizes the government to conduct surveillance of foreign targets—again, targets who need not be suspected foreign agents but who may be attorneys, human rights researchers, or journalists—with the specific purpose of learning the substance of those targets' communications with Americans.

Second, the "incidental overhear" cases involve contexts in which the government's surveillance is predicated on a warrant—that is, where a court has found probable cause with respect to the target and has limited with particularity the facilities and communications to be monitored.[72] The rule is invoked, in other words, where a court has narrowly limited the scope of the government's intrusion into the privacy of third parties. In that context, the courts have held that the judicially approved warrant satisfied the government's constitutional obligation to those third parties.

Neither the FAA nor the FISC, however, imposes analogous limitations on surveillance conducted under the FAA, and neither, therefore, accounts for the Fourth Amendment rights of Americans whose communications are swept up in the course of that warrantless surveillance. Quite the opposite: as discussed above, the FAA does not require the government to establish probable cause or individualized suspicion of any kind with respect to 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 the communications it acquires—so long as the programmatic purpose of its surveillance is to obtain foreign intelligence information. Surveillance under the statute is not particularized in any way. The rule of the "incidental overhear" cases cannot be extended to this context.[73]

Third, and relatedly, the volume of communications intercepted "incidentally" in the course of surveillance under the FAA differs dramatically from the volume of communications intercepted incidentally in the course of surveillance conducted under FISA or Title III. Unlike FISA and Title III, the FAA allows the government to conduct dragnet surveillance—surveillance that targets entire populations or geographic areas or, if the government's interpretation of the statute is correct, surveillance that scans millions of people's communications for information "about" the government's targets. The use of the term "incidental" suggests that the 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 traditional FISA might lead to the incidental collection of a handful of people's

[72] *See, e.g.*, *United States v. Kahn*, 415 U.S. 143 (1974); *Figueroa*, 757 F.2d 466.

[73] *See Donovan*, 429 U.S. at 436 n.15 (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) (finding lawful an incidental intercept because the government had obtained a judicial warrant that "did not give the monitoring agents unfettered discretion to intercept any conversations whatsoever occurring over the target cell phone").

communications over a relatively short period of time, surveillance under the FAA is likely to invade the privacy of thousands or even millions of people.[74]

D. The FAA violates the Fourth Amendment's reasonableness requirement.

The FAA would be unconstitutional even if the warrant clause were inapplicable, because the surveillance it authorizes is unreasonable.

"The ultimate touchstone of the Fourth Amendment is reasonableness,"[75] and the reasonableness requirement applies even where the warrant requirement does not.[76] Reasonableness is determined by examining the "totality of 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."[77] In the context of electronic surveillance, reasonableness demands that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions of privacy."[78] Courts that have assessed the lawfulness of electronic surveillance have often looked to Title III as one measure of reasonableness.[79] While constitutional limitations on foreign intelligence surveillance may differ in some respects from those applicable to law enforcement surveillance,[80] "the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns."[81]

---

[74] *See [Redacted]*, 2011 WL 10945618, at *27 (FISC Oct. 3, 2011) (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 ("[T]he Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a very large number."); *see also id*. at *27 (noting that the government collects more than 250 million communications each year under the FAA).

[75] *See Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (quotation marks omitted).

[76] *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985); *see In re Sealed Case*, 310 F.3d at 737 (assessing reasonableness of FISA); *Figueroa*, 757 F.2d at 471–73 (Title III); *United States v. Duggan*, 743 F.2d 59, 73–74 (2d Cir. 1984) (assessing reasonableness of FISA); *United States v. Tortorello*, 480 F.2d 764, 772–73 (2d Cir. 1973) (Title III).

[77] *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169–70 (2008).

[78] *Berger*, 388 U.S. at 58 (quotation marks omitted); *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.").

[79] *See, e.g.*, *United States v. Mesa-Rincon*, 911 F.2d 1433, 1438 (10th Cir. 1990) (evaluating reasonableness of video surveillance); *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986) (same); *United States v. Torres*, 751 F.2d 875, 884 (7th Cir. 1984) (same).

[80] *See Keith*, 407 U.S. at 323–24.

[81] *In re Sealed Case*, 310 F.3d at 737

The FAA lacks any of the indicia of reasonableness the courts have cited in upholding Title III.[82] Indeed, in its failure to cabin executive discretion, the FAA differs dramatically from Title III—and, for that matter, from traditional FISA. 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. By permitting the government such broad authority to acquire the communications of foreigners abroad, the Act guarantees that Americans' privacy will be invaded on a truly unprecedented scale.

For Americans whose international communications are swept up by FAA surveillance, the sole protection is the requirement that the government "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[83] The protection provided by the minimization requirement, however, is largely illusory. First, the minimization requirement does not extend to "foreign intelligence information,"[84] a phrase that is defined very broadly to encompass not just information relating to terrorism but information relating to "the conduct of the foreign affairs of the United States."[85]

Second, unlike Title III and FISA, the FAA does not require that minimization be particularized with respect to individual targets, and it does not subject the government's implementation of minimization requirements to judicial oversight. Title III requires the government to conduct surveillance "in such a way as to minimize the interception of" innocent and irrelevant conversations.[86] It strictly limits the use and dissemination of material obtained under the statute.[87] It also authorizes courts to oversee the government's compliance with minimization requirements.[88] FISA similarly requires that each order authorizing surveillance of a particular target contain specific minimization procedures governing that particular

---

[82] *See, e.g.*, *Duggan*, 743 F.2d at 73 (FISA); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (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); *In re Kevork*, 634 F. Supp. 1002, 1013 (C.D. Cal. 1985) (FISA), *aff'd*, 788 F.2d 566 (9th Cir. 1986); *United States v. Falvey*, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (FISA); *Tortorello*, 480 F.2d at 773–74 (Title III); *Bobo*, 477 F.2d at 982 (Title III); *United States v. Cafero*, 473 F.2d 489, 498 (3d Cir. 1973) (Title III).

[83] 50 U.S.C. § 1801(h)(1); *see id.* § 1881a(e).

[84] *Id.*

[85] *See id.* § 1881(a); *id.* § 1801(e).

[86] *Id.* § 2518(5); *see id.* (stating that "every order and extension thereof shall contain a provision" regarding the general minimization requirement).

[87] *Id.* § 2517.

[88] *Id.* § 2518(6).

surveillance.[89] It also provides the FISC with authority to oversee the government's minimization on an individualized basis during the course of the surveillance.[90]

Under the FAA, minimization is not individualized but programmatic: the minimization requirement applies not to surveillance of specific targets but rather to entire surveillance programs, the specific targets of which may be known only to the executive branch. Moreover, the FISC is granted no authority to supervise the government's compliance with the minimization requirements during the course of an acquisition—there is no requirement that the government seek judicial approval before it analyzes, retains, or disseminates U.S. communications.[91] This defect is particularly significant 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.[92] 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 or specific communications to be acquired).

Thus, the FAA's minimization requirement does not prevent intrusion into the privacy of innocent U.S. persons. Certainly, the requirement does not prohibit the government from acquiring Americans' communications en masse and mining them for foreign intelligence information. To the contrary, the minimization requirement is formulated to permit precisely this.

III. The FISA Amendments Act violates the First Amendment.

The Supreme Court has recognized that government surveillance can have a profound chilling effect on First Amendment rights. In *Keith*, the Court addressed this point at length, writing:

---

[89] *See* 50 U.S.C. § 1804(a)(4); *id.* § 1805(a)(3); *id.* § 1805(c)(2)(A).

[90] *See id.* § 1805(d)(3).

[91] *Cf. id.* § 1805(d)(3); *id.* § 1801(h)(4) (requiring court order in order to "disclose[], disseminate[], use[] . . . or retain[] for longer than 72 hours" U.S. communications obtained in the course of warrantless surveillance of facilities used exclusively by foreign powers).

[92] *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. 1971) ("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.

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. 'Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power,' . . . history abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent . . . .
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[93]

As discussed above, *Keith* involved the question of whether the government could constitutionally conduct warrantless surveillance to protect against domestic security threats, but in many other contexts the Supreme Court has recognized that the government's surveillance and investigatory activities can infringe on rights protected by the First Amendment. Thus in *NAACP v. Alabama*,[94] a case in which the Supreme Court invalidated an Alabama order that would have required the NAACP to disclose its membership lists, the Supreme Court wrote:

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations . . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs . . . .[95]

---

[93] *Keith*, 407 U.S. at 313–14 (citations omitted).

[94] 357 U.S. 449 (1958).

[95] *Id.* at 462; *accord Watkins v. United States*, 354 U.S. 178, 197 (1957) (noting, in invalidating conviction for refusal to divulge sensitive associational information, that "forced revelations [that] concern matters that are unorthodox, unpopular, or even hateful to the general public, the reaction in the life of the witness may be disastrous"); *see also McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (stating that the First Amendment protects speaker against compelled disclosure of identity); *Tally v. California*, 362 U.S. 60 (1960) (same).

Because government surveillance and investigative activities can have such an invidious effect on rights protected by the First Amendment, the Supreme Court has said that Fourth Amendment safeguards must be strictly enforced where the information sought to be collected implicates the First Amendment.[96] The Court has made clear, however, that the First Amendment also supplies its own protection against laws that burden speech. Thus, in *McIntyre v. Ohio Elections Commission*, a case that involved a statute requiring disclosure of the identity of persons distributing election literature, the Supreme Court wrote: "When a law burdens core political speech, we apply exacting scrutiny and we uphold the restriction only if it is narrowly tailored to serve an overriding interest."[97] Indeed, the Supreme Court has said that even where a challenged statute burdens speech only incidentally, the statute can withstand scrutiny under the First Amendment only "if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."[98]

The FAA imposes a substantial burden on rights protected by the First Amendment. The statute compromises the ability of advocacy organizations, journalists and media organizations, lawyers, and others to gather information, engage in advocacy, and communicate with colleagues, clients, journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States. In the debate that preceded the enactment of the FAA, some members of Congress anticipated the implications this kind of surveillance would have for expressive and associational rights. For example, Senator Cardin of Maryland stated:

> Also formidable, although incalculable, is the chilling effect which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy within lawful limits, without having to sacrifice the expectation of privacy they rightfully hold. Warrantless electronic surveillance can violate that understanding and impair the public confidence so necessary to an uninhibited political life.[99]

---

[96] *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding that mandates of the Fourth Amendment must be applied with "scrupulous exactitude" in this context); *id*. ("Where presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field.").

[97] 514 U.S. at 347 (quotation marks and citation omitted); *see also In Re Primus*, 436 U.S. 412, 432 (1978) (stating that government-imposed burdens upon constitutionally protected communications must withstand "exacting scrutiny" and can be sustained, consistent with the First Amendment, only if the burdens are "closely drawn to avoid unnecessary abridgement of associational freedoms").

[98] *United States v. O'Brien*, 391 U.S. 367, 377 (1968); *see also Ariz. Free Enter. Club's Freedom Club PAC v. Bennett*, 131 S. Ct. 2806, 2813 (2011).

[99] *See* S. Rep. 95-604(I), at 8, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3909.

Because the FAA imposes a substantial burden on First Amendment rights and lacks the particularity that the Fourth Amendment requires, it necessarily sweeps within its ambit constitutionally protected speech that the government has no legitimate interest in acquiring. As discussed above, the FAA permits the government to conduct intrusive surveillance of people who are neither foreign agents nor criminals and to collect vast databases of information that has nothing to do with foreign intelligence or terrorism. Indeed, the statute sweeps so broadly that no international communication is beyond its reach.

More precision is required when First Amendment rights are at stake.[100] Notably, the phrase "scrupulous exactitude," as used in *Zurcher*, was drawn from an earlier Supreme Court decision, *Stanford v. Texas*,[101] a decision that particularly criticized the use of "general warrants" directed at expressive activity. As discussed above, the orders issued by the FISC under the FAA are, in essence, exactly that—general warrants.

IV. The NSA's targeting and minimization procedures do not mitigate the statute's constitutional defects.

In June 2013, *The Guardian* published targeting and minimization procedures approved by the FISC in 2009.[102] More recently, the Office of the Director of National Intelligence released minimization procedures approved by the FISC in 2011.[103] The procedures give the government broad authority to acquire Americans' international communications with the government's targets overseas. This is unsurprising, because supplying the government with this authority was the statute's purpose. The procedures also indicate, however, that the government is exceeding its statutory authority in at least three respects.

---

[100] *Se. Promotions Ltd. v. Conrad*, 420 U.S. 546, 561 (1975); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963) ("the freedoms of expression must be ringed about with adequate bulwarks"); *Speiser v. Randall*, 357 U.S. 513, 520–21 (1958) ("the more important the rights at stake the more important must be the procedural safeguards surrounding those rights"); *see also Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 168 (2002) (striking down local ordinance that burdened First Amendment activity through requirement of a permit for door-to-door canvassing on the grounds that the ordinance "[was] not tailored to the Village's stated interests"); *McIntyre*, 514 U.S. at 351–53 (striking down compelled disclosure statute on grounds that statute reached speech that was beyond state's legitimate interests); *NAACP*, 357 U.S. at 463–66 (striking down order to disclose membership lists on grounds that order was not supported by state's purported justification).

[101] 380 U.S. 926 (1965).

[102] *See* Glenn Greenwald & James Ball, *Top Secret Rules That Allow NSA To Use US Data Without a Warrant*, Guardian, June 20, 2013, http://gu.com/p/3gme3/tw.

[103] *See* Press Release, James R. Clapper, DNI, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act, Nov. 18, 2013, http://1.usa.gov/1htX3ia.

A. The procedures give the government broad authority to collect purely domestic communications.

As discussed above, the FAA gives the government sweeping authority to monitor the communications of foreigners abroad. The targeting and minimization procedures indicate, however, that the government has implemented this authority in a manner that guarantees that the NSA will acquire and retain many purely domestic communications as well. First, the procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary. Second, rather than require the government to destroy purely domestic communications that are obtained inadvertently, the procedures allow the government to retain those communications if they contain foreign intelligence information, evidence of a crime, or encrypted information. This is to say that the government is using a statute that was intended to permit broad access to Americans' international communications as a tool to engage in broad surveillance of Americans' purely domestic communications.

B. The procedures allow the government to acquire huge volumes of communications that are neither to nor from, but merely "about," its targets.

Section 702 authorizes the government to acquire the communications of foreign targets overseas. The NSA's targeting and minimization procedures, however, contemplate that the agency will acquire not only communications to and from its targets but also communications that are merely "about" its targets. This form of surveillance involves the interception and search of virtually every text-based communication entering or leaving the country.[104] An August 2013 report from *The New York Times* states that the NSA is "searching the contents of vast amounts of Americans' e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance, according to intelligence officials."[105] To conduct these searches, the NSA makes a copy of "nearly all cross-border text-based data," scans the content of each message using its chosen keywords or "selectors," and saves for further analysis any communication that contains a match.[106]

This surveillance—"about" surveillance—is unlawful even if the FAA is constitutional. Nothing in the FAA's legislative history suggests that Congress understood itself to be authorizing the very thing FISA originally set out to prohibit—the indiscriminate searching of Americans' communications for foreign intelligence information. And concluding that the FAA permits "about" surveillance requires distorting the meaning of some of FISA's key terms.

---

[104] *See* Procedures Used By the National Security Agency for Targeting Non–United States Persons Reasonably Believed To Be Located Outside the United States To Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended at 1–3 (2009), https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf ("2009 Targeting Procedures"); Charlie Savage, *NSA Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1cez5ZK.

[105] Savage, *supra* note 104.

[106] *Id*.

Although the words "target" and "targeting" are not defined in FISA or the FAA, these terms have always been understood to refer to the act of intentionally subjecting a person's communications or activities to monitoring—not to the act of searching third parties' communications for information *about* that person.

Thus, in defining "electronic surveillance," FISA and the FAA limit "targeting" to the interception of communications *to* or *from* a target:

Electronic surveillance means:

> (1) [T]he acquisition . . . of the contents of any wire or radio communication *sent by or intended to be received by* a particular, known United States person who is in the United States, if the contents are acquired by intentionally *targeting* that United States person . . . .[107]

The provision that enumerates the findings the FISC must make before approving a traditional FISA application similarly contemplates surveillance of communications to and from the target, rather than merely about the target: it requires the FISC to find that the government has demonstrated probable cause to believe that the facilities it intends to monitor are "being used, or [are] about to be used, by a foreign power or an agent of a foreign power"—that is, by its targets.[108] The provision that addresses circumstances in which the government cannot specify in advance the facilities or places it intends to monitor reflects the same premise: it requires that the government attest to the FISC that "each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance."[109] These provisions assume that the target (or the target's agents) will be communicating using the facility that the government intends to monitor.[110]

FISA's definition of "aggrieved person" reflects the same premise. FISA defines an "aggrieved person" to be "a person who is the target of an electronic surveillance or any *other* person whose communications or activities were subject to electronic surveillance."[111] Congress's use of the word "other" in this context would be superfluous unless it understood the

---

[107] 50 U.S.C. § 1801(f)(1) (emphasis added); *see also id.* § 1881(a) (incorporating FISA's definitions).

[108] *See id.* § 1805(a)(2)(B).

[109] *Id*. § 1805(c)(3)(B).

[110] That the FAA does not require the government to identify the "facilities" it intends to monitor, *id.* § 1881a(g)(4), does not mean that the government may monitor any facility at all in order to obtain information *about* its targets. The term "target" limits the facilities the government may permissibly monitor. *Cf. Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?, Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (Sept. 25, 2007), http://www.fas.org/irp/congress/2007_hr/strengthen.pdf ("September 2007 SJC Hearing") (statements of Sen. Feingold, DNI Michael J. McConnell, and James A. Baker) (criticizing the PAA's authorization of surveillance "concerning" non-U.S. persons, and suggesting that "targeting" would be narrower and more precise).

[111] 50 U.S.C. § 1801(k) (emphasis added).

"target" herself to be a person whose communications or activities were subject to electronic surveillance.

Reading the statute to permit "about" surveillance also leads to perverse results. For example, it renders some individuals "aggrieved persons" even though their communications have not been acquired. This is because FISA defines "aggrieved person" to encompass any "target."[112] If the government targets one person by conducting "about" surveillance on others, its target is an aggrieved person under the statute even though her communications have not been acquired. This is nonsensical, and it is also inconsistent with legislative intent. The legislative history makes clear that Congress intended its definition of the term "aggrieved person" to be "coextensive [with], but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance."[113] Thus, it intended to exclude from the definition of "aggrieved person" those "persons, not parties to a communication, who may be mentioned or talked about by others."[114] As Congress observed, individuals "have no fourth amendment privacy right in communications *about* them which the Government may intercept."[115] A person targeted *solely* through "about" surveillance would not normally have Fourth Amendment standing. Yet, if "about" surveillance were permitted by statute, "about" targets would have standing to bring challenges under FISA.[116] Congress's definition of "aggrieved person" is tenable only if a "target" is a person whose communications have actually been intercepted.

The legislative history of the FAA confirms that a "target" is an individual whose communications or activities the government intends to monitor. I am aware of no evidence that Congress considered "about" surveillance when it enacted the FAA, or that Congress considered the implications of allowing the government to scan and search the contents of every communication entering or leaving the United States.[117] To the contrary, executive branch

---

[112] *Id.*

[113] *Id*.

[114] FISA House Report at 66.

[115] *Id*. (emphasis added) (citing *Alderman v. United States*, 394 U.S. 316 (1968)).

[116] *See* 50 U.S.C. § 1881e(a) (information acquired under Title VII is deemed to be information acquired from an electronic surveillance under Title I for certain purposes); *id*. § 1806 (defining notice, disclosure, and suppression rights of "aggrieved person[s]").

[117] *See, e.g.*, September 2007 SJC Hearing (statement of DNI Michael J. McConnell) (addressing the fact that the PAA granted authority to acquire information "concerning" persons outside the United States and stating: "[Q]uite frankly, we were not sure why the word 'concerning' was used. Different language—at one point it was 'directed at,' at another it was 'concerning.'"); *id.* (statement of James A. Baker) (suggesting that "targeting" was a more narrow, clear, and precise term than "concerning"); *see also, e.g.*, *FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability, Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (Oct. 31, 2007), https://fas.org/irp/congress/2007_hr/fisa-amend.html ("October 2007 SJC Hearing"); *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights, Hearing Before the H. Comm. on the Judiciary*, 110th Cong. (Sept. 18, 2007), http://www.fas.org/irp/congress/2007_hr/warrantless2.pdf; *FISA, Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. (Sept. 20, 2007),

officials repeatedly indicated that FAA surveillance would be directed at the communications of foreign targets.[118] According to those officials, the FAA was designed to fill a foreign intelligence gap previously addressed by the warrantless wiretapping program—a program that was focused on the communications of "foreign powers or their agents."[119] In defending the FAA before the Supreme Court, the Justice Department, too, emphasized that the statute was focused on communications to and from the government's foreign intelligence targets. It argued that plaintiffs lacked standing to sue because they could not demonstrate that their foreign contacts would be "target[ed]."[120]

The practice of "about" surveillance is consistent neither with the statute's language nor with its legislative history.[121]

---

http://www.fas.org/irp/congress/2007_hr/fisa092007.pdf; *FISA, Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. (Sept. 18, 2007), http://www.fas.org/irp/congress/2007_hr/fisa091807.pdf; *FISA Amendments Act of 2008, Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, H. Comm. on the Judiciary*, 112th Cong. (May 31, 2012), http://1.usa.gov/1hsfvaU.

[118] *See, e.g.*, October 2007 SJC Hearing (statement of Kenneth Wainstein) ("When we talk about the program, the interception of signals or communications intelligence is absolutely critical, and that is how we learn what our adversaries are planning to do. We capture their communications. We capture their conversations.").

[119] *See* Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 9 n.2 (Jan. 19, 2006), http://www.fas.org/irp/nsa/doj011906.pdf; *id.* at 13 n.4 ("The NSA activities are proportional because they are minimally invasive and narrow in scope, targeting only the international communications of persons reasonably believed to be linked to al Qaeda . . . ."); *id.* at 41 ("The NSA activities are targeted to intercept international communications of persons reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization, a limitation which further strongly supports the reasonableness of the searches.").

[120] Br. of Petitioners at 19, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (No. 11-1025) ("But it is wholly speculative, for instance, whether the government will imminently target respondents' (largely unidentified) foreign contacts abroad for foreign-intelligence information . . . ."); *id.* at 21–22 ("Respondents' self-inflicted harms flow from their and their foreign contacts' fears that the government will monitor their contacts' communications, but respondents do not seek to enjoin all possible government surveillance of their contacts."); *id.* at 30 ("Respondents, for instance, rely on conjecture that the government will choose to expend its limited resources to target respondents' own (largely unidentified) foreign contacts."); Tr. of Oral Argument at 11:21–12:1, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (No. 11-1025) (statement of the Solicitor General) ("But, in addition to the speculation I just described, once you get through all that, you still have to speculate about whether the communication that—whether the persons *with whom the Respondents are communicating are going to be targeted* . . . ." (emphasis added)).

[121] Even if it is unclear whether the statute allows "about" surveillance, the doctrine of constitutional avoidance weighs heavily against reading the statute as the government reads it. *See, e.g.*, *Clark v. Martinez*, 543 U.S. 371, 381 (2005); *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Const. Trades Council*, 485 U.S. 568, 575 (1988). Permitting the government to mine Americans' international communications for foreign intelligence information would raise grave constitutional concerns. The FAA should not be read to permit such surveillance absent clear evidence that Congress intended to permit it.

C. The procedures allow the government to circumvent the prohibition against reverse targeting.

As discussed above, the FAA prohibits the government from "reverse targeting"—it prohibits the government from "intentionally target[ing] a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States."[122] The prohibition against reverse targeting was meant to limit the government's ability to use the surveillance of foreign targets as a pretext for the monitoring of Americans.

It appears that since at least 2011, however, the NSA's minimization procedures have allowed the agency to circumvent the prohibition against reverse targeting by searching communications already-acquired under the FAA for information about "particular, known" Americans.[123] The agency's 2009 minimization procedures barred such searches, stating that "[c]omputer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will not include United States person names or identifiers."[124] The agency's 2011 minimization procedures, however, omit that proscription and indicate instead that "use of United States person identifiers as terms to identify and select communications" will be permitted if "first approved in accordance with NSA procedures."[125]

If, as they seem to do, the NSA's 2011 minimization procedures permit so-called "backdoor" searches of communications acquired under the FAA, they render the prohibition against reverse targeting all but meaningless, because they allow the government to use the surveillance of communications to, from, or "about" foreign targets as a means of facilitating the surveillance of particular, known Americans.[126] The problem is magnified because of the sheer volume of communications that the NSA acquires under the statute.[127] Given the absence of any

---

[122] 50 U.S.C. § 1881a(b)(2) (emphasis added); *see supra* § II.C.

[123] *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, Guardian, Aug. 9, 2013, http://gu.com/p/3tva4 ("Senator Ron Wyden told the *Guardian* that the law provides the NSA with a loophole potentially allowing 'warrantless searches for the phone calls or emails of law-abiding Americans'").

[124] Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702, As Amended § 3(b)(5) (July 29, 2009), https://s3.amazonaws.com/s3.documentcloud.org/documents/716634/exhibit-b.pdf.

[125] Minimization Procedures Used by National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § 3(b)(6) (Oct. 31, 2011), http://1.usa.gov/1e2JsAv ("2011 Minimization Procedures") (omitting same restriction and stating that "use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures").

[126] 154 Cong. Rec. S753, S776 (Feb. 7, 2008) (statement of Sen. Feingold) ("The bill pretends to ban reverse targeting, but this ban is so weak as to be meaningless.").

[127] Marty Lederman, *Key Questions About the New FISA Bill*, Balkinization (June 22, 2008, 8:27 PM EST), http://balkin.blogspot.com/2008/06/key-questions-about-new-fisa-bill.html (explaining that the potential consequences of "incidentally" collected communications are far more severe under the FAA

meaningful limitation on the NSA's authority to acquire international communications under the statute, it is likely that the NSA's databases already include the communications of millions of Americans. The 2011 minimization procedures allow the NSA to search through these communications and to conduct the kind of targeted investigations that in other contexts would be permitted only after a judicial finding of probable cause. Such searches would amount to an end run around both the ban on reverse targeting and the Fourth Amendment's warrant requirement.[128]

---

than under FISA because the FAA gives the government a "vastly expanded reservoir of foreign-to-domestic communications from which it can cull information about nontargeted U.S. persons").

[128] Notably, the President's Review Group recommended that the government be prohibited from "search[ing] the contents of communications acquired under section 702 . . . in an effort to identify communications of particular United States persons," except (a) when the information is necessary to prevent a threat of death or serious bodily harm," or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism." PRG Report 146.

October 29, 2015

Hon. James R. Clapper
Director, Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Clapper:

The undersigned organizations, which are dedicated to preserving privacy and civil liberties, write to request that you provide certain basic information about how Section 702 of the Foreign Intelligence Surveillance Act (FISA) affects Americans and other U.S. residents. Disclosing this information is necessary, we believe, to enable informed public debate in advance of any legislative reauthorization efforts in 2017.

We acknowledge that you have publicly released a significant amount of information about Section 702, as well as declassifying information for inclusion in the report of the Privacy and Civil Liberties Oversight Board (PCLOB). These disclosures have been helpful, and we appreciate them. However, there remains a significant and conspicuous knowledge gap when it comes to the impact of Section 702 surveillance on Americans.

Information about that impact is critical in light of official representations that Section 702 is aimed at foreign threats and that collection of Americans' information is merely "incidental." The American public must have the data necessary to evaluate and weigh these official claims. Moreover, it is unacceptable that the government itself has no idea how many Americans are caught up in an intelligence program ostensibly targeted at foreigners. We therefore ask that you disclose the following information, as discussed further below:

- A public estimate of the number of communications or transactions involving American citizens and residents subject to Section 702 surveillance[1] on a yearly basis.

- The number of times each year that the FBI uses a U.S. person identifier to query databases that include Section 702 data, and the number of times the queries return such data.

- Policies governing agencies' notification of individuals that they intend to use information "derived from" Section 702 surveillance in judicial or administrative proceedings.

---

[1] This request seeks an estimate corresponding to each of the following categories:

(1) The number of communications or transactions involving U.S. residents whose contents or metadata are "screened" for selectors in the course of upstream surveillance;
(2) The number of communications or transactions involving U.S. residents that are retained after their contents or metadata have been screened for selectors in the course of upstream surveillance;
(3) The number of communications or transactions involving U.S. persons that are retained in the course of PRISM surveillance; and
(4) The number of U.S. residents whose information is examined or obtained using any other type of surveillance conducted pursuant to Section 702.

Estimate of How Many Communications Involving U.S. Residents Are Subject to Surveillance

As you know, Senators Wyden and Mark Udall repeatedly have requested that you provide an estimate of how many American communications are collected under Section 702. In 2012, the NSA Inspector General studied whether such an assessment would be feasible. As relayed in a letter from the Inspector General (IG) for the Intelligence Community, the NSA IG concluded that dedicating sufficient resources to such an assessment "would likely impede the NSA's mission." He also concluded that reviewing the NSA's intake to ascertain the effect on American citizens and residents "would itself violate the privacy of U.S. persons."

We disagree with these conclusions and believe that they are undermined by subsequent disclosures. With regard to the question of resources, an October 3, 2011 opinion of the Foreign Intelligence Surveillance Court (FISC) reveals that the NSA, in an effort to address the court's concerns about how many wholly domestic communications were acquired through upstream collection, "conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period." There is no evidence that this undertaking impeded any NSA operations.

Moreover, the NSA's mission is broader than the IG's letter implies. "[P]rotection of privacy and civil liberties" is an express component of the NSA's stated mission. *See* https://www.nsa.gov/about/mission/. Yet the NSA apparently does not know, even at the level of an estimate, how many U.S. person communications it screens or retains under Section 702. The government's lack of information on this critical aspect of its own intelligence activities is remarkable. Ascertaining this information would assist the NSA in pursuing its mission, not impede it.

We understand that the NSA's privacy concerns stem from the possibility that assessing whether communications involve U.S. persons could require a manual review of communications that otherwise would not be accessed or examined. This concern should not arise when ascertaining the impact on U.S. persons of "upstream" surveillance (the term used for obtaining Internet and telephone communications in transit over the telecommunications backbone). These communications contain routing information – the IP address for Internet communications and the country code for telephone communications – that provide a rough, albeit imperfect, indication of the communicants' U.S.-person status. While not an appropriate basis for other extrapolations, this data should be sufficient to provide a broad estimate without any need for manual review. Indeed, the PCLOB has recommended that the NSA count and disclose the number of telephone communications acquired in which one caller is located in the United States, as well as the number of Internet communications acquired through upstream surveillance that originate or terminate in the United States.

About 90 percent of the communications retained under Section 702, however, are stored communications obtained from companies under the PRISM program, which may not contain the same routing information that accompanies communications in transit. In light of the overriding need for Americans to know how this massive surveillance program affects them, the undersigned groups, including many organizations whose missions are centrally focused on

protecting privacy, believe that a one-time, limited sampling of these communications would be a net gain for privacy *if* conducted under appropriate safeguards and conditions.

Many of the undersigned groups possess or have access to significant technical expertise, and are happy to work with the Intelligence Community to devise a minimally intrusive way of ascertaining the U.S.-person status of those whose information is acquired under PRISM. If, after all other alternatives are thoroughly explored, it appears that manual review is required in some instances, measures to mitigate the privacy intrusion would be critical. For instance, the review should be conducted by an independent office; it should use a sample that is about to reach the "age-off" date (*i.e.*, is reaching the end of the applicable retention limit) and is representative of current collection practices; and the communications should be destroyed immediately after review. The review could be used to gauge the percentage of data obtained under PRISM that involves U.S. persons, which then could be applied to the current total number of communications or transactions obtained under PRISM in order to estimate the number of U.S. persons affected.

FBI's Use of U.S. Person Identifiers to Query Section 702 Data

As you know, so-called "back door searches" of Section 702 data are highly controversial. These searches use U.S. person identifiers to query data, even though the data was obtained pursuant to a certification that no U.S. persons were targets. In order to have an informed debate on how Congress should address this issue in 2017, the public needs and deserves better information.

You have disclosed the yearly number of U.S.-person queries that the CIA and NSA perform on Section 702-derived data. You have not disclosed this same figure for the FBI, however, and the USA FREEDOM Act conspicuously exempts the FBI from such a requirement. Given the PCLOB's description of how the FBI uses this information, there is every reason to believe the number of FBI queries far exceeds those of the CIA and NSA. To present a fair overview of how foreign intelligence surveillance is used, it is essential that you work with the Attorney General to release statistics on the FBI's use of U.S. person queries.

There is no practical reason why this information cannot be reported. According to the PCLOB, the FBI does not track U.S. person queries because its minimization rules do not require officials to record whether search terms relate to U.S. persons. However, as evidenced by the NSA and CIA statistics, it is clearly *possible* to record and track that information. Moreover, to the extent the FBI maintains databases in which Section 702 and non-Section 702 data are commingled, that should not be an obstacle. The law requires Section 702 data to be clearly marked as such. For commingled databases, the FBI could simply report the total number of U.S.-person queries, as well as the number of these queries that returned Section 702-derived data.

Notification of Use of Information "Derived From" Section 702

The law requires the government to notify individuals if it intends to use information "obtained or derived" from Section 702 against them in legal or administrative proceedings. Until recently, however, this requirement was honored in the breach. Although the Administration began notifying criminal defendants of the use of Section 702-derived information in October 2013, it

did so in only five cases, and there has not been a single notification in seventeen months. In addition, the Treasury Department's Office of Foreign Assets Control reportedly relies on Section 702-derived information but has never notified those affected by its proceedings. Reports also indicate that some agencies engage in "parallel construction": they reconstruct Section 702-derived information using less controversial methods in order to avoid disclosing the use of Section 702, on the dubious ground that the reconstructed evidence is not "derived from" Section 702 surveillance.

Individuals should know whether they are being given a fair opportunity to challenge Section 702 surveillance when the fruit of such surveillance is used against them. We ask that you disclose how the Department of Justice and other agencies interpret the statutory notification requirement, including the legal interpretations that control when those agencies consider evidence to be "derived from" Section 702 surveillance. These disclosures also should make clear whether evidence collected based on a "tip" arising from Section 702 surveillance is considered "derived" evidence, and the circumstances in which agencies permit investigators to reconstruct evidence originally obtained under Section 702 in order to avoid notification. Keeping these key legal interpretations secret prevents the public from understanding how Section 702 is used in practice, and perpetuates the anti-democratic practice of secret law.

***

The Principles of Intelligence Transparency, adopted by your office in January and reaffirmed through an implementation plan issued by your office two days ago, state that the Intelligence Community will "[b]e proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to . . . provide timely transparency on matters of public interest." This is exactly such a case. The FISA Amendments Act is set to expire on December 31, 2017. Knowing the impact of the law on Americans is not only important to an informed public debate, it is essential. Disclosing the information requested above will remove three of the most significant barriers to that debate.

Sincerely,

Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Bill of Rights Defense Committee
Brennan Center for Justice
Center for Democracy & Technology
The Constitution Project
Constitutional Alliance
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org, Inc.

Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press
Government Accountability Project
Liberty Coalition
National Association of Criminal Defense Lawyers
National Security Counselors
New America's Open Technology Institute
Niskanen Center
OpenTheGovernment.org
PEN American Center
Project On Government Oversight
R Street
Restore the Fourth
The Sunlight Foundation
TechFreedom
World Privacy Forum
X-Lab

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

23 December 2015

Ms. Elizabeth Goitein
Co-Director, Liberty & National Security Program
Brennan Center for Justice
1140 Connecticut Ave., NW
11th Floor, Suite 1150
Washington, D.C. 20036

Dear Ms. Goitein:

Thank you for submitting the letter dated 29 October 2015 to Director of National Intelligence James Clapper, signed by a number of civil society organizations. Director Clapper asked me to respond on his behalf. Please share this response with the organizations that signed that letter.

We share your interest in ensuring transparency sufficient to enable informed public discussion about Section 702 of the Foreign Intelligence Surveillance Act. As you know, we are committed to enhancing intelligence transparency, consistent with our recently published plan for implementing the Principles of Intelligence Transparency for the Intelligence Community. As laid out in that plan—as well as in the Third Open Government National Action Plan—the Intelligence Community will work with civil society to establish a structured series of engagements to discuss issues of public interest.

Director Clapper has requested that we hold a meeting with civil society as soon as mutually convenient, so that we can discuss the matters raised in your letter that are within the Intelligence Community's purview. We would like to ensure we fully understand your requests and the concerns that underlie them, and to explain the status of our existing efforts. We believe we have made progress in addressing certain aspects of your requests, but remaining challenges constrain our ability to provide the information requested. Accordingly, we would also like to explore with you whether there might be alternative approaches to address your concerns.

I will work with your representatives to schedule this meeting, which will include officials from the relevant elements of the Intelligence Community. In the meantime, I would like to provide some initial information in advance of that meeting.

Your letter requests that we disclose additional information regarding "the number of communications or transactions involving American citizens and residents subject to Section 702 surveillance on a yearly basis." As discussed in your letter, this topic has been the subject of prior reviews. Indeed, the Privacy and Civil Liberties Oversight Board (PCLOB) examined this issue as part of its examination of Section 702 implementation. The Intelligence Community worked intensively over many months to provide the PCLOB with the information it requested in order to carry out this review and publish its *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2 July 2014).

Regarding requests that the government disclose information about how many communications of U.S. persons are incidentally acquired under Section 702, the PCLOB noted:

> [T]he executive branch has responded that it cannot provide such a number—because it is often difficult to determine from a communication the nationality of its participants, and because the large volume of collection under Section 702 would make it impossible to conduct such determinations for every communication that is acquired. The executive branch also has pointed out that any attempt to document the nationality of participants to communications acquired under Section 702 would actually be invasive of privacy, because it would require government personnel to spend time scrutinizing the contents of private messages that they otherwise might never access or closely review.

The PCLOB issued a recommendation focused on this topic:

> **Recommendation 9:** The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director's annual report and should be released publicly to the extent consistent with national security.

In its *Recommendations Assessment Report* (29 January 2015), the PCLOB subsequently reported that NSA was assessing how to implement this recommendation. In particular, the PCLOB noted:

> Subparts (1) and (2) of the recommendation involve counting how many telephone calls and upstream Internet communications the NSA acquires in which one participant is located in the United States. As noted in the Board's report, questions remain about whether such figures can accurately be recorded. The NSA has committed to studying this question, and staff from the NSA and the PCLOB have made arrangements to discuss the ongoing progress of its efforts.

NSA has been reviewing how to implement subparts (1)–(3) of this recommendation and is continuing to engage with the PCLOB in that regard. Regarding subpart (4), the USA FREEDOM Act requires the DNI to annually (and publicly) report, with respect to NSA and CIA, numerical information regarding the number of queries that employ U.S. person identifiers. We are in the process of implementing that requirement. Regarding subpart (5), NSA already tracks and reports the number of instances in which it disseminates non-public information regarding U.S. persons. We are reviewing this for potential inclusion in public reporting.

Your letter also requests that we disclose additional information regarding "[t]he number of times each year that the FBI uses a U.S. person identifier to query databases that include Section 702 data, and the number of times the queries return such data." The PCLOB examined this issue carefully with the FBI during its review of Section 702. As discussed in the PCLOB's 702 report, FBI systems do not track the number of queries using U.S. person identifiers. The PCLOB made a two-part recommendation with respect to such queries by the FBI:

> **Recommendation 2:** The FBI's minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters.

In its January 2015 assessment report, the PCLOB stated that the Administration has committed to implementing both parts of this recommendation. With the recent reauthorization of the 702 Certification, many of the Board's recommendations, including this recommendation 2, have been implemented.

Finally, your letter asks about "[p]olicies governing agencies' notification of individuals that they intend to use information 'derived from' Section 702 surveillance in judicial or administrative proceedings." I am informed by the Department of Justice that it has been notifying individuals who are "aggrieved persons" if it intends to use information against them that is either obtained or derived from FISA—including Section 702—in legal or administrative proceedings, and remains committed to fulfilling its notice obligations under the law. According to the Department of Justice, in determining whether information is "obtained or derived from" FISA collection, the appropriate standards and analyses are similar to those appropriate in the context of surveillance conducted pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522. The courts have interpreted Title III's "derived from" standard effectively to codify the fruit-of-the-poisonous-tree doctrine.

You also asked about the language in FISA requiring that such notice be provided when FISA information is used against an aggrieved person in "any trial, hearing or other proceeding." We understand from the Department of Justice that further guidance on this issue can be found in a June 2011 OLC opinion regarding FISA notice requirements for administrative proceedings. See *Applicability of the Foreign Intelligence Surveillance Act's Notification Provision to Security*

Clearance Adjudications by the Department of Justice Access Review Committee (3 June 2011) available at http://www.justice.gov/olc/opinion/applicability-foreign-intelligence-surveillance-acts-notification-provision-security. We defer any further discussions on these topics to the Department of Justice.

Again, we appreciate your reaching out to us to engage on these important transparency topics and look forward to engaging with you to discuss how we might be able to enhance transparency in these and related areas.

Sincerely,

Alexander W. Joel
Civil Liberties Protection Officer
Office of the Director of National intelligence