No. 11-1025

IN THE

Supreme Court of the United States

JAMES R. CLAPPER, JR.,
DIRECTOR OF NATIONAL INTELLIGENCE, *et al.*,
Petitioners,

v.

AMNESTY INTERNATIONAL USA, *et al.*,
Respondents.

On Writ of Certiorari to
The United States Court of Appeals
For the Second Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), THIRTY-TWO TECHNICAL EXPERTS AND LEGAL SCHOLARS, AND EIGHT PRIVACY AND TRANSPARENCY ORGANIZATIONS IN SUPPORT OF RESPONDENTS

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

September 24, 2012

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

ADMINISTRATIVE & LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1] The EPIC Advisory Board includes leading technical experts and legal scholars whose work has contributed to many of the techniques and policies that help safeguard privacy in the modern era.[2]

EPIC has participated as *amicus curiae* before this Court and many other courts in matters concerning the impact of electronic surveillance on civil liberties. *See*, *e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012); *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010); *Herring v. United States*, 555 U.S. 135 (2009); *Hiibel v. Sixth Judicial Circuit of Nev.*, 542 U.S. 177 (2004); *In re US for Historical Cell Site Data*, 747 F. Supp. 2d 827 (2010), *appeal docketed*,

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

[2] EPIC Fellows David Brody, Julia Horwitz, and Jeramie Scott contributed to this brief.

No. 11-20884 (5th Cir. Dec. 14, 2011). EPIC has also recently testified before Congress on the need for oversight in the FISA Amendments Act. *See Hearing on the FISA Amendments Act of 2008: Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary* (2012) (testimony and statement of Marc Rotenberg, Executive Director, EPIC).

This case presents the question of what showing is required to establish Article III standing to challenge the secret collection of private communications. The likelihood of injury depends in part upon the capacity of the Government to engage in the collection program described, and the willingness and authority granted to collect the type of communications at issue – the communications of United States persons. The Government's emphasis on targeting is unhelpful in addressing the standing issue, which relates to the potential interception and collection of Respondents' private communications.

The public's knowledge of the government's activity is limited, and its reasonable concern about the interception of communications is increased by the lack of public reporting and notification under the FISA Amendments Act. Without adequate reporting and accountability, there is insufficient assurance that the communications of U.S. persons will not be intercepted. The costs incurred by respondents to avoid disclosure of confidential communications are therefore reasonable in light of the government's surveillance capabilities and its failure to provide

adequate reporting of the use of its surveillance authority.

Technical Experts and Legal Scholars

Dr. Alessandro Acquisti, Associate Professor of Information Technology and Public Policy, Carnegie Mellon University

Steven Aftergood, Senior Research Analyst, Federation of American Scientists

Ross Anderson, Professor of Security Engineering, Cambridge University

James Bamford, Author and Journalist

Grayson Barber, Esq., Grayson Barber, LLC

Colin J. Bennett, Professor, University of Victoria

Julie E. Cohen, Professor of Law, Georgetown University Law Center

Simon Davies, Project Director, London School of Economics

Dr. Whitfield Diffie, Visiting Scholar, Stanford Center for International Security and Cooperation

Laura K. Donohue, Associate Professor of Law, Georgetown University Law Center

Cynthia Dwork, Researcher, Microsoft

David Farber, Distinguished Career Professor of Computer Science and Public Policy, School of Computer Science, Carnegie Mellon University

Addison Fischer, Former Owner, RSA Data Security, Co-Founder, Verisign

David H. Flaherty, Professor Emeritus of History and Law, University of Western Ontario; Information Privacy Commissioner for British Columbia, 1993-99

Philip S. Friedman, Friedman Law Offices, PLLC

Jerry Kang, Professor of Law, UCLA School of Law

Deborah Hurley, Chair, EPIC Board of Directors

Ian Kerr, Associate Professor, Canada Chair of Ethics, Law, and Technology, University of Ottawa

Chris Larsen, CEO and Co-Founder, Prosper Marketplace, Inc.

Rebecca MacKinnon, Schwartz Senior Fellow, New America Foundation

Mary Minow, Library Law Consultant

Pablo Molina, Adjunct Professor, Georgetown University

Dr. Peter G. Neumann, SRI International

Helen Nissenbaum, Professor, Media, Culture & Communication, NYU

Ray Ozzie, (former) Chief Software Architect, Microsoft

Dr. Deborah Peel, M.D., Founder and Chair, Patient Privacy Rights

Chip Pitts, Lecturer, Stanford Law School and Oxford University

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Barbara Simons, (former) IBM Research

Latanya Sweeny, Professor of Government and Technology in Residence, Harvard University

Frank M. Tuerkheimer, Professor of Law,
University of Wisconsin Law School

Privacy and Transparency Organizations

American Library Association

The American Library Association ("ALA"), established in 1876, is a nonprofit professional organization of more than 60,000 librarians, library trustees, and other friends of libraries dedicated to providing and improving library services and promoting the public interest in a free and open information society.

Bill of Rights Defense Committee

The Bill of Rights Defense Committee is a national non-profit grassroots organization. We defend the rule of law and rights and liberties challenged by overbroad national security and counter-terrorism policies.

Center for Financial Privacy and Human Rights

The Center for Financial Privacy and Human Rights was founded in 2005 to defend privacy, civil liberties and market economics. The Center was the first non-profit human rights and civil liberties organization whose core mission recognizes traditional economic rights as a necessary foundation for a broad understanding of human rights. CFPHR is part of the Liberty and Privacy Network, a

non-governmental advocacy and research 501(c)(3) organization.

Consumer Watchdog

Consumer Watchdog is a tax-exempt 501(c)(3) nonprofit organization dedicated to educating and advocating on behalf of consumers for over 25 years. Its mission is to provide an effective voice for the public interest. Consumer Watchdog's programs include health care reform, oversight of insurance rates, energy policy, protecting privacy rights, protecting legal rights, corporate reform, and political accountability.

OMB Watch

OMB Watch is a nonprofit research and advocacy organization in Washington, D.C., dedicated to providing citizens and activists with the information, tools, and opportunities they need to participate in the policymaking that directly affects their lives and communities. OMB Watch has particular interest in ensuring that federal information policy supports transparent and accountable government.

Privacy Activism

PrivacyActivism is a non-profit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal level.

Remar Sutton, Founder, Privacy Rights Now Coalition

Privacy Times

Since 1981, Privacy Times has provided its readers with accurate reporting, objective analysis and thoughtful insight into the events that shape the ongoing debate over privacy and Freedom of Information.

World Privacy Forum

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. The organization is focused on conducting in-depth research, analysis, and consumer education in the area of privacy.

SUMMARY OF THE ARGUMENT

The FISA Amendments Act of of 2008 ("FAA") permits the interception and collection of the private communications of U.S. persons who are suspected of no crime. This threat to privacy is especially acute given the capabilities of the National Security Agency ("NSA") and the absence of meaningful oversight. Where enormous surveillance capabilities and blanket secrecy coexist, the public may reasonably fear the interception and collection of private communications.

ARGUMENT

The rules and practices regarding electronic surveillance have changed substantially since the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197, and the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783. The federal Wiretap Act requires the government to report in detail on the use of electronic surveillance authority. 18 U.S.C. § 2519, which until 20003, accounted for the majority of court-approved wire surveillance. *See generally*, EPIC, *Wiretapping*;[3] Administrative Office of the United States Courts,

---

[3] *Available at* http://epic.org/privacy/wiretap/ (last accessed Sept. 20, 2012).

Wiretap Reports.[4] For thirty years the FISA required the government to provide specific, targeted requests aimed at agents of foreign powers and other non-U.S. persons before lawful surveillance was permissible.

The FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261, 122 Stat. 2463, replaced that system with one of broad authority with limited prohibitions on the interception and collection of communications involving U.S. persons. *See* FAA § 702 (codified at 50 U.S.C. § 1881a). The FAA, as adopted, 50 U.S.C. §§ 1881a *et seq*, expanded executive authority to conduct surveillance without particularized suspicion where a "significant purpose" is to obtain "foreign intelligence." § 1881a(g)(2)(A)(v). Such acquisitions are conducted subject to certain "targeting" and "minimization" procedures established by the Director of National Intelligence ("DNI") and the Attorney General, which are reviewed annually by the FISA Court of Review ("FISC"). *See* 50 U.S.C. § 1881a(d) and (e). There are a limitations to acquisition under the FAA.[5] However,

---

[4] *Available at* http://www.uscourts.gov/Statistics/WiretapReports.aspx.

[5] There are only five statutory limitations to acquisition under Section 702 of the FAA. The "acquisition" may not "intentionally target" any of the following: (1) a person "known at the time of acquisition to be located in the United States;" (2) a person "reasonably believed to be located outside the United States" if the purpose is to target "a particular, known person reasonably believed to be in the United States;" (3) a "United States person" believed to be located outside of the United States. 50 U.S.C. §

because the limitations are focused on "targeting" rather than collection, the limitations do not prevent broad collection of international and domestic communications, without significant judicial, legislative, or public oversight. This approach is commonly described as "programmatic surveillance." *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 Tex. L. Rev. 1633 (2010).

Given the authorities established by the FAA, the capacity of the National Security Agency ("NSA") to collect domestic communications, and the lack of public understanding and reporting on the operation of FAA surveillance, it is reasonable for Respondents to believe that there is an imminent threat that their international communications will be intercepted. An expert panel of the National Academies found that the public's awareness of the government's capacity to monitor their private communications "is compounded by attempts to justify past incidents as having been required for purposes of national security. Such an approach both limits public scrutiny and vitiates policy-based protection of personal privacy." Comm. to Study Nat'l Cryptography Policy, Computer Sci. & Telecomms. Bd., Nat'l Research Council, *Cryptography's Role in*

1881a(b). The Government also may not "intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id.*

Securing the Information Society (Kenneth W. Dam & Herbert S. Lin eds., 1996). "Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance." Bruce Schneier, *The Eternal Value of Privacy*, Wired (May 18, 2006).[6] It is also important to consider the impact that monitoring has on other values, because "[a] realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior." Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1424 (2000).

The interception of private communications is difficult to detect. Unlike physical entry into a home or the seizure of private property, electronic surveillance routinely occurs without any noticeable disturbance to the target or to surveilled innocent bystanders. "It is inherent in telecommunication — and inseparable from its virtues — that the sender and receiver of a message have no way of telling who else may have recorded a copy." Whitfield Diffie and Susan Landau, *Privacy on the Line* 175 (2007). Federal wiretap law addressed this problem by establishing both public reporting requirements, 18 USC § 2519, and Government notification requirements, once an investigation is closed, to those who had been the subject of surveillance. 18

---

[6] *Available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886.

U.S.C. § 2518(8)(d) (Wiretap Act notification provision); 50 U.S.C. § 1806(c) (FISA notification provision). These notification procedures help ensure accountability. However, subject notification has been eliminated under the FAA. By limiting reporting and eliminating the notification procedures that existed under previous wiretap law, the FAA has done much to undermine means of accountability.

In the absence of public reporting, similar to the annual reports provided for Title III wiretaps, the Respondents and others who engage in international communications may reasonably fear that their communications will be intercepted. The Inspector General of the Intelligence Community recently informed U.S. Senators that it is "beyond the capacity" of NSA to determine how many U.S. persons' communications the NSA has intercepted. Letter from I. Charles McCullough III, Inspector General of the Intelligence Community, to Senators Ron Wyden and Mark Udall, Senate Select Committee on Intelligence (June 15, 2012).[7]

The FAA limits the Attorney General and Director of National Intelligence's ability to "intentionally target" a U.S. person when acquiring intelligence information. See 50 U.S.C. § 1881a(a)-(b). However, this "intentional targeting" would occur after, not before, the collection of raw

---

[7] *Available at* http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.

communications data.[8] The NSA has the capability to collect traffic from entire networks and infrastructures without "intentionally targeting" any particular person. "As of 1995, NSA was capable of intercepting the equivalent of the entire collection of the U.S. Library of Congress (one quadrillion bits of information) every three hours, and this figure has increased by several orders of magnitude since 9/11." Matthew M. Aid, *The Secret Sentry* 300 (2009). Thus, as part of a program of surveillance, the NSA could gather the raw data of all communications into or out of a particular point on the grid (be it a city, region, or country), and store it for later exploitation and analysis.[9]

---

[8] Some early estimates of the Presidential Surveillance Program indicated that thousands of U.S. citizens had "conversations recorded and read by intelligence analysis," but "[t]he program has touched many, many more Americans than that." Barton Gellman, Dafna Linzer, & Carol D. Leonnig, *Surveillance Net Yields Few Suspects*, Washington Post, Feb. 5, 2006, at A01. "Surveillance takes place in several stages, officials said, the earliest by machine. Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States before selecting the ones for scrutiny by human ears." *Id.*

[9] This approach is exemplified in the official "consumer's guide" outlining how the intelligence community operates. Office of the Dir. of Nat'l Intelligence, *U.S. National Intelligence: An Overview* (2011) available at http://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf. The guide says that "collection" of raw data occurs at the stage prior to the "processing and exploitation" stage. Id. at 11.

This Court has held that a party may have standing when the government operates a program that is likely to affect the party, even if the party has only a reasonable suspicion, "at the pleading stage," that the government program will target them specifically. *See Bennett v. Spear,* 520 U.S. 154, 167-68 (1997). Likewise in this case, without subject notification and public reporting to show whether or not the government is intercepting the communications of U.S. persons through its programmatic FAA surveillance, it is understandable that respondents are concerned that their communications would be swept up in the vast signals interception program.

I. The NSA's SIGINT Capabilities and Past Practices Support a Reasonable Belief That the Communications of United States Persons Will Be Intercepted

The Director of National Intelligence currently controls the enormous infrastructure of the U.S. Intelligence Community. Since its inception, the

---

"Exploitation" is defined as "[T]he process of obtaining intelligence from any source and taking advantage of it for intelligence purposes." Id. at 80. Thus, the mere collection of raw data would not constitute "obtaining intelligence" because that occurs at this later exploitation step. If intelligence is not obtained until raw data is exploited, then intentional targeting to acquire intelligence does not occur until after the raw data (e.g. electronic communications) have already been collected.

NSA's mission has been to provide its signals intelligence product ("SIGINT") to these agencies, including the Central Intelligence Agency, the Federal Bureau of Investigation, and the State Department. *See* George Brownell, *The Origin and Development of the National Security Agency* (1981).

The NSA is charged with providing "the technical expertise necessary to create" mass surveillance programs, like the recent "President's Surveillance Program" conducted from 2001-2007. Office of the Inspector General of the Dep't of Def. et al., *Unclassified Report on the President's Surveillance Program* 1 (2009). Thus, NSA coordinates with the seventeen other intelligence community organizations to obtain intelligence under the direction of the DNI. *See* Office of the Dir. of Nat'l Intelligence, *U.S. National Intelligence: An Overview* (2011).

This intelligence-gathering activity involved the collection of the communications of United States persons without a warrant, as described by former NSA Director Michael Hayden. In a recent speech, General Hayden discussed efforts to "dial things up a bit" in response to the attacks of September 11, 2001. General Michael Hayden, *Law, Policy, and the War on al-Qaida: An Emerging Consensus?*, Lecture from the Gerald R. Ford School of Public Policy (Sept. 7,

2012).[10] General Hayden discussed the 9/11 Commission's criticism that the NSA was too "timid" on the collection of certain communications that might be related to terrorist activities. "In other words communications [with] one end here – here in the United States." *Id.* The former NSA Director stated the President's authorization of increased intelligence gathering would result in a "higher probability you're going to intercept the communication, one end of which might be in the United States related to the al-Qaeda threat . . . ." *Id.*

The result was the warrantless wiretapping program that was first revealed in a New York Times expose, later described in an official Inspector General's Report, and eventually led to the enactment of the FAA. *See* Eric Licthtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 16, 2009 at A1. As General Hayden said, "[t]he FISA Act not only legitimated everything President Bush had told me – almost everything President Bush had told me to do under his Article II authorities as commander-in-chief – but, in fact, gave the National Security Agency a great deal more authority to do these kinds of things . . . ." Hayden, *supra*.

The NSA has the ability to engage in broad collection of electronic messages, and the

---

[10] Transcript is available at http://www.fordschool.umich.edu/files/transcripts/2012-hayden-rosenthal.txt.

communications of U.S. persons are invariably swept up by the agency. This programmatic surveillance presents an imminent threat that the international communications of U.S. persons will be intercepted.

A. The NSA Has an Almost Boundless Capacity to Intercept Private Communications, Including Those of U.S. Persons

The National Security Agency has coordinated SIGINT activities since its inception in 1952,[11] and its interception network has grown to match the enormous volume of global communications. In 1975, Senator Frank Church warned that the NSA apparatus "at any time could be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter." James Bamford, *The Puzzle Palace* 389 (1982) (quoting *Meet the Press* (NBC television broadcast Aug. 17, 1975). The NSA's intelligence-gathering infrastructure has grown exponentially

---

[11] *See* Memorandum from President Harry S. Truman to Sec'y of State and Sec'y of Defense, *Communications Intelligence Activities* (Oct. 24, 1952), *available at* http://www.nsa.gov/public_info/declass/truman.shtml.

since the Church Committee uncovered its domestic surveillance programs in the mid-1970s.[12]

The system of interception and collection as it currently exists likely incorporates the majority of traffic passing through United States telecommunications lines. Former Director Mike McConnell recently stated that eliminating "any telephone transmission or e-mail that incidentally flowed into U.S. computer systems" and other U.S. traffic would reduce the NSA's intercept capacity "by seventy per cent." Lawrence Wright, *The Spymaster*, The New Yorker (January 21, 2008). The result is collection of the private communications of U.S. persons, no matter how "incidental" to other targets. As Director McConnell noted in his discussion of the debates surrounding enactment of the FAA, "[n]aturally, some innocent Americans would be overhead . . . . What do you do about it?" *Id.* Both of these intelligence directors see collection of United States persons' communications as a natural, if unfortunate, result of the FAA system.

Previously, in the absence of meaningful oversight, the NSA routinely collected the private communications of U.S. persons. "[F]rom August 1945 to May 1975, NSA obtained copies of many international telegrams sent to, from, or through the United States from three telegraph companies." Final

---

[12] *See* Final Report of the S. Select Comm. to Study Gov't Op. with Respect to Intelligence Activities (Book II), S. Rep. No. 94-755 (1976).

Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book III), S. Rep. No. 94-755 at 735 (1976) [hereinafter *Church Committee Report*]. In addition, the "NSA targeted the international communications of certain American citizens" from the 1960s through 1973. *Id.* Thus the NSA conducted domestic surveillance even though its mission "is directed to *foreign intelligence*. . . ." *Intelligence Activities – The National Security Agency and Fourth Amendment Rights: Hearing Before the S. Select Committee to Study Governmental Operations With Respect to Intelligence Activities* (1975) (testimony of Lt. Gen. Lew Allen, Jr., Director, National Security Agency).

Despite internal NSA policies and directives intended to limit the interception of U.S. persons' communications, such communications were in fact intercepted by the agency pursuant to three programs including "Operation SHAMROCK," and information derived from such communications was "disseminated by NSA to other intelligence agencies." Church Committee Report, *supra*, at 738. Through SHAMROCK the NSA gained access to "virtually all the international telegrams of Americans" carried by two of the three major telecommunications providers, and NSA analysis reviewed an estimated 150,000 messages per month in later years.[13] *Id.* at 740. The

---

[13] The collected messages were initially sorted manually, but the NSA transitioned to an "electronic sorting process" that allowed

companies hesitantly agreed to participate in this program after receiving repeated assurances from the Attorney General and the Secretary of Defense that their participation in the program was legal. *See* Memorandum from Record, Armed Forces Security Agency, *SHAMROCK Operations* (Aug. 25, 1950); Church Committee Report at 768-69.

The NSA quickly expanded its capability to intercept international communications beyond telegraphs to voice and other electronic communications. As early as 1970, the NSA "had access to international calls placed from, or received in, cities all over the United States that were switched through New York." Church Committee Report at 741. It used this access to assist the Bureau of Narcotics and Dangerous Drugs in monitoring select phone calls "between the United States and certain countries in South America," a function which the CIA later determined violated the National Security Act of 1947. *Id.*

More recently, the NSA collaborated with other intelligence organizations on a program known as "ECHELON," a data sharing agreement involving the UK, the USA, Canada, Australia and New Zealand ("UKUSA") for the purposes of intelligence interception. European Parliament: Temporary Committee on the ECHELON Interception System,

---

them to select particular communications based on key terms (like the name of the sender or recipient). Church Committee Report at 765.

Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), 1 July 2001.[14] While the NSA and its UKUSA intelligence partners had been exchanging intercepted communications since the beginning of their partnership in 1946, the development of ECHELON allowed the UKUSA partners to pool all of their signals intelligence data automatically. James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, 394-404 (1st ed. 2002). As a result, "agencies would be able to submit targets to one another's listening posts and, likewise, everyone would be allowed to share in the take – to dip their electronic ladles into the vast cauldron of intercepts and select what they liked." *Id* at 404.

The NSA is currently building a $2 billion data center in Buffdale, Utah that will encompass 1 million square feet. James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, Wired, Mar. 15, 2012 [hereinafter *Bamford Wired Article*].[15] 100,000 square feet of the data center will be filled with servers. *Id.* With this type of capacity, the NSA could access and collect a majority of US-to-international telecommunications

---

[14] Available at:
http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

[15] *Available at*
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

traffic. *See id.* Reports indicate that this has largely been accomplished through "backdoor access" via arrangements with "some of the nation's largest telecommunications companies." James Risen & Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times (Dec. 24, 2005). One senior NSA official even confirmed that in 2006 "the N.S.A. had access to records of most telephone calls in the United States" because in order to perform the types of traces they used "you'd have to have all the calls or most of them." Eric Lichtblau & Scott Shane, *Bush is Pressed Over New Report on Surveillance*, N.Y. Times (May 12, 2006).[16]

This NSA's SIGINT apparatus collects communications through a number of different channels: eavesdropping satellites that orbit the earth, secret monitoring rooms in U.S. telecom facilities, monitoring of satellite dishes in the US, and taps on overseas communication links. James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, Wired, Mar. 15, 2012.[17] According to the agency, the nature of modern communications requires the NSA to "live on the network" in order to "perform both its offensive and defensive missions." National Security Agency,

---

[16] *Available at* http://www.nytimes.com/2006/05/12/washington/12nsa.html.

[17] *Available at* http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

Transition 2001 at 31 (Dec. 2000).[18] All this information can now be stored in one central location—the Utah Data Center.

According to James Bamford, the only thing stopping the NSA from complete access to all the collected information is encryption. *See id.* NSA is working on building the world's fastest supercomputer at its Oak Ridge, Tennessee facility, in order to break the encryption on the mounds of data it "currently collects". *Id.*

The routine collection and storage of domestic communications is a significant concern. Former telecommunications provider and NSA employees have noted that the NSA has installed intercept equipment at key junction points where domestic communication can be captured. *See Declaration of Mark Klein in Support of Plaintiffs' Motion for Partial Summary Judgment*, *Jewel v. NSA*, No. 08-4373 (N.D. Cal. Jul. 2, 2012); *Declaration of William E. Binney in Support of Plaintiffs' Motion for Partial Summary Judgment* ¶ 8, *Jewel v. NSA*, No. 08-4373 (N.D. Cal. Jul. 2, 2012) [hereinafter *Binney Decl.*].

The capabilities of the NSA go beyond the ability to capture and store massive amounts of data. As another former NSA employee points out, the "NSA has the capability to do individualized searches, similar to Google, for particular electronic

---

[18] *Available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf.

communications in real time through such criteria as target addresses, locations, countries and phone numbers, as well as watched-listed names, keywords, and phrases in email." *Declaration of Thomas A. Drake in Support of Plaintiffs' Motion for Partial Summary Judgment* ¶ 8, *Jewel v. NSA*, No. 08-4373 (N.D. Cal. Jul. 2, 2012) [hereinafter *Drake Decl.*]. Former NSA employees estimate that the agency is now collecting most if not all communications in U.S. and analyzing these communications later from static databases. *See Binney Decl.* ¶ 13-17; *Drake Decl.* ¶ 8-9.

B. Current Technologies Developed by Intelligence Contractors and Other Agencies Show That the Government Is Capable of the Type of Broad Signal Collection That Respondents Allege

The NSA has long depended upon technological development by private contractors and researchers. In addition to the traditional research and development model, a more direct market for surveillance technology has developed over the last 10 years into a $5 billion industry. Jennifer Valentino-Devries et al., *Document Trove Exposes Surveillance Methods*, Wall St. J. (Nov. 19, 2011). These technologies are showcased for U.S. Intelligence Agencies each year at the Intelligence Support Systems World conference held by

TeleStrategies. *See* TeleStrategies, *ISS World Americas 2012*.[19] More than 244 U.S. agencies, including the Office of the Director of National Intelligence, attended the 2011 surveillance technology conference. *See* Valentino-Devries, *supra*. Given the Government's access to and involvement in this market, the technologies showcased clearly represent a baseline of their surveillance capabilities.

The Wall Street Journal obtained documents from the 2011 surveillance conference, which provide insight into the capabilities of modern intelligence agencies such as the NSA and the CIA, as well as the FBI. This includes technology to enable massive interception of electronic communications, such as OnPath Technologies.[20] The Telesoft Technologies *Hinton 5000 Interceptor*, described in one of the brochures, can provide "the target or mass capture of 10s of thousands of simultaneous conversations from fixed or cellular networks for law enforcement or

---

[19] *Available at* http://www.issworldtraining.com/ISS_WASH/index.htm (last accessed Sept. 17, 2012).

[20] The CEO of OnPath, a New Jersey company, is quoted as saying "[w]e're allowing a whole new level of intelligence in the networks . . . . We can take a copy of everything coming through our switch and dump it off to the FBI." Wall Street Journal, *The Surveillance Catalog: OnPath Technologies – Notes* (2011), *available at* http://projects.wsj.com/surveillance-catalog/documents/267794-documents-266211-onpath-technologies-lawful/ (last accessed Sept. 17, 2012).

intelligence purposes." Wall Street Journal, *The Surveillance Catalog: Telesoft Technologies* (2011).[21]

In addition to off-the-shelf surveillance technologies, the NSA is developing new techniques to enable the interception of communications. For example, "EINSTEIN 3" filters Internet traffic around certain hubs and automatically reroutes information marked by a "threat signature" through an "Access Provider" for further analysis by a government agency. Dep't of Homeland Sec., Privacy Impact Assessment for the Initiative Three Exercise, Mar. 18, 2012.[22] The NSA developed EINSTEIN 3 to "identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to *automatically* detect and respond appropriately to cyber threats before harm is done." *Id* (emphasis added). The EINSTEIN software is able to make this kind of determination by analyzing the content of the emails and other electronic messages that are sent to or from government agencies., "EINSTEIN monitors not only federal executive agency employees' work e-mails or other official Internet activity, but also any information accessed

---

[21] *Available at* http://projects.wsj.com/surveillance-catalog/documents/267027-telesoft-technologies-hinton-5000-interceptor/#document/p1/a38601 (last accessed Sept. 17, 2012).

[22] Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf [accessed Sept. 17, 2012].

on a federal agency computer including personal e-mails accessed from sites such as Gmail or Hotmail, or other Internet communications such as Facebook and Twitter." Edward C. Liu et. al., Cong. Research Serv., R42409, *Cybersecurity: Selected Legal Issues* (Mar. 14, 2012).

In the lexicon of EINSTEIN 3's real-time full packet inspection, a "threat signature" is a designation given to a "pattern of network traffic" that has been identified by NSA as potentially compromising government information. Privacy Impact Assessment at 7. These signatures do not necessarily identity harmful traffic – they can identify either "known or suspected cyber threats." *Id.* For example, "a specific signature might identify a known computer virus," or "for example phishing, IP spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware." *Id.* at 4.

EINSTEIN 3 operates by automatically detecting these "threat signatures determined by NSA" and then rerouting the incoming information, along with an explanatory memo, to a special department within DHS where it is tagged with an "alert" and stored for review by analysts. *Id.* at 5.

This report reveals two important facts about NSA's capabilities. First, it reveals that NSA's technical competencies include a network rerouting system that can automatically scan, intercept, store, and subject to analytic scrutiny all emails going in and out of government computers that are tagged in a particular way. Liu at 15. Second, it reveals that

the communications of all federal employees – or of anyone using a federal government internet connection – are potentially subject to screening and analysis. This means that recipients of "tagged" communications could find their emails intercepted and blocked if, for example, they forwarded or replied to tagged messages. *Id.* at 17. As one expert has warned, "while earlier iterations of Einstein implemented signatures based on malicious computer codes, Einstein 3 could include signatures based on personally identifiable information. The privacy implications are great. Any citizen logging on to a ".gov" website would trigger this." Jesselyn Radack, *NSA's Cyber Overkill: A Project to Safeguard Governmental Computers, Run by the NSA, Is Too Big a Threat to Americans' Privacy,* L. A. Times, July 14, 2009.[23]

II. Without Adequate Public Reporting, Respondents' Apprehension That NSA Intercepts the Communications of U.S. Persons is Reasonable

The FAA grants broad surveillance authority with little oversight. Unlike the Wiretap Act, this statute does not contain substantive public reporting or notification provisions. Without such provisions, there is no public mechanism to ensure that the privacy of communications is ensured for United

---

[23] *Available at* http://articles.latimes.com/2009/jul/14/opinion/oe-radack14.

States persons. The need to establish effective oversight for government surveillance, including matters involving national security, is well understood and a long-standing concern. In 1971, a conference led by students at Princeton University highlighted the importance of standing for those "indirectly" effected by electronic surveillance to challenge the collection. *Boundaries of Privacy*, *infra*, at 35 ("Commission II - State & Local Gathering Data-Gathering Activities" at 2). "A Federal Court of Warrants should be created to issue warrants for electronic surveillance in all cases involving national security." Samuel Alito, *The Boundaries of Privacy in America* 5 (1972) ("Report of the Chairman"). The Report of the Chairman of that conference, Samuel Alito, recognized both that "the usual procedures [for electronic surveillance] may be inappropriate in cases involving the national security," and that the "system proposed by the government is highly susceptible to abuses." *Id.* Therefore the system requires specific oversight procedures to ensure that privacy rights are not violated.

A. The Wiretap Act Provides for Public Reporting That Details the Number of Persons Affected by Interception

Under provisions of the Wiretap Act, judges and the Attorney General must submit annual reports to the Administrative Office of the United States Courts detailing wiretap orders. 18 U.S.C. § 2519. These reports include the type of orders granted or denied, interception durations, offenses

under investigation, the frequency of incriminating and collateral interceptions, the number of persons affected, costs, and the number of resulting arrests, trials, and convictions. § 2519(1)-(2). The Administrative Office then reports this data to Congress. § 2519(3).

This report is likely the most comprehensive report on wiretap authority produced by any government agency in the world. *See Hearing on the FISA Amendments Act of 2008: Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary* (2012) (testimony and statement of Marc Rotenberg, Executive Director, EPIC). People might disagree over whether the federal government engages in too much or too little electronic surveillance, but this annual report provides a basis to evaluate the effectiveness of wiretap authority, to measure its cost, and even to determine what percentage of communications captured are relevant to an investigation.

These reports allow Congress and the public to evaluate the efficiency of government programs and ensure that civil rights are protected. Furthermore, such reports do not reveal sensitive information about particular investigations, but rather provide aggregate data about the government's surveillance activities.

B. The FAA Provides for No Public Reporting and Minimal Oversight of Collection on a Mass Scale

In contrast, the FAA lacks adequate public oversight. The public, the judiciary (but for the FISC) and almost all Members of Congress are kept in the dark as to the most extensive electronic surveillance program undertaken by the US government. While the DNI and Attorney General provide internal reporting requirements,[24] none of this information is made available to the whole Congress or the public broadly, and thus no meaningful public oversight can occur. In addition, the reports only relate to the application of "minimization" procedures, which are themselves inadequate to prevent the injury of collection. Director McConnell made clear before the FAA was passed that "minimization" occurs after the communications have already been collected.[25] *See Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II): Hearing Before the H. Comm. on the Judiciary*, 110th Cong. 79 (2007) (testimony of J. Michael McConnell, Dir. Of Nat'l Intelligence).

---

[24] The Attorney General and DNI semi-annually report targeting and minimization procedural compliance to only the Foreign Intelligence Surveillance Court ("FISC"), congressional intelligence committees, and congressional judiciary committees. 50 U.S.C. § 1881a(l)(1). Each intelligence agency's inspector general submits similar semi-annual assessments. §

The Attorney General's annual FISA letter, which is the only publicly available document discussing the application of the law, provides little information about the use of FISA authority other than the total number of (1) FISA applications made to the FISC, (2) FISA requests for electronic surveillance, (3) FISA requests withdrawn, denied, or modified, and similar information about access to business records and National Security Letters. *See*, *e.g.*, Letter of Ronald Weich, Assistant Attorney General, U.S. Dep't of Justice to the Honorable Joseph R. Biden, Jr., President, United States Senate

---

1881a(l)(2). Agencies also conduct an annual review of FISA-authorized "acquisitions" and account for their impacts on domestic targets and American citizens. § 1881(a)(l)(3).

[25] This is exemplified by an exchange, which occurred during the hearing:

> REP. BERMAN: … How do you minimize without knowing?
>
> MR. MCCONNELL: If you look at it, then you know.
>
> REP. BERMAN: So all you do is minimize the ones you happen to look at.
>
> MR. MCCONNELL: Right. If there is something in there that – it doesn't come up for some reason, you just wouldn't know …

Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II): Hearing Before the H. Comm. on the Judiciary, 110th Cong. 79 (2007) (testimony of J. Michael McConnell, Dir. Of Nat'l Intelligence).

(Apr. 30, 2012) (2011 FISA Letter).[26] The letter does not even distinguish between traditional FISA orders and programmatic surveillance orders under the FAA.[27] There is no information about cost, purposes, effectiveness, or even the number of non-incriminating communications of U.S. persons the government collects. Under the new procedures that authorize programmatic surveillance without a specific target, it is almost impossible to assess and compare the aggregate numbers of individuals affected by interception since passage of the FAA.

Furthermore, the degree of oversight by the FISC is elusive at best. Often referred to as a secret court, the FISC rarely publishes any substantive information regarding the cases it hears; only a handful of written opinions have been released since the Court's inception.[28]. The only information currently available about the FISC on the U.S. Courts website is its adopted rules of procedure from November 2010. *See* U.S. Foreign Intelligence

---

[26] *Available at* http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[27] This is significant because while a traditional FISA order has a narrow scope, the number of communications impacted by an FAA order is essentially unbounded.

[28] It is clear from the Attorney General's annual reports that FISC applications are routinely approved with very rare exceptions. EPIC, *Foreign Intelligence Surveillance Act Orders 1979-2011*, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Sept. 20, 2012).

Surveillance Court, *Rules of Procedure*, Nov. 1, 2010.[29] *See also* EPIC, *Comments to Proposed Amended FISC Rules* (Oct. 4, 2010).[30]

In a prescient comment about proposed changes in FISA procedures a decade ago, Senator Patrick Leahy noted:

> We were talking about development of the secret body of laws without public scrutiny, and that is very unusual, not only in our democracy but any democracy. The Department is urging broader use of the FISA in criminal cases. And you are going to lose, ultimately lose public confidence both in the Department and in the courts, unless you can, by public reporting or otherwise show this is being used appropriately.

The USA PATRIOT Act in Practice: Shedding Light on the FISA Process: H. Before the S. Comm. on the Judiciary, 107th Cong. 37-38 (2002).

---

[29] *Available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/FISC2010.pdf

[30] http://epic.org/privacy/terrorism/fisa/EPIC%20Comments_FISC%202010%20Proposed%20Rules.pdf

C. Increased Public Reporting and Oversight Would Enable Meaningful Review and an Evaluation of Costs and Benefits

In the FAA reauthorization currently pending in Congress, proposed amendments to the FAA seek to address this lack of accountability by requiring enhanced inspector general scrutiny and unclassified, publicly available reports. Such public reporting would not only ensure greater accountability, it would also strengthen the executive's ability to protect national security.

For example, Representative Scott (D-VA) proposed an amendment that would require reviews under Section 702(l) of the FAA to be "provided in unclassified form," which would encourage public accountability for surveillance programs under Section 702. H.R. Rep. No. 112-645, pt. 1, at 7 (2012). Representatives Nadler (D-NY) and Schakowsky (D-Ill) proposed an amendment that would require the Attorney General to "make publicly available" unclassified summaries of FISC opinions that "includ[e] a significant construction or interpretation of section 702" and have been submitted to Congress. *Id.* at 6. Representative Jim Sensenbrenner (R-Wisc.) agreed at a recent FAA reauthorization hearing, noting that "perhaps decisions of the FISA Court, particularly review of the FISA court appropriately redacted, would be able to give us the answer . . . ." *The FISA Amendments Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland*

Security of the H. Comm. on the Judiciary, 112th Cong. (2012) (statement of Chairman Sensenbrenner).

The publication of FISC opinions regarding the legal interpretation of Section 702 would promote understanding of the system and limit any potential misconceptions based on the plain text of the FAA. The House of Representatives accepted neither of these amendments, and as a result the current FAA system lacks significant public oversight and accountability.

Senator Patrick Leahy has proposed amendments that would add public reporting and accountability procedures. *See, e.g.,* S. 3276, 112th Cong. §3 (2012) ("Leahy Amendment"). The amendment provides for a new review and public report to be issued by the Inspector General of the Intelligence Community, which would focus on the impact of FAA surveillance on the communications of U.S. persons. Such a report would clarify the effect of this law on the privacy of individuals in Respondents' position. The Senate has yet to act on the measure.

Former Assistant Attorney General Jack Goldsmith recently noted that, inspectors general are "an established, legitimate, and consequential mechanism of executive branch accountability." Jack Goldsmith, *Power and Constraint* 106 (2012). As Professor Goldsmith noted, "credible independent inspectors general inside the executive branch can enhance executive power." *Id.*

In order to maintain both security and privacy, the government requires complimentary tools that maximize efficiency. When the law gives new authority to conduct electronic surveillance, there should also be new means of oversight and accountability. The FISA Amendments Act fails this test. There is simply too little known about the operation of the FISA today to determine whether it is effective and whether the privacy interests of Americans are adequately protected. What is needed is what Professor Charles Fried has described as a "well-grounded degree of protection against arbitrary abuse of investigative power." Charles Fried & Gregory Fried, *Because It Is Wrong* 107 (2010).

Legal actions brought by parties seeking to safeguard electronic privacy, such as those of Respondents, form a vital part of our system of checks and balances. As Professor Goldsmith has noted, "[t]his is all very healthy for the presidency and for national security," because the continued efficacy of executive branch oversight "depends on just this type of skeptical attitude about its efficacy." Goldsmith, at 241. The ability of Respondents to have their claims heard is thus essential not only to protect privacy, but also to safeguard national security.

CONCLUSION

For the foregoing reasons EPIC respectfully asks this Court to uphold the decision of the Second Circuit below.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

September 24, 2012