BRENNAN CENTER
FOR JUSTICE

at New York University School of Law

U.S. SURVEILLANCE: UNCHECKED AND UNSUPERVISED

A shadow report by the Brennan Center for Justice
at *New York University School of Law*
prepared for the United Nations Human Rights Committee
on the occasion of its review of

The United States of America's Fourth Periodic Report
to the UN Committee on Human Rights Concerning the
International Covenant on Civil and Political Rights

September 2013

TABLE OF CONTENTS

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from racial justice in criminal law to constitutional and human rights protection in the fight against terrorism.

The Liberty and National Security Program at the Brennan Center promotes national security policies that are both effective and respect human rights values and the rule of law. The Program focuses on revamping data collection programs to protect the privacy of individuals; restoring the proper flow of information between the government and the people by securing increased public access to government information; ensuring government counterterrorism policies are free of religious and ethnic biases; and bolstering oversight and accountability of the national security establishment.

I. INTRODUCTION & ISSUE SUMMARY

Advances in technology have allowed governments to dramatically increase surveillance of private persons. Legal safeguards have not kept pace. Surveillance programs now operate in ways that fundamentally undermine individual rights under the International Covenant on Civil and Political Rights (ICCPR). Recent reports show that the U.S. government is collecting and analyzing an enormous amount of their own citizens' communications, as well as those of persons in other countries. Inadequate judicial oversight over the government's surveillance programs exposes both U.S. and non-U.S. persons to systematic invasions of their right to privacy (Article 17), and their related rights to free speech (Article 19) and association (Article 22). Moreover, laws that make it difficult for individuals to challenge government surveillance programs deprive them of an effective judicial remedy for possible violations of their privacy, speech and association rights (Article 2(3)).

The Committee first expressed concern about the surveillance programs carried out by the U.S. National Security Agency (NSA) after a 2005 *New York Times* report that the agency had been collecting the electronic communications of Americans without the court issued warrant traditionally required under the U.S. Constitution.[1] In its 2006 List of Issues, the Committee expressed concern about the lack of "any judicial oversight" of the programs and questioned whether they complied with Article 17 of the ICCPR.[2] Although the U.S. government initially did not respond to the Committee's questions, its 2011 periodic report stated that the NSA's surveillance programs were brought under the judicial supervision of the Foreign Intelligence Surveillance Court (FISC) in 2008, when the Foreign Intelligence Surveillance Act (FISA) was amended by Congress to "solidify the role of the FISC in approving electronic surveillance."[3]

But instead of increasing oversight of the United States' surveillance operations, the 2008 FISA Amendments Act (FAA) has played a key role in expanding the government's authorities to collect billions of pieces of private data around the world. Information about these programs was kept secret and only became known to the public through leaks by a former NSA contractor, Edward Snowden. While the full extent of U.S. surveillance is not yet known, valuable information has emerged from Snowden's revelations and the government's release of previously classified documents. A few important surveillance programs bear mention:

---

[1] Eric Lichtblau & James Risen, *Eavesdropping Effort Began Soon after Sept. 11 Attacks*, N.Y. TIMES, December 18, 2005, *available at* http://www.nytimes.com/2005/12/18/politics/18spy.html?_r=0.

[2] U.N. Human Rights Comm., *List of Issues to be Taken Up in Connection with the Consideration of the Second and Third Periodic Reports of the United States of America* ¶ 13, at 4, U.N. Doc. CCPR/C/USA/Q/3 (Apr. 26, 2006), *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G06/426/26/PDF/G0642626.pdf?OpenElement.

[3] U.S. DEP'T OF STATE, FOURTH PERIODIC REPORT OF THE UNITED STATES OF AMERICA TO THE UNITED NATIONS COMMITTEE ON HUMAN RIGHTS CONCERNING THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS ¶585-586 (2011), *available at* http://www.state.gov/j/drl/rls/179781.htm.

- *Collection of telephone metadata*: Under the PATRIOT Act, the U.S. government is entitled to obtain any business record or other "tangible things" (such as phone records) if deemed "relevant" to a terrorism or foreign intelligence investigation.[4] This provision of the law was interpreted by the FISC to allow the government to collect information about *all* phone calls made to, from and within the United States.[5] Such telephone metadata – which includes data on who a person calls, when, for how long and from where – can be aggregated to form a detailed picture of a person's life.[6] U.S. Supreme Court Justice Sonia Sotomayor recently observed in a case involving location monitoring that metadata "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[7] The government is also reportedly gathering metadata about Americans' emails, although less is known about this program.[8]

- *Collection of telephone and Internet communications, including their contents:* The content of telephone and Internet communications have been collected separately under a provision of FAA that authorizes the acquisition of foreign intelligence information.[9] One program, called Upstream, copies both the content and metadata of communication passing through undersea fiber-optic cables in the U.S. and abroad,[10] which carry 99% of international phone and Internet data.[11] Another

---

[4] USA PATRIOT Act of 2001, 50 U.S.C. § 1861 (2013); *see also* Spencer Ackerman, *Obama Publishes Legal Background to Surveillance – But Much Is Still Unclear*, GUARDIAN, August 9, 2013, *available at* http://www.theguardian.com/world/2013/aug/09/obama-legal-background-surveillance-nsa.

[5] In re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Dec. 12, 2008), *available at* https://www.aclu.org/files/assets/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.

[6] This was vividly demonstrated when German Green Party politician Malte Spitz sued Deutsche Telekom to give him 6 months of the phone metadata they had collected in 2009 and 2010. ZEIT ONLINE used this information and Spitz's other public work-related and social media information to create a map of his life, revealing everything from his favorite beer gardens to his preferred means of transportation, when and how long he slept, and where exactly he went on work trips and vacation. *Tell-All* Telephone, ZEITONLINE, http://www.zeit.de/datenschutz/malte-spitz-data-retention. This is the kind of profile the NSA can assemble from the phone metadata it collects alone, not including the even greater privacy breaches allowed by gathering phone content or internet communications.

[7] U.S. v. Jones, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[8] The United States government may be able to access e-mail metadata through Internet intelligence gathering via fiber optic cables. *See e.g.* Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance*, WASH. POST, July 6, 2013, *available at* http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.

[9] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1881a (2013)).

[10] Reports from Brazil, Germany, and Australia find the United States has access to fiber-optic cables and communications facilities abroad. *See* Glenn Greenwald, Roberto Kaz & José Casado, *EUA Espionaram Milhões de E-mails e Ligações de Brasileiros*, O GLOBO, June 7, 2013, *available at* http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934; Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark & Jonathan Stock, *How the NSA Targets Germany and Europe*, SPIEGEL ONLINE (July 1, 2013), http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-

> program called PRISM collects emails, texts, video conversations, photographs, Internet searches, and more from at least 9 leading Internet companies, including Google, Facebook, and Apple.[12]

The United States is part of a global surveillance network that collects and shares private data about hundreds of millions of individuals worldwide. Leaked documents show that the NSA has partnered with the United Kingdom's intelligence agency GCHQ to crack encryption technologies that secure e-mails, banking transactions and other personal records.[13] During the G20 summit in 2009, the NSA also worked closely with the GCHQ to intercept the communications of Russian President Dmitry Medvedev and other government leaders and delegates.[14] The U.S. and the U.K. are also part of an intelligence sharing alliance with Australia, Canada and New Zealand known as the 'Five Eyes.'[15] The nature and scope of their information sharing arrangement is still unknown.[16] A recently leaked memorandum of understanding between the U.S. and Israel reveals that the NSA is sharing large volumes of raw private data with Israeli intelligence. Such data include transcripts of telephone and online communications, voice clips, facsimiles and telephony metadata concerning both U.S. and non-U.S. persons.[17] These intelligence partnerships significantly extend the reach of U.S. surveillance operations, exacerbating the already grave privacy concerns these operations raise.

908609.html; Philip Dorling, *Snowden Reveals Australia's Links to U.S. Spy Web,* SYDNEY MORNING HERALD, July 8, 2013, *available at* http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html.

[11] Justin Elliot, *Does the NSA Tap That? What We Still Don't Know About the Agency's Internet Surveillance*, PROPUBLICA (July 22, 2013, 1:41 PM), https://www.propublica.org/article/what-we-still-dont-know-about-the-nsa-secret-internet-tapping.

[12] James Ball, *NSA's Prism Surveillance Program: How it Works and What it Can Do*, GUARDIAN, June 8, 2013, *available at* http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

[13] James Ball, Julian Borger & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN, Sept. 5, 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[14] Ewan MacAskill, Nick Davies, Nick Hopkins, Julian Borger & James Ball, *GCHQ Intercepted Foreign Politicians; Communicatinos at G20 Summits*, GUARDIAN, June 16, 2013, *available at* http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits; Ewan MacAskill, Nick Davies, Nick Hopkins, Julian Borger & James Ball, *G20 Summit: NSA Targeted Russian President Medvedev in London*, GUARDIAN, June 16, 2013, *available at* http://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit.

[15] Conor Friedersdorf, *Is 'The Five Eyes Alliance' Conspiring to Spy on You?*, ATLANTIC, June 25, 2013, *available at* http://www.theatlantic.com/politics/archive/2013/06/is-the-five-eyes-alliance-conspiring-to-spy-on-you/277190/.

[16] Glenn Greenwald, Laura Poitras & Ewan MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, GUARDIAN, Sept. 11, 2013, *available at* http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[17] *Id.*

II. EXECUTIVE SUMMARY

In its 2013 review of the United States, the Human Rights Committee again highlighted concerns regarding oversight of government surveillance. In particular, its List of Issues asked the U.S. for "information on steps taken to ensure judicial oversight over National Security Agency surveillance of telephone, email and fax communications both within and without the State party."[18] In light of recent revelations about the U.S. government's surveillance programs, the Brennan Center for Justice welcomes this opportunity to comment on the United States' Fourth Periodic Report and the Human Rights Committee's continued concerns regarding judicial oversight of the NSA's surveillance programs.

This report will examine the oversight failures of the FISC. The FISC suffers from three primary deficiencies that inhibit its effectiveness as an oversight mechanism: first, the court's proceedings are entirely closed, resulting in the creation of a secret legal framework that expands the government's surveillance authorities at the expense of the privacy of hundreds of millions of people across the world; second, the FISC is unable to conduct oversight of the vast surveillance programs it authorizes; and third, there is little opportunity for surveillance targets to prospectively or retroactively challenge these programs.

[18] U.N. Human Rights Comm., *List of Issues in Relation to the Fourth Periodic Report of the United States of America* ¶ 22, at 5, U.N. Doc. CCPR/C/USA/4 and Corr.1 (Apr. 29, 2013), *available at* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fQ%2f4&Lang=en.

III. DEFICIENCIES OF THE FISC

The FISC was established in the wake of revelations in the 1970s that major U.S. intelligence and law enforcement agencies were conducting invasive surveillance of American and foreign citizens around the world in violation of their civil liberties and human rights.[19] In 1978, Congress passed FISA to tighten regulation and oversight of the nation's foreign intelligence activities. A cornerstone of FISA was the creation of the FISC, a court that would oversee applications for electronic surveillance and physical searches in foreign intelligence cases but operate largely in secret in order to preserve the integrity of covert surveillance operations.[20]

After 9/11, the oversight role of FISC assumed heightened importance as the U.S. government expanded it surveillance operations. The number of applications submitted to the FISC jumped from 199 in 1979 to 1228 in 2002. [21] In 2012 alone, the FISC heard 1,856 applications. [22] Until recently, the secrecy surrounding FISC proceedings and records has made it almost impossible to determine whether it exercises meaningful oversight of the government's surveillance operations. But recent disclosures, including the declassification and release by the U.S. government of some FISC opinions, show that the FISC is ill-equipped to supervise vast intelligence collection programs and protect the privacy rights of Americans, much less foreign citizens. It is entirely dependent on the NSA to report violations of the minimal privacy protections the court attempted to impose. Faced with repeated non-compliance, the court itself has declared that it "no longer has … confidence" that "the government is doing its utmost to ensure that those responsible for implementation fully comply with the court's orders."[23] The risk of privacy violations is compounded by the near impossibility of challenging the legality of the government's surveillance operations before both the FISC and regular courts.

Secret Law

The FISC has developed a body of undisclosed law that empowers the U.S. government to conduct wide-ranging, invasive surveillance of hundreds of millions of individuals around the world. It has issued a number of significant decisions that define the scope of the U.S. government's authority to conduct surveillance. FISC records are presumed secret unless a "judge who authored an order, opinion, or other opinion may *sua sponte* or on motion by a

---

[19] *See generally* SELECT COMM. TO STUDY GOV'T OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT, S. REP. NO. 94-755, bk. II, at 66, 77, 84-89, 99-102, 170, 211-16 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf.

[20] Foreign Intelligence Surveillance Act of 1978, 50 USC § 1803.

[21] *Foreign Intelligence Surveillance Act Court Orders 1979 – 2012*, ELEC. PRIVACY INFO. CTR. (May 4, 2012), http://epic.org/privacy/wiretap/stats/fisa_stats.html.

[22] *Id.*

[23] In re Production of Tangible Things From [Redacted], No. BR 08-13, at 12 (FISA Ct. Mar. 2, 2009), *available at* https://www.aclu.org/files/assets/pub_March%202%202009%20Order%20from%20FISC.pdf.

party request that it be published." The Presiding Judge of the court has exclusive authority to grant or deny any such request.[24]

Up till the Snowden disclosures in June 2013, the FISC had released only three substantive opinions relating to the obligations of third party providers and the permissible uses of the intelligence collected.[25] Since the disclosures, some fourteen additional opinions and orders have been made public.

However, these revelations provide only a glimpse of the extensive legal framework that allows the government to collect massive amounts of data on the lives of individuals at home and abroad. From its inception, the FISC has heard 33,949 government applications for surveillance and physical searches.[26] It is likely that several of the orders issued in response to these applications are accompanied by substantive legal interpretations relevant to the government's surveillance authorities. The latest disclosures may constitute only a handful of the universe of legally significant decisions that should be made available to the public.

The importance of these opinions cannot be overstated. One of the first documents released by Snowden was an order from the FISC authorizing the collection of *all* American telephone records under a provision of the PATRIOT Act that authorized the collection of business records that were "relevant" to a terrorism or foreign intelligence investigation.[27] Several members of the U.S. Congress who had been involved in passing the PATRIOT Act were stunned to learn that the FISC had interpreted the statute so broadly[28] and this interpretation

---

[24] FOREIGN INTELLIGENCE SURVEILLANCE COURT, RULES OF PROCEDURE FOR THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, Rule 62, at 15 (Nov. 1, 2010), *available at* http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

[25] In re All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002); In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002); In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008).

[26] *See Foreign Intelligence Surveillance Act Court Orders 1979 – 2012*, *supra* note 21. Presiding Judge Reggie B. Walton asserted in a letter to Congress that these statistics do not take into account the Court's requests for additional information and modifications to the proposed terms of surveillance "in a significant percentage of cases." However, the secrecy surrounding FISC proceedings makes it impossible to evaluate the nature and scope of these modifications as well as their effectiveness in minimizing privacy intrusions. Letter from Reggie B. Walton, Presiding Judge, Foreign Intelligence Surveillance Court, to Charles E. Grassley, Senator and Ranking Member, Comm. on the Judiciary 3 (Jul. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/honorable-charles-grassley.pdf.

[27] USA PATRIOT Act of 2001, 50 U.S.C. § 1861 (2013); *see also* Spencer Ackerman, *Obama Publishes Legal Background to Surveillance – but Much Is Still Unclear*, GUARDIAN, August 9, 2013, *available at* http://www.theguardian.com/world/2013/aug/09/obama-legal-background-surveillance-nsa.

[28] *See e.g.* Letter from F. James Sensenbrenner, Jr., Comm. on the Judiciary, U.S. H.R., to Eric H. Holder, Jr., Att'y Gen., U.S. Dep't of Justice (Sept. 6, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf; Press Release, Louise M. Slaughter, U.S. H.R., House Rules Committee Ranking Member Slaughter reacts to reports of NSA collection of telephone records (Jun. 6, 2013), *available at* http://www.slaughter.house.gov/index.php?option=com_content&task=view&id=2953&Itemid=100072; Press Release, Bernie Sanders, U.S. H.R., Sanders Slams Secret Surveillance (Jun. 6, 2013), *available at* http://www.sanders.senate.gov/newsroom/press-releases/sanders-slams-secret-surveillance; Press Release, Rand Paul, U.S. Senate, Sen. Paul Statement on National Security Agency Surveillance (Jun. 6, 2013) *available at*

was rejected by 205 members of the U.S. House of Representatives who voted to overturn it.[29] The FISC's justification for interpreting the statute in this way was only made public on Sept 17, 2013[30] and has garnered extensive criticism from both members of Congress and the legal community.[31]

Limited Ability to Ensure Respect for Privacy Safeguards

The FISC not only approves applications for the surveillance of certain individuals but also bulk intelligence collection programs.[32] Unlike the individually tailored warrants that are traditionally approved by U.S. courts, such programs cover entire programs that sweep up the data and communications of millions of individuals at home and abroad. These programs collect information about people without regard for whether they are suspected of criminal or terrorist activity. As required by statute, the FISC has attempted to establish legal and procedural safeguards to protect individuals from unnecessary invasions of privacy under these

---

http://www.paul.senate.gov/?p=press_release&id=837. For a roundup of Congress's reaction to the NSA's surveillance operations, *see* Janet Hook, *Lawmakers' Mixed Reactions on NSA Surveillance of Phone Records*, WALL ST. J. WASH. WIRE BLOG (June 6, 2013), http://blogs.wsj.com/washwire/2013/06/06/congress-reacts-to-nsa-surveillance-of-phone-records/.

[29] The proposed legislative amendment to end authority for the blanket collection of telephone records under the PATRIOT Act failed by a vote of 205-217. The amendment would have limited the collection of telephone records to persons already subject to a foreign intelligence investigation. H. Amdt. 413 to H.R. 2397, 113th Cong. (2013); *H. Amdt. 413 to H.R. 2397 Overview*, U.S. Cong, http://beta.congress.gov/amendment/113/house-amendment/413 (noting the amendment failed by recorded vote on July 24, 2013); *see also* Jonathan Weisman, *House Defeats Effort to Rein in NSA Data Gathering*, N.Y. TIMES, July 24, 2013, *available at* http://www.nytimes.com/2013/07/25/us/politics/house-defeats-effort-to-rein-in-nsa-data-gathering.html?pagewanted=all&_r=0.

[30] *In Re* Application of The Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [redacted], No. BR 13-109, at 18 (FISA Ct. August 28, 2013), *available at* https://www.aclu.org/files/assets/br13-09-primary-order.pdf ("Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215.").

[31] *See* Jonathan Weisman, *supra* note 29; *see also* Michael McAuliff, *NSA Commits 'Troubling' Surveillance Violations, Senators Say*, HUFFINGTON POST (July 30, 2013, 10:03 PM), http://www.huffingtonpost.com/2013/07/30/nsa-surveillance_n_3679528.html; Elizabeth Goitein, *The Spying on Americans Never Ended*, WALL ST. J., June 6, 2013, *available at* http://www.brennancenter.org/analysis/spying-americans-never-ended; Jameel Jaffer, *Our Surveillance Laws Are Too Permissive*, N.Y. TIMES ROOM FOR DEBATE, June 9, 2013, *available at* http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined.

[32] *See, e.g.*, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc., No. BR 13-80, at 1-2 (FISA Ct. July 19, 2013), *available at* https://www.aclu.org/files/natsec/nsa/20130816/Section%20215%20-%20Secondary%20Order%20-%20Verizon.pdf (secondary order granting the government's application to the collect all telephone metadata created by Verizon for communications to, from and within the United States).

bulk collection programs,[33] but these safeguards still afford the government sweeping authority to use, keep and share the data it collects, and in practice have been difficult to enforce.[34] Given that the FISC approves entire surveillance programs, it is no surprise that it has struggled to oversee the functioning of the NSA's surveillance operations. The court's Presiding Judge Reggie Walton recently admitted that the court is forced to rely on intelligence agencies to report and correct noncompliance with these safeguards.[35] The FISC's reliance on U.S. intelligence agencies to self-regulate creates tremendous potential for abuse and wrongdoing. Indeed, even the limited number of court records and government documents that have been made public thus far reveal a litany of "noncompliance incidents":

---

[33] 50 U.S.C. § 1861(g); 50 U.S.C. § 1881a(e). A March 2009 FISC opinion revealed that the court had approved procedures controlling the accessing, dissemination and retention of records collected under Section 215 of the PATRIOT Act by the NSA and the FBI. Among other things, the NSA and the FBI could only search the records for links to a particular telephone number if they had "reasonable, articulable suspicion" that that number was associated with certain suspicious persons or groups. *In re* Production of Tangible Things From [Redacted], No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), *available at* https://www.aclu.org/files/assets/pub_March%202%202009%20Order%20from%20FISC.pdf. The NSA's handling of records under Section 702 of the FAA is governed by a separate (if overlapping) set of court-approved guidelines. ERIC H. HOLDER, JR., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE 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 (2011) [hereinafter MINIMIZATION PROCEDURES], *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. These guidelines were modified in 2011 in response to the FISC's concerns that the NSA's collection of internet communications was overbroad. [REDACTED NAME], [REDACTED NO.], (FISA Ct. Oct. 3, 2011) (opinion of Judge John D. Bates), *available at* http://www.dni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf (concluding that the NSA's minimization procedures did not sufficiently protect the privacy of the Internet communications of U.S. persons); [REDACTED NAME], [REDACTED NO.], (FISA Ct. Nov. 30, 2011) (opinion and order of Judge John D. Bates), *available at* https://www.aclu.org/files/assets/november_2011_fisc_opinion_and_order.pdf (concluding that the NSA's revised minimization procedures adequately address the deficiencies identified in the FISC's ruling from October 3, 2011).

[34] For example, the minimization procedures prescribed for data collected under Section 702 of the FAA permit the government to retain and disseminate information that is related to "foreign intelligence information." However, "foreign intelligence information" has been defined broadly and includes not only information about terrorism or clandestine intelligence activities, but also information about national defense and the conduct of U.S. foreign affairs. 50 USC § 1801(e). Under such a broad standard, a significant amount of communications can be considered data relating to "foreign intelligence information." *See Oversight Hearing on the Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. 11 – 12 (2013), *available at* http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf; *see also How the NSA's Surveillance Procedures Threaten Americans' Privacy*, AM. CIVIL LIBERTIES UNION (June 21, 2013), https://www.aclu.org/nsa-surveillance-procedures. Furthermore, these procedures fail to regulate certain kinds of data. For example, encrypted data may be retained indefinitely. *See* MINIMIZATION PROCEDURES, *supra* note 33, § 5(3)(a), 6(a)(1)(a). There are also no restrictions on the sharing and dissemination of data belonging to foreign citizens located outside the United States. MINIMIZATION PROCEDURES, *supra* note 33, § 7.

[35] In response to the release of an internal audit showing the NSA had overstepped its legal authority thousands of times since 2008, Presiding Judge Walton wrote in a statement to The Washington Post that "the FISC is forced to rely upon the accuracy of the information that is provided to the Court" and "does not have the capacity to investigate issues of noncompliance." Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST, Aug. 15, 2013, *available at* http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html

- An August 2009 internal audit revealed that one of the NSA's partner agencies had improperly included credit card numbers in its databases in 2006. The problem recurred in 2008.[36]

- In February 2009, the government reported to the FISC that it had, on multiple occasions, inappropriately queried its phone records database in violation of the government-devised and court-mandated oversight regime.[37] In a March 2009 opinion, the court found that the privacy safeguards it adopted had "been so frequently and systematically violated that it can fairly be said that this critical element of the overall [surveillance] regime has never functioned effectively."[38] The court also found that its authorizations of the vast surveillance program in question were based on the government's "material misrepresentations" of its efforts to comply with privacy safeguards.[39]

- In October 2011, the FISC ruled that the government's collection of thousands of e-mails and other Internet communications was unconstitutional. Although the court had previously authorized the collection of *discrete* Internet communications, "the volume and nature of the information [the government] has been collecting is fundamentally different from what the Court had been led to believe."[40] The court was also "troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[41]

- In May 2012, an internal government audit recorded 2,776 violations of FISC-mandated privacy safeguards over a one-year period. These violations arose from the unauthorized

---

[36] Report of the United States at 20-21, 47-48, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 09-09 (FISA Ct. Aug. 17, 2009), *available at* https://www.aclu.org/files/assets/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf.

[37] Notice of Compliance Incidents, *In re* Production of Tangible Things [REDACTED], No. BR 08-13 (FISA Ct. Feb. 26, 2009), *available at* https://www.aclu.org/files/assets/pub_Feb%2026%202009%20Notification%20of%20Compliance%20Incident.pdf.

[38] In re Production of Tangible Things From [REDACTED], No. BR 08-13, at 11 (FISA Ct. Mar. 2, 2009), *available at* https://www.aclu.org/files/assets/pub_March%202%202009%20Order%20from%20FISC.pdf. The court found that the NSA had flagrantly violated the minimization rules and had instead instituted a daily check of phone records against 17,800 names on an "alert list" that it maintained; only some 10% of the numbers on the alert list met the "reasonable, articulable suspicion" standard required to access the data. *Id.*, at 4 n. 2.

[39] *Id*. at 7, 10-11.

[40] [REDACTED NAME], [REDACTED NO.], slip op. at 28 (FISA Ct. Oct. 3, 2011) (opinion of Judge John D. Bates), *available at* http://www.dni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf.

[41] *Id*. at 16 n.14.

> collection, retention and distribution of information concerning Americans and foreign targets in the United States.[42]

What little oversight the FISC maintains over the U.S. government's surveillance programs does not extend to the government's conduct concerning foreign citizens located outside the United States. The FAA provides the U.S. government with expansive authority to "targe[t] … [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[43] However, it fails to regulate the collection and subsequent retention and distribution of information about such foreigners: Under FISA, procedures to minimize the retention and sharing of information collected only protect *United States* persons.[44] As a result, U.S. surveillance programs contain no checks aimed at protecting the privacy of the millions of people who are not American citizens or living in the United States.

No Remedy for Privacy Violations

Because FISC proceedings are secret, affected persons have no opportunity to challenge the court's orders. Only the government and communications providers ordered to turn over information may appear before the court; surveillance targets have no role in FISC proceedings. And since the court has found that there is no public right of access to its records,[45] affected persons often do not know that they have been targeted by court-approved surveillance operations and therefore cannot challenge such operations.

Regular courts also do not provide an avenue for challenging the legality of the government's surveillance operations. In February 2013, the U.S. Supreme Court in *Clapper vs. Amnesty International* held that a group of lawyers, journalists and human rights activists lacked standing to challenge the government's alleged surveillance of their communications.[46] Plaintiffs had argued that given the nature of their work, it was likely that their communications were intercepted by the government. The Court rejected this argument, reasoning that since the plaintiffs had "no actual knowledge of the government's [surveillance] practices," allegations that their communications had been monitored were too speculative to allow them to sue.[47] Plaintiffs had argued that requiring this type of actual knowledge of presumably secret

---

[42] Memorandum from Chief, SID Oversight and Compliance, to Director, SIGINT, NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2013) – EXECUTIVE SUMMARY, at 2 (May 3, 2012), *available at* http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/.

[43] 50 U.S.C. 1881a(a).

[44] 50 U.S.C. § 1821(4). A U.S. person is defined as "a citizen of the United States, an alien lawfully admitted for permanent residence … an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States ..." 50 U.S.C. § 1801(h).

[45] In re Motion for Release of Court Records, 526 F. Supp. 2d 484, 492 (FISA Ct. 2007) (holding that the common law provides no right of access to FISC records).

[46] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

[47] *Id.* at 1141.

surveillance rendered the program being challenged immune from judicial review.[48] The government countered that review is possible if a criminal case is brought based on information obtained from FAA surveillance operations, prosecutors are obliged to reveal this fact to the defendant allowing him to challenge the underlying surveillance.[49] In practice, however, prosecutors have refused to disclose to defendants whether they are relying on evidence arising from such operations, effectively depriving them of their right to challenge.[50]

In sum, the FISC's secretive role in endorsing whole surveillance programs as well as its failures of oversight hamper its ability to protect individuals from violations of their privacy, speech and association rights. The daunting procedural hurdles that U.S. litigants must overcome in order to challenge the legality of the government's surveillance programs also exclude such programs from meaningful judicial review.

IV. Recommendations

The state party should:

- Explain to the Committee steps it is taking or will take to ensure that the operation of FISC and the adjudication of government surveillance requests conform with Articles 17, 18 and 19 of the ICCPR, with a view of fully implementing such steps by the next Universal Periodic Review in April 2015;

- Develop and release redacted versions or summaries of FISC opinions and other government documents containing significant legal interpretations of the scope of the government's surveillance authorities or findings of governmental non-compliance;

- Establish an independent ombudsman, special advocate, or other such office that will be charged with protecting the rights and interests of those persons whose information the government will or may be collecting, and that will appear in FISC proceedings involving significant legal questions; and

- Reform current procedural laws (including but not limited to laws that regulate access to the FISC, FISC rules of procedure and the laws on standing) to preserve the right of U.S. persons to obtain effective judicial remedies for privacy violations arising from U.S. surveillance operations.

---

[48] Press Release, Am. Civil Liberties Union, Ruling Shields Surveillance Program from Judicial Review (Feb. 26, 2013), *available at* https://www.aclu.org/national-security/supreme-court-dismisses-aclus-challenge-nsa-warrantless-wiretapping-law.

[49] Brief for Petitioner at 15, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025), *available at* http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/briefs/11-1025_pet_reply.authcheckdam.pdf.

[50] Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 15, 2013, *available at* http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?pagewanted=all&_r=0.