KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Statement of the Center for Democracy & Technology On Human Rights and Communications Surveillance By the United States and Other OAS Member States

October 25, 2013

The Center for Democracy and Technology ("CDT") submits this testimony in advance of the thematic hearing on the human rights implications of communications surveillance by the United States and other OAS Member States as requested by the American Civil Liberties Union in a letter dated August 16, 2013.

ABOUT CDT

CDT is a U.S. based civil society organization, defending global online civil liberties and human rights. We are dedicated to keeping the Internet open, innovative, and free, and we are committed to finding forward looking and technically sound solutions to the medium's most pressing challenges. For over 20 years, since the Internet's infancy, CDT has played a leading role in shaping the policies, practices and norms that have empowered individuals to more effectively use the Internet as speakers, entrepreneurs, and active citizens. CDT brings legal and technical expertise, thought leadership, and coalition-building skills to its work with domestic and global policy institutions, regulators, standards bodies, governance organizations, and courts.

Since CDT's founding, one of our central priorities has been to promote robust checks and balances limiting government surveillance, consistent with the U.S. Constitution, the ICCPR and other global human rights instruments including American Convention on Human Rights. We helped lead opposition to the PATRIOT Act and the FISA Amendments Act ("FAA") and are currently advocating for major reform of FISA, including providing additional protections for the rights of non-Americans.

I. An Overview of the New Surveillance Paradigm

Recent revelations about the scope and scale of surveillance programs in the U.S. have highlighted what national security officials candidly admit: that we have entered a "golden age" of surveillance.[1] There are at least three factors driving a paradigm shift away from particularized or targeted monitoring to systemic or bulk collection, in which government agencies seek larger and larger volumes of data, claiming that bulk access is necessary to find "the needle in the haystack."

First, the storage revolution and big data analytic capabilities, combined with fears about terrorism, are driving a steadily growing governmental appetite for access to data held by the private sector. Governments are demanding more data on the theory that big data analytic capabilities will allow them to extract small but crucial pieces of information from huge datasets.

Second, as Internet-based services have become globalized, trans-border surveillance has flourished, posing new challenges for human rights. As Frank La Rue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression, noted, there is "serious concern with regard to the extraterritorial commission of human rights violations and the inability of individuals to know they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance or seek remedies."[2]

Gone are the days when intelligence agencies had to establish foreign listening posts or position satellites or antennas to capture communications that stayed largely within the country of origin. Now, in many instances, communications pass through or are stored in other countries. In that respect, the United States holds a unique position in terms of access to global communications data since a great deal of global communications travel over U.S. networks or are stored with U.S. cloud companies.

Third, national security legal authorities have become increasingly powerful since 9/11 in the U.S. It has long been the case that governments have claimed greater powers to collect data in the name of national security than in ordinary criminal law enforcement cases. In the post 9/11

---

[1] *See* Dana Priest, The Washington Post, *NSA growth fueled by need to target terrorists* (July 21, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html (NSA head told his staff that, by exploiting digital technologies, they could realize "the golden age" of electronic surveillance). CDT Fellow Peter Swire predicted this two years ago. Peter Swire and Kenesa Ahmad, CDT Blog, *Going Dark or a Golden Age of Surveillance* (November 28, 2011), *available at* https://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance ("[W]hile government agencies claim to be worried about 'going dark' in the face of technological change, today should be understood as a 'golden age of surveillance'").

[2] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue, to the Human Rights Council, at 64 (April 17, 2013), available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

worlds, activities conducted in the U.S. under these separate rules for national security have vastly expanded even as privacy safeguards have eroded.[3]

This paradigm shift has been supported in the U.S. by extreme secrecy. The powerful authorities in the PATRIOT Act and the FISA Amendments Act of 2008 ("FAA") have been stretched beyond imagination by secret interpretations of law that are just now coming to light. Oversight has been dangerously weakened ,depriving the American people—until now—of critical democratic debate. The result is a surveillance regime that violates the protections under the Fourth Amendment to the U.S. Constitution as well as U.S. obligations under international human rights agreements. To the extent that the programs intentionally or inadvertently collect the data of persons outside the U.S., the privacy and free expression rights of those persons have been abrogated as well.

II. The Protections and Gaps in U.S. Law

A. The Constitution and Statutes

U.S. law is complicated with respect to privacy. Communications privacy as between the individual and the government is a fundamental right in the U.S., protected by the Fourth Amendment to the U.S. Constitution. For decades, the courts and Congress have struggled to apply that provision, which was written in 1789, to newer technologies, and the results have been uneven. However, the U.S. Constitution definitely treats privacy of the home and the confidentiality of communications as fundamental rights vis-à-vis interference by the government.[4] Under the Fourth Amendment, which prohibits unreasonable searches and seizures, the government, in order to carry out electronic surveillance targeted at persons inside the U.S., generally requires a warrant issued by an independent judge, based on a finding of factual justification and necessity, and, while the U.S. doesn't use the same term, the surveillance must be proportional.

Moreover, the Fourth Amendment, like many human rights provisions in the U.S. Constitution, applies equally to citizens and non-citizens who are *physically inside* the U.S. In addition, the federal statutes that define precise procedures for electronic surveillance require a court order, naming a specific person or account, to intercept the communications of both citizens and non-citizens inside the U.S., in both law enforcement and national security matters.

---

[3] There have been reports of close cooperation in surveillance programs and intelligence sharing between the U.S. and a number of other countries, at least some of which also engage in mass surveillance activities: (Ewen MacAskill et al, The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications (June 21, 2013), available at http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; Spiegel Online, The German Prism: Berlin Wants to Spy Too (June 17, 2013), available at http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html; Angelique Chrisafis, The Guardian, France 'runs vast electronic spying operation using NSA-style methods'(July 4, 2013), available at http://www.guardian.co.uk/world/2013/jul/04/france-electronic-spying-operation-nsa.)

[4] Our constitutional safeguards do not apply directly to private actors who process personal data. A variety of sectoral laws on health, children, education, finance and the like fill part of the gap as do state laws. In addition the Federal Trade Commission has used its powers to enforce against "unfair and deceptive" trade practices to establish some horizontal rules for consumer data. CDT has advocated for enactment of a comprehensive baseline consumer privacy law to simplify and strengthen this regime.

The problem from an international perspective is that the Fourth Amendment right to communications privacy *does not* apply to searches of non-citizens conducted by the U.S. government *outside* the U.S. Even U.S. citizens, however, do not enjoy the full protection of the Constitution when the U.S government is conducting searches outside the United States.[5] Further, the Constitution has been interpreted to not require a judicial warrant for surveillance conducted inside the U.S. but targeted at certain non-citizens ("agents of foreign powers") who are physically outside the U.S.[6] This position is consistent with the U.S. interpretation of its obligations under the ICCPR that limits such obligations to individuals who are within both its territory and jurisdiction.

B. The "third party records" doctrine

A further aspect of US constitutional law which has supported mass surveillance can be found in a Supreme Court decision from many years ago which held that the Constitution does not provide *any* privacy protection to so-called "third party" or business records, which includes traffic data or metadata associated with communications. [7] Importantly, U.S. citizens and others lawfully in the country enjoy no greater protection for their communications metadata than non-Americans outside of the country. CDT believes this line of cases is woefully outdated and that it should be – and some day will be – reversed, but for now, the Constitution as interpreted by the courts does not require any court order for the U.S. government (in law enforcement or national security investigations) to acquire call detail records and Internet metadata for citizens or non-citizens alike.

In response to this Constitutional doctrine, Congress has created statutes that specify multiple different standards (some requiring court orders, some not) for the government to acquire transactional data inside the U.S. Those standards differ substantially between law enforcement and national security investigations, but under most of those laws, the standard under each pillar (law enforcement and national security) is the same for U.S. citizens and non-U.S. citizens inside the U.S.

There is broad agreement among privacy advocates and legal scholars in the U.S. that the third party records doctrine needs to be substantially limited, especially as applied to communications data.[8] Until recently, however, the courts have applied a very broad interpretation of the doctrine

---

[5] The warrant clause of the Fourth Amendment does not apply to surveillance conducted outside the U.S. even targeting U.S. citizens. Instead, such surveillance is judged only under the reasonableness standard of the Fourth Amendment. By statute, Congress has required the intelligence agencies to obtain a warrant when targeting U.S. citizens abroad, but law enforcement agencies do not need a warrant when conducting electronic surveillance outside the U.S. for criminal investigative purposes, even when targeting U.S. citizens.

[6] One appellate court has held that the warrant requirement of the Fourth Amendment does not apply to foreign intelligence surveillance conducted inside the U.S. aimed at foreign powers or agents of foreign powers reasonably believed to be outside the U.S. S*ee*, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). Nevertheless, the Court did scrutinize that surveillance under the clause of the Fourth Amendment that requires searches to be reasonable, holding that there were sufficient limits on the surveillance to make it Constitutional.

[7] *Smith v. Maryland*, 442 U.S. 735 (1979).

[8] Greg Nojeim, *Why the Third Party Records Doctrine Should Be Revisited*, *available at* http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch4/ch4_ess10.html.

and that broad interpretation has guided Congress in drafting the statutes governing electronic surveillance and it has also been key to the executive branch's view of its surveillance powers. However, in January 2012, in *United States v. Jones*, where the U.S. Supreme Court held that the collection of GPS data over time did require a warrant, five Justices of the Court approached the case in a way that provided the first suggestion that the third party records doctrine was vulnerable.[9] Unfortunately, the executive branch continues to argue that even prolonged collection of telephony metadata involves no "search" under the Constitution and other courts have not yet taken up the suggestions in the *Jones* opinions.

C. The NSA's telephony metadata program (Section 215 of the Patriot Act)

When it comes to the collection of metadata, U.S. law treats citizens and non-citizens equally poorly. That point is demonstrated by the telephony metadata order that Mr. Snowden leaked. That order, and subsequent admissions by the government, show that the National Security Agency ("NSA") has been routinely collecting metadata associated with a large percentage of telephone calls to, from, and within the U.S.[10] The metadata being collected includes the phone number placing the call, the number receiving the call, SIM card numbers and other numerical identifiers associated with phone devices, and the time and duration of each call.[11] Most of the data collected under the program relates to U.S. citizens and other persons inside the U.S., but it also collects information about persons outside the U.S. in connection with calls to and from the U.S. As approved by the courts, this comprehensive metadata collection program has been ongoing continuously for the last seven years.[12] However until the initial publication by *The Guardian* on June 5, it was unknown to the public.

The metadata program has been approved by the Foreign Intelligence Surveillance Court ("FISC") (which we describe further below) under Section 215 of the PATRIOT Act, which permits the government to acquire "any tangible thing" relevant to an investigation to prevent terrorism.[13] Before the PATRIOT Act, a predecessor "business records" law[14] allowed the government to obtain a court order to require private sector entities to disclose information that pertained to a suspected terrorist, spy or other agent of a foreign power. Under that earlier law, the records sought had to pertain to a specified person or entity; bulk data collection was not authorized. Section 215 of the PATRIOT Act substantially rewrote the business records statute

---

[9] *See generally*, *United States v. Jones*, 132 S. Ct. 945, 946, 181 L. Ed. 2d 911 (2012); *see also*, *United States v. Jones*, 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012) (J. Sotomayor, concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks") (internal citations omitted).

[10] Glenn Greenwald, The Guardian, *NSA collecting phone records of millions of Verizon customers daily* (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also*, Center for Democracy & Technology, *NSA Spying Under Section 215 of the PATRIOT Act: Illegal, Overbroad, and Unnecessary* (June 19, 2013), *available at https://www.cdt.org/files/pdfs/Analysis-Section-215-Patriot-Act.pdf*, *hereafter*, *CDT § 215 Analysis*.

[11] *Id*.

[12] Parmy Olsen, Forbes, *U.S. Senators: NSA Cellphone Spying Has Gone On 'For Years'* (June 6, 2013), *available at* http://www.forbes.com/sites/parmyolson/2013/06/06/u-s-senators-nsa-cellphone-spying-has-gone-on-for-years/.

[13] 50 U.S.C. § 1861.

[14] In 1998, Congress adopted Section 602 of the Intelligence Authorization Act of 1999 (P.L. 106-120). It created a very limited authority to obtain business records under the Foreign Intelligence Surveillance Act.

to allow the government to demand any "tangible thing" that was "relevant" to an ongoing investigation. Secret orders from the FISC have interpreted the term "relevant" very broadly and have required leading telephone service providers to turn over all call detail records for all of their customers on an on-going basis.[15] The court orders, and the underlying legal rationale, draw no distinction between U.S. citizens and non-U.S. citizens, and the vast majority of people whose records are disclosed to the NSA under the telephony metadata program are undoubtedly U.S. citizens in the U.S. People outside of the U.S. communicating with people inside the U.S. are likely caught up in the telephony metadata dragnet as well.[16] The telecommunications companies receiving these orders are prohibited by law from revealing orders or notifying customers.[17] Telecommunication companies are required to provide data "on an ongoing daily basis" for a three month period.[18] Although the Office of the Director of National Intelligence ("ODNI") stresses the fact that communications content is not collected under this program,[19] metadata "can be incredibly revealing—sometimes more so than the actual content."[20] This is especially true when these data are collected in bulk and subject to powerful analytics. "Phone records can actually be *more* revealing than content when someone has as many records and as complete a set of them as the NSA does."[21] When collected in bulk, metadata can reveal information such as political affiliation and activities, intimate relationships, conduct at ones' job, and medical treatment and family planning.[22]

---

[15] *See*, Foreign Intelligence Surveillance Court Amended Memorandum Opinion (J. Eagan) of August 29, 2013, *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf; *see also*, Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act Reauthorization (August 9, 2013), *available at* https://www.eff.org/sites/default/files/filenode/section215.pdf. One of the primary Congressional authors of the PATRIOT Act has vigorously disputed the Executive's broad interpretation of the relevance requirement.

[16] Recent disclosures have also shown that the NSA conducted for many years a program that collected metadata regarding Internet transactions to, from, and within the U.S. That program was discontinued in 2011 due to an assessment by NSA that it was ineffective as a counterterrorism tool.

[17] 50 U.S.C. § 1861(d)(1) ("No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section, other than to—(A) those persons to whom disclosure is necessary to comply with such order; (B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or (C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director").

[18] CDT § 215 Analysis; *see also*, Glenn Greenwald, The Guardian, *NSA collecting phone records of millions of Verizon customers daily* (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[19] *See*, Office of the Director of National Intelligence, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information, hereafter, DNI Disclosure June Response.

[20] Joe Mullin, Ars Technica, *In ACLU lawsuit, scientist demolishes NSA's "It's just metadata" excuse* (August 27, 2013), *available at* http://arstechnica.com/tech-policy/2013/08/in-aclu-lawsuit-scientist-demolishes-nsa-its-just-metadata-excuse/.

[21] Matt Blaze, Wired, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)* (June 19, 2013),*available at* http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/.

[22] Aubra Anthony, The Center for Democracy and Technology, *When Metadata Becomes Megadata: What the Government Can Learn* (June 17, 2013), *available at* https://www.cdt.org/blogs/1706when-metadata-becomes-megadata-what-government-can-learn-metadata; Joe Mullin, Ars Technica, *In ACLU lawsuit, scientist demolishes NSA's "It's just metadata" excuse* (August 27, 2013), *available at* http://arstechnica.com/tech-policy/2013/08/in-aclu-lawsuit-scientist-demolishes-nsa-its-just-metadata-excuse/.

According to recent official disclosures, the data obtained through the telephony metadata program may be queried by the NSA "when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization."[23] This standard is not set out in any publicly enacted law. Rather, the standard was developed in secret by the executive branch and approved in secret by the FISC. Judges do not approve the queries; instead, NSA analysts make the determination as to whether the standard has been met for any particular query.[24]

Furthermore, analysts may query the metadata three "hops" from a suspected individual.[25] Each hop consists of a level of contact; the first hop provides information about all numbers in contact with a specific suspect, the second hop provides data on the phone activity of all those individuals, and the third hop then takes this even wider pool and identifies the calls made or received by all numbers in the second hop.[26] By engaging in "three hop" analysis, the NSA can scrutinize data relating to as many as a million persons in a single query.

Recently, opinions of the FISC related to the Section 215 metadata program have been released and they reveal troubling misrepresentations to the Court by the government and systemic violations of the FISC's rules on access to the telephony metadata. In an October 2011 opinion, the FISA Court stated, "[M]isperception [regarding the bulk collection program] by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime."[27] According to the FISC:

> Contrary to the government's repeated assurances, NSA has been routinely running queries of the metadata using querying terms that did not meet the standard required for querying. The Court concluded that this requirement had been so frequently and systematically violated that it can be fairly said that this critical element of the overall ... regime has never functioned effectively.[28]

Several lawsuits have been filed challenging the telephony metadata bulk collection program, alleging violations of various statutes and the United States Constitution.[29] Additionally,

---

[23] DNI Disclosure June Response.

[24] *See*, *id*.

[25] Sari Horwitz and William Branigin, The Washington Post, *Lawmakers of both parties voice doubts about NSA surveillance programs* (July 17, 2013), *available at* http://articles.washingtonpost.com/2013-07-17/world/40624274_1_phone-records-nsa-surveillance-programs-collection.

[26] Id.

[27] Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) of October 3, 2011, fn 14, available at https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf, hereafter, FISC October 2011 Opinion.

[28] Id. (internal citation omitted).

[29] *See,* First Unitarian Church of Los Angeles v. NSA, 2013 WL 3678094 (N.D.Cal.)

advocacy groups have filed suits seeking disclosure of additional information regarding the nature of the program and the FISC's evaluation of it.[30]

CDT believes that the telephony metadata program of the NSA violates American's Fourth Amendment rights under the U.S. Constitution as well as the privacy and free expression rights of Americans and non-citizens outside the country. We believe that the third party records doctrine, which was very narrow when first endorsed by the Supreme Court in the 1970s, should not be stretched to encompass the collection of call detail records of all customers of a service provider on an ongoing, indefinite basis. We also believe that the statute being relied on by the government and the FISC to authorize the telephony metadata program (Section 215 of the PATRIOT Act) is being misinterpreted, contrary to its plain language and the intent of Congress when it adopted the language. We believe that the government's secret interpretation of the law, even if endorsed by a secret court, was undemocratic, and we are urging Congress to amend the law to prohibit the program.

D. PRISM and other communications content collection programs targeted at non-citizens outside the United States

The other major surveillance activity revealed by Snowden is the PRISM program and other related programs authorized under Section 702 of the Foreign Intelligence Surveillance Act as amended in 2008. These programs collect the content of communications of persons reasonably believed to be outside the U.S., when those communications are available inside the U.S.

In order to understand the context for the Section 702 program, it is useful to understand the history of the Foreign Intelligence Surveillance Act ("FISA"). FISA was enacted in 1978 after disclosure of politically motivated FBI wiretapping of civil rights activists and political dissidents in the U.S. This law subjects intelligence surveillance in the U.S. to judicial control by the Foreign Intelligence Surveillance Court ("FISC"), which is comprised of regular federal judges designated by the Chief Justice of the Supreme Court for additional duty on this special court. The key provisions of FISA require the government, before conducting electronic surveillance for intelligence purposes inside the U.S., to obtain an order from the FISC based on a finding of probable cause to believe that the target of the surveillance is a terrorist, spy, or other agent of a foreign power. In addition, the government has to certify that a significant purpose of the surveillance is to collect broadly defined "foreign intelligence information."[31]

---

[30] American Civil Liberties Union v. Federal Bureau of Investigation, 2011 WL 9282938 (S.D.N.Y.); see also, Motion of the American Civil Liberties Union, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic for the Release of Court Records (June 10, 2013), available at http://www.uscourts.gov/uscourts/courts/fisc/aclu-misc-13-02.pdf.

[31] FISA defines "foreign intelligence information" broadly as: "[I]nformation that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e).

Those requirements effectively bar intelligence surveillance in the U.S. for purely political reasons. As noted above, FISA generally requires a court order whether the target is a U.S. citizen or not, if the target is inside the U.S. (The standard varies somewhat for citizens and permanent resident aliens and non-citizens, but a court order is required for both.) With one small exception, FISA has never applied to surveillance conducted outside the U.S.

In 2008, Congress enacted the FISA Amendments Act ("FAA") to empower the government to compel telephone companies, Internet Service Providers and on-line service providers to assist with surveillance conducted *inside the U.S.* of *persons reasonably believed to be abroad.* For this surveillance, there is no requirement that the FISC find that the target of surveillance is an agent of a foreign power. Instead Section 702 of the FAA[32] permits the NSA – with some limitations – to designate the targets for surveillance. Rather than review and approve individual targets, the FISC approves "Targeting Guidelines," which set out the process for designating of targets, and "Minimization Guidelines," which are intended to limit the retention and use of Americans' communications. Thus, Section 702 stands in stark contrast to traditional FISA, under which the government is required to obtain a particularized warrant from a court before engaging in electronic communications monitoring.

Collection of electronic communications to, from, and about targets occurs through both upstream and downstream collection techniques. Through upstream collection, NSA engages in collection of communications on the Internet backbone, meaning "on fiber cables and infrastructure as data flows past."[33] We currently do not know the precise means by which NSA is able to engage in this collection. It may be that the NSA is tapped into the fiber cables that connect North America to the rest of the globe, and carry the majority of the world's Internet traffic,[34] or alternatively, that it requires telecommunications providers to provide a separate stream. In any event, it is clear that the agency is systematically albeit temporarily copying the contents of international e-mails and other text-based communications, using so-called "selectors" to look for communications "to" "from" or "about" a target.[35] We believe that communications not "selected" are not retained.

PRISM governs downstream collection of information on targets. It appears that secret "tasking orders" are sent to electronic communication providers, requiring access to "a wide range of digital information, including e-mails and stored data."[36] The level of access that NSA has to

---

[32] 50 U.S.C. 1881a.

[33] The Washington Post, *NSA slides explain the PRISM data-collection program* (June 6, 2013), *available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[34] *See, id*

[35] *See*, *Exhibit A: 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, as Amended* (July 28, 2009), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf; *see also*, Charlie Savage, The New York Times, N.S.A. Said to Search Content of Messages to and From U.S. (August 8, 2013), *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

[36] The Washington Post, *NSA slides explain the PRISM data-collection program* (June 6, 2013), *available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

user data from the companies issued orders is unclear.[37] However, providers have stated that the orders are limited to specific targets. The law, however, restricts their ability to discuss their role in this process, including prohibitions on discussing the receipt of orders, efforts to protect user data, the manner in which they provide information to the NSA, and the specific number of requests or accounts affected by orders.[38]

In our view, the NSA's Targeting Guidelines and collection procedures fall far short in their promise to protect the rights of Americans' communication. They offer no protection to the communications of people outside the U.S.

The principal requirement for targeting under the FAA is a determination of foreignness of potential surveillance targets.[39] Leaked documents suggest that the NSA deems that a mere 51 percent confidence in a target's foreignness is sufficient to engage in surveillance of that individual.[40] On the basis of these broad standards, the NSA has compiled a list of 117,675 active targets.[41] The Targeting Guidelines permit the monitoring of communications not only of targets themselves, but also all communications that are "about" a target.[42]

Under the NSA's Minimization Guidelines, there are numerous exceptions that permit retention, querying, and sharing of communications of Americans and other U.S. persons.[43] For example, the Minimization Guidelines permit the retention and sharing of any wholly domestic communications that are believed to contain foreign intelligence information, evidence of any domestic criminal activity, or technical data such as knowledge of security vulnerabilities.[44] The Minimization Guidelines not only allow retention of all communication that may contain evidence of a crime, but also permit the NSA to share these communications with domestic law

---

[37] Craig Timberg, The Washington Post, *The NSA slide you haven't seen* (July 10, 2013), *available at* http://articles.washingtonpost.com/2013-07-10/business/40480665_1_nsa-slide-prism ("[NSA's] description of PRISM as "collection directly from the servers" of technology giants such as Google, Microsoft and Facebook has been disputed by many of the companies involved (They say access to user data is legal and limited)").

[38] *See*, Claire Cain Miller, The New York Times, *Tech Companies Escalate Pressure on Government to Publish National Security Request Data* (September 9, 2013), *available at* http://bits.blogs.nytimes.com/2013/09/09/tech-companies-escalate-pressure-on-government-to-publish-national-security-request-data/.

[39] See, 50 U.S.C. 1881a(b).

[40] See, Barton Gellman and Laura Poitras, The Washington Post, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program* (June 6, 2013), *available at* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in- broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html.

[41] The Washington Post, *NSA slides explain the PRISM data-collection program* (June 6, 2013), *available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[42] See, *Exhibit A: 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, as Amended* (July 28, 2009), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf; see also, Charlie Savage, The New York Times, *N.S.A. Said to Search Content of Messages to and From U.S.* (August 8, 2013), *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=0.

[43] See, Office of the Director of National Intelligence, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702, as amended (August 21, 2013), *available at* http://www.dni.gov/files/documents/Minimization Procedures used by NSA in Connection with FISA SECT 702.pdf.

[44] *Id.*

enforcement and intelligence agencies.[45] The NSA may also retain all encrypted communications indefinitely.[46]

The Minimization Guidelines provide no limits on the retention or sharing of the communications of non-U.S. persons. Once such communications are collected, they may be shared and used within the government for any lawful purpose. There is no way to know how many people worldwide have had their communications collected under these programs, shared within the government, nor can it be ascertained how such data has been used.

The Snowden leaks have revealed that the NSA has "broken privacy rules or overstepped its legal authority thousands of times each year" since the passage of the FAA.[47] The scale of these errors, documented in an internal audit, was not disclosed to the public or the U.S. Congress – including the Chairman of the Senate Intelligence Committee – until they were reported in *The Washington Post* this year.[48]

III. Suggested Questions

Given the details that have been revealed about U.S. surveillance programs and the questions that are still unanswered about these activities, potential risks to privacy and freedom of expression are significant and alarming. CDT recommends inquiry on the following topics:

- Does the U.S. government recognize that foreign nationals located outside the United States have rights with respect to surveillance conducted by the U.S. government inside the United States that requires U.S. companies to turn over data on servers located inside the United States?

- Section 702 permits the U.S. government to compel companies participating in the PRISM program to conduct surveillance of targets reasonably believed to be abroad to obtain foreign intelligence information that has nothing to do with terrorism, espionage or attacks by a hostile power, but that merely relates to the conduct of the foreign affairs of the United States. To what extent is this authority being used? To the extent it is used, to what extent does this surveillance collect communications of persons engaged in activities, which, if conducted in the United States, would be protected by either (i) the First Amendment to the U.S. Constitution.

- Describe the restrictions on collection, dissemination and use of information collected about non-U.S. persons outside the United States under Section 702 of FISA.

---

[45] *See, Id.*

[46] *See*, *Id*; *see also*, Andy Greenberg, Forbes*, Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It* (June 20, 2013), *available at* http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/.

[47] Barton Gellman, The Washington Post, *NSA broke privacy rules thousands of times per year, audit finds* (August 15, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules- thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

[48] Id.

- How do these restrictions differ from the restrictions that may apply to such information collected about U.S. persons?

- Will the U.S. government provide a country-by-country accounting of the number of targets of surveillance under Section 702 of FISA, based on the targets' known or believed location or nationality?

- By what process does the United States remove a person from the list of Section 702 targets and what transparency and accountability measures govern those decisions?

- What steps does the U.S. government take to ensure that the FISA Court receives all the information necessary to make decisions and is not misled by the National Security Agency or other intelligence officials? What additional steps are needed?

IV. Suggested Recommendations

The following reforms would help to ensure that the United States protects the human rights of U.S. citizens and people around the world:

- Make the FISC's significant legal interpretations publicly available with any necessary deletions to protect national security.
  ▪

- Disclose annually the number of surveillance requests the U.S. government makes under each surveillance authority in FISA, and likewise the number of people whose information was disclosed using that authority.

- Narrow the purposes for which surveillance can be conducted under the PRISM program to protect the privacy and free speech rights of people outside the U.S.

- Limit the collection of information under Section 702 and Section 215 to that which pertains directly to a particular intelligence target.

- Provide additional protection for privacy and free speech by empowering advocates of these rights to participate in the FISA Court proceedings at which significant intelligence surveillance legal questions are resolved.

- The U.S. Congress should bar the NSA from circumventing U.S. law by obtaining from other intelligence agencies information U.S. law bars it from collecting itself.

- Refrain from circumventing U.S. criminal law protections by using FISA authorities to conduct surveillance that is primarily for criminal prosecution purposes.

- Refrain from using information collected under Section 702 or Section 215 to prosecute a person for crimes other than terrorism, espionage and other national security crime.

For further information, please contact CDT Policy Analyst Emily Barabas, ebarabas@cdt.org.