KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

TESTIMONY OF LESLIE HARRIS
President & CEO, CDT

Before the European Parliament LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens

September 24, 2013

Members of the LIBE Committee,

On behalf of the Center for Democracy & Technology ("CDT"), I am honored to participate in the LIBE Committee inquiry on electronic mass surveillance on EU citizens.

CDT is a 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. We helped lead opposition to the PATRIOT Act and the FISA Amendments Act ("FAA"). With our partners, we have successfully opposed data retention mandates and recent proposals to expand the government's power in the name of cybersecurity. We have organized a major coalition of civil society groups, trade associations, and leading technology companies that is urging the U.S. Congress to strengthen the privacy protections in a key federal law on government surveillance, the Electronic Communications Privacy Act ("ECPA").

Over the last decade, CDT has expanded its global engagement, supporting Internet freedom advocates in developing countries, participating in global standards and governance bodies, and most recently establishing a full time presence here in Brussels.

The European Union and its Member States have a critical role to play in presenting a model for the Internet grounded in human rights, the rule of law, and multi-stakeholder governance. In the face of aggressive efforts by China, Russia, and others to promote a government controlled counter-model to the open Internet, the policies adopted in the EU matter not only to EU citizens but also to the future of the global Internet. This will be especially true of measures that the EU may take separately or in agreement with the U.S. in response to the revelations of pervasive surveillance by the U.S. and by some

Member States, I am hopeful that a path forward can be found in this crisis that will protect the human rights of both EU and U.S. citizens and preserve the Internet's essential openness.

I. National Security Surveillance in the Era of Global Data Flows and Big Data Analytics

Recent revelations about the scope and scale of surveillance programs in the U.S. and in some EU Member State 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 has 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. and in Europe. 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 world, activities conducted in the U.S. (and possibly in

---

[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.

other countries) 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"), which CDT vigorously opposed, have been stretched beyond imagination by secret law. Oversight has been dangerously weakened, depriving the American people—until now—of critical democratic debate. The result is a surveillance regime that CDT believes violates the protections under the Fourth Amendment to the U.S. Constitution as well as U.S. obligations under the International Covenant on Civil and Political Rights. To the extent that the programs intentionally or inadvertently collect the data of persons outside the U.S., they plainly violate the privacy and free expression rights of those persons as well.

While U.S. surveillance capabilities far outstrip those of other nations, the Snowden disclosures and other recent reports have revealed that systemic surveillance is also employed by some EU Member States as well as in other countries.

- Britain's spy agency, GCHQ, monitors cables that carry the world's phone calls and Internet traffic. Indeed, according to leaked documents, Britain's GCHQ produces larger amounts of metadata than the NSA.[4]
- Germany's foreign intelligence agency, the BND, is monitoring communications at a Frankfurt communications hub that handles international traffic to, from, and through Germany, and the BND is seeking to significantly extend its capabilities.[5]
- Le Monde reports that France runs a vast electronic spying operation using NSA-style methods, but with even fewer legal controls.[6]
- Russia's notorious SORM system is reportedly even more intrusive than the American system. Notably, SORM allows Russia officials to bypass any corporate controls on access.[7]
- India, the world's largest democracy, is building its own version of PRISM to monitor internal communications in the name of national security.[8]

---

[3] There have been reports of close cooperation in surveillance programs and intelligence sharing between the U.S. and some Member States as well as between the U.S. and other countries outside the EU.

[4] 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.

[5] 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.

[6] Jacques Follorou and Franck Johannès, Le Monde, *Révélations sur le Big Brother français* (July 4, 2013), *available at* http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.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.

[7] Kristen Blyth, The Moscow News, *PRISM and SORM: Big Brother is watching* (June 17, 2013), *available at* http://themoscownews.com/russia/20130617/191621273.html; Andrei Soldatov, Privacy International, *Lawful interception: the Russian approach,* (March 5, 2013) https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach.

[8] Anjani Trivedi, Time, *In India, Prism-like Surveillance Slips Under the Radar* (June 30, 2013), available at http://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

International and regional human rights treaties recognize the right to privacy, but expressly state that the right is not absolute. The European Convention on Human Rights states that a public authority can interfere with the right to privacy for national security purposes "in accordance with the law" when "necessary in a democratic society." The European Court of Human Rights has set out a detailed set of criteria to govern surveillance. Among other criteria, government surveillance must be subject to a strong legal framework that is transparent, necessary to achieve a legitimate goal and proportionate to that goal, authorized by a competent judicial authority, and subject to public oversight.[9] We do not believe the current national security programs in the U.S. meets these standards, but are less than sanguine that EU member state programs fare any better.

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

A. The Constitution and Statutes

Before addressing the U.S. programs, I would like to briefly explain U.S. law, which is complicated with respect to privacy. Some commentators in Europe have said that the U.S. does not view privacy as a fundamental right and therefore does not afford privacy rights to non-citizens. The truth is more complicated. To begin with, 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.[10] 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.

The problem from a European 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 American citizens, however, do not enjoy the full protection of the Constitution when the U.S. government is conducting searches outside the

---

[9] See, *Klass and others v. Federal Republic of Germany, European Court of Human Rights* (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978; ***see also***, *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006; ***see also***, *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008; ***see also***, *Kennedy v United Kingdom*, Application No. 26839/05, 18 May 2010.

[10] 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.

U.S.[11] 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.[12]

B. The "third party records" doctrine

The Supreme Court has 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. 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 US government (in law enforcement or national security investigations) to acquire call detail records and Internet metadata for citizens or non-citizens alike (whether such individuals are inside or outside the U.S. at the time of acquisition).

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.[13] Until recently, however, the courts have applied a very broad interpretation of the doctrine 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.[14] 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.

---

[11] 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.

[12] 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.

[13] 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.

[14] *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).

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.[15] 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.[16] 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.[17] 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.[18] Before the PATRIOT Act, a predecessor "business records" law[19] 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 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.[20] 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. Europeans communicating with Americans are undoubtedly caught up in the telephony metadata

---

[15] 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*.

[16] *Id.*

[17] 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/.

[18] 50 U.S.C. § 1861.

[19] 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.

[20] *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.

dragnet as well.[21] The telecommunications companies receiving these orders are prohibited by law from revealing orders or notifying customers.[22] Telecommunication companies are required to provide data "on an ongoing daily basis" for a three month period. [23] Although the Office of the Director of National Intelligence ("ODNI") stresses the fact that communications content is not collected under this program,[24] metadata "can be incredibly revealing—sometimes more so than the actual content."[25] 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."[26] 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.[27]

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."[28] 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.[29]

Furthermore, analysts may query the metadata three "hops" from a suspected individual.[30] 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

---

[21] 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.

[22] 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").

[23] *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.

[24] *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*.

[25] 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/.

[26] 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/.

[27] 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/.

[28] *DNI Disclosure June Response*.

[29] *See*, *id*.

[30] 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.

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.[31] By engaging in "three hop" analysis, the NSA can scrutinize data relating to as many as a million persons.

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 metatdata. 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."[32] 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.[33]

Several lawsuits have been filed challenging the telephony metadata bulk collection program, alleging violations of various statutes and the United States Constitution.[34] Additionally, advocacy groups have filed suits seeking disclosure of additional information regarding the nature of the program and the FISC's evaluation of it.[35]

CDT believes that the telephony metadata program of the NSA violates the Constitution. 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. We note that an amendment offered this summer in the House of Representative to end the program failed by a remarkably narrow margin of 217 to 205 but we also must advise you that there remains strong support in Congress for the program.

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

This brings me to the other major surveillance activity revealed by Snowden, and that is the

---

[31] *Id*.

[32] *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*.

[33] *Id.* (internal citation omitted).

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

[35] 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.

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."[36] 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[37] 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."[38] 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

---

[36] FISA defines "foreign intelligence information" 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).

[37] 50 U.S.C. 1881a.

[38] 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/.

world's Internet traffic,[39] 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[40] 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."[41] The level of access that NSA has to user data from the companies issued orders is unclear.[42] 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.[43]

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 foreigners outside the U.S. Perhaps the most significant restriction on Section 702 surveillance -- and it isn't much -- is that a significant purpose of the surveillance must be to collect foreign intelligence information. However, as noted above, that term is broadly defined to include, for example, information that relates to U.S. foreign affairs.

The principal requirement for targeting under the FAA is a determination of foreignness of potential surveillance targets.[44] 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.[45] On the basis of these broad standards, the NSA has compiled a list of 117,675 active targets.[46] The Targeting Guidelines permit the monitoring of communications not only of targets themselves, but also all communications that are "about" a target. [47]

---

[39] *See*, *id*.

[40] 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?pagewanted=all&_r=2&.

[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] 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)").

[43] 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/.

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

[45] *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.

[46] 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/.

[47] *See*, 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?pagewanted=all&_r=2&.

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 [48] 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.[49] 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 enforcement and intelligence agencies.[50] The NSA may also retain all encrypted communications indefinitely.[51]

The Minimization Guidelines provide no restrictions to limit 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 EU citizens have had their communications collected under these programs or shared within the government.

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.[52] 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.[53]

In light of the clear need for greater transparency about the scope and nature of the NSA's programs, CDT has organized a broad coalition of dozens of Internet companies and civil society organizations to press the government on this issue. That coalition, which includes major companies like Google and Facebook as well as key civil society organizations like Human Rights Watch and the Electronic Frontier Foundation, issued a joint letter in July addressed to key leaders in the U.S. Executive Branch and Congress.[54] It asked that the Obama Administration give the companies permission to publish basic data about the specific numbers of government requests that the companies receive under specific national security surveillance authorities, and it asked Congress to pass a law clarifying that service providers have the right to publish such transparency reports even without special permission.

---

[48] *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%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[49] *Id*.

[50] *See*, *Id*.

[51] 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/.

[52] 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.

[53] *Id*.

[54] *See* Center for Democracy & Technology, *CDT Brings Together Major Internet Companies & Advocates To Demand More Transparency Around Government Surveillance* (July 18, 2013), *available at* https://www.cdt.org/pr_statement/cdt-brings-together-major-internet-companies-advocates-demand-more-transparency-around-.

In response to the Justice Department's refusal to permit companies to publish specific numbers about the surveillance requests they receive, five companies—Microsoft, Google, Yahoo!, Facebook, and LinkedIn—have brought motions before the FISC pressing for their First Amendment right to publish such data.[55] CDT, along with a coalition of free speech organizations, has filed a friend-of-the-court brief in support of several of these motions,[56] which have not yet been decided on. Meanwhile, the government has recently committed to the annual release of its own surveillance statistics.[57] However, we are concerned that these statistics may be more misleading than useful, not only because of the government's intent to combine several different categories of surveillance orders into single numbers, but also because the government will only be reporting on the number of "targets" affected by those orders rather than the number of all people, targeted and non-targeted alike, who's information the government has collected.[58]

III. Calls for reform in the U.S.

CDT has been working with other civil society groups, companies, and members of the U.S. Congress to support reform of key U.S. surveillance authorities. For a variety of technical reasons, an enormous portion of the world's international data traffic flows through the United States. U.S. cloud providers store a large proportion of the world's data in the U.S. and the U.S. can compel them to grant access under the broad authorities I have outlined. In addition, the U.S. government has developed unique capabilities to conduct surveillance and to draw intelligence from analysis of the product of that surveillance. With these strong surveillance capabilities and outsized access to communications data for surveillance purposes comes increased U.S. responsibilities. We believe that those responsibilities extend to protecting the privacy rights not just of Americans, but of Europeans and of other people world-wide. Our reform agenda reflects this belief.

- First, the PATRIOT Act should be amended to make it clear that the law does not permit the NSA to collect telephone, Internet, and other records in bulk. Instead, collection should be limited to records that pertain to terrorists, spies and the like, and to those in direct contact with them. This reform would ensure that the innocent, everyday communications of Americans, including those with family, friends and colleagues in Europe, are not swept up into a vast NSA database to be queried at the NSA's discretion. Members of Congress have introduced eight bills intended to end bulk collection;[59] none has yet been approved by the relevant committees.

---

[55] *See*, Sam Gustin, TIME, *Tech Titans Press Feds in Battle Over NSA Transparency* (September 10, 2013), *available at* http://business.time.com/2013/09/10/tech-titans-press-feds-in-battle-over-nsa-transparency/ (discussing Google, Facebook, Microsoft and Yahoo! Motions); *see also*, Center for Democracy & Technology, *LinkedIn Enters The Surveillance Transparency Fray in a Big Way* (September 18, 2013), *available at* https://www.cdt.org/pr_statement/linkedin-enters-surveillance-transparency-fray-big-way.

[56] *See*, Center for Democracy & Technology, *Civil Liberties Groups Support Google and Microsoft in Demanding Transparency from Secret Surveillance Court* (July 9, 2013), *available at* https://www.cdt.org/pr_statement/civil-liberties-groups-support-companies-demanding-transparency-fisc.

[57] *See*, Office of the Director of National Intelligence, IC On The Record, *Official Statement: DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities* (August 2, 2013), *available at* http://icontherecord.tumblr.com/post/59719173750/dni-clapper-directs-annual-release-of-information.

[58] *See*, Center for Democracy & Technology, *Administration Continues to Disappoint on Transparency Around NSA Surveillance* (August 30, 2013), *available at* https://www.cdt.org/pr_statement/administration-continues-disappoint-transparency-around-nsa-surveillance.

[59] Those bills, and other legislation introduced in response to disclosures about NSA surveillance, are summarized here: https://www.cdt.org/report/bills-pending-91113-relate-nsa-surveillance.

- Second, the procedures under which the FISC authorizes intelligence surveillance must be reformed so that a voice for privacy and human rights counterbalances the government's surveillance demands. Because FISC proceedings are conducted secretly and authorize surveillance the legality of which is seldom tested in open court, a special advocate should be appointed to argue the case for liberty. President Obama has endorsed this concept as have several former members of the FISC.

- Third, excessive secrecy that surrounds intelligence surveillance must be lifted, at least in part, and in a way that protects national security. The FISC's significant legal interpretations should be made available to the public with any necessary deletions to protect national security. The government should disclose annually the number of surveillance requests its makes under each surveillance authority, and likewise the number of people whose information was disclosed using that authority. Companies that receive government intelligence surveillance demands should be able to disclose similar information about the impact of those demands on their customers. As I mentioned earlier, there is a significant effort among companies and advocates in the U.S. to support reforms that would permit companies to provide greater transparency to their customers, including several lawsuits. Legislation has been introduced in the U.S. House of Representatives (the Surveillance Order Reporting Act, H.R. 3055) and in the U.S. Senate (the Surveillance Transparency Act, S. 1452) to require this transparency.

- Fourth, the United States government should acknowledge, and protect, the human right to privacy enjoyed by Europeans and others outside the United States. So far, it has not done that even though the right to privacy of correspondence is enshrined in Article 17 of the International Covenant on Civil and Political Rights, to which the U.S. is a signatory. Jurisdictional ambiguities in that treaty and in other international human rights instruments cannot justify in-country surveillance that deprives people abroad of their privacy rights.

- Fifth, U.S. law permits the government to compel companies to assist with NSA surveillance conducted for the purpose of collecting "foreign intelligence information" even though the target of surveillance is not a suspected terrorist, spy, or other hostile actor. Foreign intelligence information is so broadly defined that it includes purely political activities, such as a protest at a U.S. military installation or even a demonstration against racism. These kinds of activities are "related to" U.S. foreign affairs and therefore fit within the purpose restriction governing this surveillance. This must change. The broad purposes for which surveillance can be conducted under the PRISM program should be narrowed to protect the privacy and free speech rights of people outside the U.S.

- Finally, conducting surveillance through the back door should be outlawed. 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. It should also bar the NSA from searching through data collected in the PRISM program for information about Americans unless it meets the domestic standard for surveillance of Americans.

We presented[60] much of this reform agenda to the U.S. Privacy and Civil Liberties Oversight Board, a new, independent entity in the executive branch of the U.S. government. It is

[60] CDT's statement for the record at the PCLOB can be found here: https://www.cdt.org/pr_statement/cdt-submits-recommendations-privacy-civil-liberties-board.

charged with recommending to Congress and the President ways of ensuring that measures designed to protect against terrorism do not infringe on human rights.

PCLOB can act to protect the rights of both Americans and Europeans. Seizing on this, we also organized a letter to PCLOB[61] from civil society groups around the world calling for PCLOB to make recommendations designed to protect the human rights of people outside the United States. The U.S. obligations under the ICCPR should not be swept under the carpet.

As I said before, jurisdictional limitations in the ICCPR and other treaties should not cancel out a country's obligations to conduct surveillance in a way that respects privacy rights outside its borders. To that end, CDT is also organizing a project designed to assess human rights law in this area. We intend to develop scholarship and new thinking about preserving the human right to privacy in a world of big data and transnational data flows. We have addressed this issue already in public statements. [62]

In addition to reaching out to civil society groups, we have also reached out to tech companies in an effort to enlist their support for parts of this reform agenda. This outreach resulted so far in a letter to Congress and the Administration from an unprecedented coalition of Internet companies and advocates of free speech and privacy rights urging that companies be allowed to be transparent, on a granular level, about the intelligence surveillance demands they are receiving and must comply with.[63]

Finally, many, including EDRi, have called for the U.S. Congress to create a new, special committee to investigate intelligence surveillance broadly and make recommendations to rein it in to protect human rights. It would be similar to the Church Committee, which, in the 1970's, issued a report on abuses by the intelligence community that led Congress to enact the Foreign Intelligence Surveillance Act and other measures to protect privacy. We support this call. However, creation of such a committee should not be an excuse for officials to delay reforms already clearly needed and that I have set forth above. We also caution that such a special committee would likely, given the make up of Congress, include some of the most vocal supporters of the intelligence surveillance activity we would seek to curtail.

IV. Promoting Reform on an International Basis

The Snowden leaks have brought to the forefront an issue of global concern in this digital age: the mismatch between legal protections for privacy and governments' surveillance capabilities. Earlier this year, before the leaks, the U.N. special rapporteur Frank LaRue surveyed the significant changes in the way communications surveillance is conducted by States and concluded that there was an "urgent need … to revise national laws regulating these practices in line with human rights standards." The European institutions clearly have an important role to play in this process by helping to define and enforce a set of rules that could be globally influential.

---

[61] The letter can be found here: http://bestbits.net/pclob/.

[62] *See*, Leslie Harris, *Surveillance is no longer the Cold War mentality of "us" and "them" in Index on Censorship*, *available at* http://www.indexoncensorship.org/2013/08/bringing-global-human-rights-into-the-surveillance-debate/; *see also*, Emma Llanso, Center for Democracy and Technology, Bringing global human rights Into the surveillance debate (August 7, 2013), *available at* https://www.cdt.org/commentary/bringing-global-human-rights-surveillance-debate.

[63] Submission by European Digital Rights Initiative and Fundamental Rights Experts Group on Surveillance Activities, p.4, *available at* https://www.cdt.org/weneedtoknow.

In our view, reform is most likely if institutions and stakeholders in the U.S. and Europe work together. On the one hand, European governments must assess their own security surveillance practices against human rights principles and must develop more explicit agreement about the criteria and oversight structures that translate those principles to national security surveillance in this era of globalized communications services and networks. At the same time, Europe should commence a dialogue with the U.S. aimed at seeking a common, trans-Atlantic understanding of those rules and oversight structures in both the national and trans-border contexts.[64] This approach, if successful, would "lift all boats," enhancing protections for both Europeans and Americans. And it could set a standard for the rest of the world.

A. Transparency

The process of reform must begin with transparency. Although the Snowden leaks have been accompanied by some startling disclosures about the nature and extent of systematic surveillance in some EU Member States,[65] we still know far too little about surveillance laws and practices in the EU overall. As a result, it is difficult to know to what extent the laws of EU Member States measure up against the principles in the European Convention as interpreted by the European Court of Human Rights.

For the past several years, CDT has been involved in a project researching the laws under which surveillance programs operate in a cross-section of countries.[66] A key finding of our research is that it is very difficult to assess actual practices, because the relevant laws are at best vague and government interpretations of them are often hidden or even classified (as they are in the U.S.).[67] This lack of clarity was raised in a 5 September statement by the German State and Federal DPAs,[68] who pointed to the very real possibility that surveillance programs operated by EU Member States fail to live up to the human rights standards and principles set out in the COE Convention and the Fundamental Charter. As several MEPs have pointed out, there has been near silence from EU Member State since the Snowden revelations started appearing, suggesting a reluctance to open these practices to scrutiny.

On 12 September, Jacob Kohnstamm pointed out to this Committee that several European countries operate data collection programs that are similar in nature if not in scope to the NSA's systems. And, we have also learned that there seems to be very widespread sharing

---

[64] A petition signed by several European and international civil society groups calls on EU leaders to address this problem urgently: http://www.change.org/en-GB/petitions/eu-leaders-stop-mass-surveillance.

[65] *See*, 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; *see also*, 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; *see also*, Le Monde, *Révélations sur le Big Brother français* (July 4, 2013), *available at* http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html; *see also*, 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.

[66] Country reports: http://idpl.oxfordjournals.org/content/2/4.toc.

[67] Fred H. Cate, James X. Dempsey, and Ira S. Rubinstein, 'Systematic government access to private-sector data' (2012) 2 *International Data Privacy Law* 195. http://idpl.oxfordjournals.org/content/early/2012/09/17/idpl.ips027.full

[68] Hunton and William LLP, Privacy and Information Security Law Blob, *German DPAs Pass Resolution on PRISM, Tempora and XKeyscore* (September 10, 2013), *available at* http://www.huntonprivacyblog.com/2013/09/articles/german-dpas-pass-resolution-on-prism-tempora-and-xkeyscore/.

of data among the intelligence agencies of a wide range of countries, within and outside the EU. The most prominent example this inquiry heard of was the 5EYES program, comprising the U.K., U.S., New Zealand, Australia, and Canada, but we were also told that Sweden has extensive collaboration with the intelligence agencies of these countries.

The key point is that we lack an accurate or comprehensive understanding of systematic access because both its legal basis and actual practice are hidden from public view. Furthermore, as Jacob Kohnstamm told this committee on 12 September, most of the Data Protection Authorities in Member States have no jurisdiction or oversight of the activities of intelligence agencies.

As I explained earlier, there is a concerted effort in the U.S. to demand greater public transparency in surveillance programs. There should be a concerted effort to enhance transparency in Europe as well. Clarity on the laws and practices in place in Member States is critical so that citizens and policymakers can understand the extent to which broad systemic surveillance programs are in place in Member States and what safeguards if any are provided and to whom. Key questions that might be addressed include: What data is collected and how? Which other European and non-European intelligence services, if any, is data shared with? In addition to national security programs, what data is being systematically collected by other public authorities, such as law enforcement, tax, and social services? Is data systematically collected with the assistance (mandated or voluntary) of companies, and if so, what agreements exist between law enforcement, national security agencies, and private sector companies?

B. Developing Common Criteria for National Security Surveillance

The European human rights framework is well-developed.[69] But it is not certain that the European Court of Human Rights will always view systematic surveillance as inconsistent with human rights standards. For example, in *Liberty v. United Kingdom*, the Court found that a UK systematic surveillance program violated the COE convention. However, in another case, *Weber & Saravia v. Germany*, the Court found that the German program of strategic (non-particularized) surveillance did not violate the Convention.[70] In these two cases, and a handful of others, the Court identified a set of criteria that it used to evaluate a statutory and oversight structure surrounding national security surveillance, especially where there are trans-border implications. However, to our knowledge, the criteria articulated by the ECtHR on a case-by-case basis have not yet been comprehensively compiled nor have they been uniformly adopted by Member States in their surveillance laws and practices.

And while the Charter of Fundamental Rights establishes protection of privacy as a fundamental right, so far EU law has not addressed these surveillance issues (and we recognize there are limits to the competency of EU institutions to do so). Both existing and draft EU data protection law explicitly do *not* cover the processing of data for national security purposes. This is the case both for the proposed Data Protection Regulation

[69] The human rights standards set out in the European Convention on Human Rights and the EU Charter of Fundamental Rights are reflected in the Treaty on the Functioning of the EU. These principles closely follow those set out in the ICCPR, and are reinforced in the recent report to the United Nations Human Rights Council by the Special Rapporteur on promotion and protection of the right to freedom of expression and opinion. *Available at*, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx

[70] *Liberty v. United Kingdom*, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207#{%22itemid%22:[%22001-87207%22]}; *Weber and Saravia v. Germany*, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-76586#{%22itemid%22:[%22001-76586%22]}.

("DPR") and the proposed Directive on Data Protection in law enforcement.[71] (And that Data Protection Directive, while it would put some controls on processing by law enforcement after collection, does not set *any* limits on the measures authorities can take to collect data for law enforcement in the first place.)

We know that there are some proposals to address in the DPR the concerns raised by the U.S. surveillance programs, possibly by creating some type of adequacy provision that would curtail transfers of data to third countries that do not provide adequate protections against government surveillance. CDT strongly supports the core principles and objectives of the DPR. Alongside our efforts to reform FISA and other U.S. laws on government surveillance, we are pushing hard in the US for enactment of a comprehensive federal consumer privacy law. However, we do not see how an adequacy provision for national security access is possible when the criteria articulated by the ECtHR have not been uniformly adopted by all EU Member States for national security surveillance. Likewise, without a process to benchmark Member States' laws and practices against the Human Rights Convention, the Charter, and the case law on government surveillance, the suspension of the safe harbor would seem to limit data flows because the U.S. government does not adhere to a standard that has not even been evenly applied by Member States.

In this regard, we are mindful of the point we made above, which is that any actions taken by Europe will be looked to as a model by the rest of the world. In this context, we have concerns about proposals to require that data be confined to particular jurisdictions. CDT and other civil society groups worldwide have worked hard to maintain the free and open Internet. Frequently, authoritarian regimes have argued for more government and national control of the Internet. One of the means to ensure such control is to mandate local storage of data, and to restrict the free flow of information on the Internet. Such requirements risk fragmentation of the Internet and suppression of human rights. If the EU, a globally recognized as a leader in promotion of human rights and an open Internet, were to go down this road, even for entirely understandable reasons, we worry that it would create a bad precedent, which repressive regimes would be only too eager to follow.

It is for these reasons that we recommend a trans-Atlantic process to develop a comprehensive understanding of the criteria that should apply to government surveillance and especially to national security surveillance. In our view, the current state of affairs both in the U.S. and in the EU is indefensible. This is a shared problem, and the timing is right for both the U.S. and the EU Member States to bring greater transparency, proportionality and oversight to their electronic surveillance practices – in order to ensure that human rights principles are respected in both jurisdictions and to develop an agreement on what constitutes adequacy for government access to data, raising standards and practices across the board.

There is no silver bullet, and no quick fix. This will be a long and difficult process, but it is the only principled way to address these concerns. My organization looks forward to working with this Committee and all interested parties in advancing that process.

[71] *Available at* http://ec.europa.eu/justice/data-protection/law/index_en.htm#h2-5.