Testimony of

Alex Abdo
Staff Attorney
National Security Project
American Civil Liberties Union Foundation

Before the
Inter-American Commission on Human Rights

Hearing on Freedom of Expression and
Communications Surveillance by the United States

October 28, 2013

On behalf of the American Civil Liberties Union ("ACLU"), I would like to thank the Commission for holding this timely hearing and for the opportunity to testify on the recently revealed and unprecedented electronic surveillance efforts of the U.S. National Security Agency ("NSA").

The ACLU is a nationwide, nonprofit, nonpartisan organization dedicated to protecting human rights and civil liberties in the United States. The ACLU is the largest civil liberties organization in the country, with offices in 50 states, Washington, DC, and Puerto Rico, and over 500,000 members dedicated to the protection and advancement of liberty, equality, fairness, and freedom, especially for the most vulnerable in our society.

I understand that the goal of this hearing is for the Commission to assess the compliance of the NSA's surveillance programs with the United States's international obligations with respect to the right to freedom of expression and related rights as recognized by the Inter-American system for the protection of human rights. In light of that goal, I will seek to clarify the scope of the recently revealed surveillance programs, the effects they may have on democratic freedoms, and the efforts undertaken by the ACLU and other civil society organizations to limit them.

Introduction

Thanks to Edward Snowden and a handful of particularly courageous reporters, the United States is now in the middle of a long-overdue debate about government surveillance and civil liberties.

Over the past four months, it has become clear that the NSA is engaged in far-reaching, intrusive, and in certain respects unlawful surveillance of telephone calls and electronic communications both within and outside the United States.

- Under Section 215 of the Patriot Act—formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001—the NSA is collecting the "telephony metadata" of every single phone call into, out of, and within the United States.

- Under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") Amendments Act of 2008, the NSA is surveilling the content of electronic communications all around the world to an extent not previously understood.

- The NSA has defeated most encryption tools used to guard global commerce and banking systems, protect sensitive data like trade secrets and medical records, and secure the emails, Web searches, Internet chats and phone calls of Americans and others around the world. Security experts have raised the concern that in undermining the security of communications for its own purposes, the NSA has made everyone's communications less safe from other governments and private actors as well.

- Through the Hemisphere Project, the Drug Enforcement Agency ("DEA") has routine access, using subpoenas, to an enormous database of AT&T call records stretching back as far as 1987. While this particular program appears to focus on analyzing call data for domestic law enforcement investigations, the Commission should take note that mass data surveillance programs are not inherently limited to the arena of national security.

These surveillance programs should be of particular concern to the Commission because they rely upon an extraordinarily permissive view of the scope of legitimate governmental surveillance, particularly with regard to the communications of foreigners. We now live in an age in which digital communication not only enables our expressive and associational freedoms, but has become central to them. Our ability to trust the relative security of those communications from unjustified government interference has, however, been deeply eroded by the astonishing breadth of the NSA's surveillance programs.

Simply put, if every country were to embrace as unfettered an approach to surveillance as the NSA, we would soon live in a world of pervasive monitoring. And if every country were to embrace as seemingly lenient a policy on the sharing of surveillance with other countries, then there would be no refuge for the world's dissidents, journalists, and human rights defenders.

It is our hope that the Commission will help forestall those dire possibilities by recommending that, in conducting surveillance, the United States respect and ensure the rights to

freedom of expression and opinion, to privacy, and to freedom of association, long recognized under international law, including in Articles 4 (freedom of expression and opinion), 10 (right to privacy of communications) and 22 (right to association) of the American Declaration on the Rights and Duties of Man, as well as the corresponding articles of the International Covenant on Civil and Political Rights, Articles 19 (freedom of expression and opinion), 17 (right to privacy) and 22 (freedom of association).

In the balance of my testimony, I will discuss what we now know of the NSA's surveillance programs.

The NSA's Sweeping Surveillance of the World

For many years, the ACLU has been concerned about the breadth of Section 702 of the FISA Amendments Act, which is the legal basis for the recently disclosed PRISM and UPSTREAM surveillance programs. While questions remain about the exact scope of these programs, they prompt deep concern because private citizens around the world have a strong interest in ensuring that governments eavesdrop upon their communications in only a targeted manner when there is an adequate reason to do so.

Under the FISA Amendments Act, however, the NSA is authorized to engage in dragnet surveillance of international communications when two primary conditions are satisfied: first, the targets of the NSA's surveillance must be foreigners, and second, the purpose of the NSA's surveillance must be to gather "foreign intelligence."[1]

Neither of these restrictions has any bite. Although the NSA must target its surveillance efforts, it is authorized to monitor international communications "about" its targets. The NSA has interpreted this authority to allow it to scan the content of any communication that originates or terminates outside the United States for keywords related to its targets.[2] Additionally, the phrase "foreign intelligence" is defined extraordinarily broadly to include information related to the United States's "foreign affairs."[3] Thus, the NSA's surveillance authority is *not* limited to the investigation of suspected terrorists or criminals, but includes the gathering of information about anything relevant to U.S. interests abroad. That already lax requirement is implemented even more laxly: the NSA considers the fact that a foreigner is a party to an international communication to be evidence that the communication contains "foreign intelligence."[4]

The effect of the NSA's broad understanding of its surveillance authority under the FISA Amendments Act is to make virtually every international communication fair game for surveillance. Recent news stories have suggested that the NSA's surveillance is in fact this broad

[1] 50 U.S.C. § 1881a(g)(2).

[2] Charlie Savage, *NSA Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

[3] 50 U.S.C. § 1801(e).

[4] Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed To Be Located Outside the United States To Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended 4–5 (Jan. 8, 2007), https://www.aclu.org/files/natsec/nsa/20130816/FAA%20Targeting%20Procedures.pdf.

in practice. Two separate programs, known as PRISM and UPSTREAM, collect the content of electronic communications in which at least one party is believed to be a non-U.S. person. Through the PRISM program, the U.S. government regularly demands emails, audio and video chats, photographs, and other internet traffic from nine major service providers, including Microsoft, Google, and Facebook.[5] Under the UPSTREAM program, the government scans the contents of nearly all text-based communications that enter or leave the United States for keywords "about" foreign intelligence targets.[6] Documents have confirmed that at least twenty-nine foreign nations have been subjected to surveillance by the NSA.[7] For example, the media has reported that the NSA collects and stores data from approximately half a billion German communications each month.[8] Just a few days ago, *Le Monde* reported (based on documents disclosed by Mr. Snowden) that "from 10 December 2012 to 8 January 2013, 70.3 million records of French citizens' telephone data were made by the NSA.[9]

The NSA has also engaged in targeted surveillance of friendly foreign governments, including members of the Organization of American States. Reports recently surfaced that the United States had monitored the phone calls of President Dilma Rousseff of Brazil, and the communications of Petrobras, Brazil's state oil corporation.[10] And just last week, *Der Spiegel* (again using documents obtained from Mr. Snowden) revealed that the NSA had hacked the email accounts of former President of Mexico Felipe Calderón and his cabinet to obtain "diplomatic, economic and leadership communications which continue to provide insight into Mexico's political system and internal stability."[11] Reports also indicate that the NSA has bugged the headquarters of the United Nations and the European Union.[12]

In at least one respect, the revelation of the NSA's extraordinary surveillance of foreigners is not surprising, for the U.S. government takes the position that there are few if any domestic limits on its authority to surveil foreigners. The U.S. government has yet to explain

---

[5] *NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post, July 10, 2013, http://wapo.st/1bafoN6.

[6] *Id*.

[7] Andrea Peterson, *The NSA's Alleged Global Spying Operation in One Map*, Wash. Post, Sept. 17, 2013, http://wapo.st/1fdYjrK.

[8] Laura Poitras, Marcel Rosenbach & Holger Stark, *Partner and Target: NSA Snoops on 500 Million German Data Connections*, Der Spiegel Online, June 30, 2013, http://spon.de/adYxM.

[9] Jacques Follorou & Glenn Greenwald, *France in the NSA's Crosshair: Phone Networks under Surveillance*, Le Monde, Oct. 21, 2013, http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html.

[10] Simon Romero, *N.S.A. Spied on Brazilian Oil Company, Report Says*, N.Y. Times, Sept. 9, 2013, http://nyti.ms/15KWNuz.

[11] Jens Glüsing et al., *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*, Der Spiegel, Oct. 20, 2013, http://spon.de/ad3M5.

[12] Jason Burke, *NSA Spied on Indian Embassy and UN Mission, Edward Snowden Files Reveal*, Guardian, Sept. 25, 2013, http://gu.com/p/3j3zq/tw; *U.S. Spy Agency Bugged U.N. Headquarters: Germany's Spiegel*, Reuters, Aug. 25, 2013, http://reut.rs/18dDapC; Laura Poitras et al., *Attacks from America: NSA Spied on European Union Offices*, Der Spiegel, June 29, 2013, http://spon.de/adYwQ.

whether it believes its international obligations constrain its foreign intelligence surveillance in any meaningful way.

In the public debate that has taken place inside the United States since the Snowden revelations, the government has suggested that Americans should be unconcerned with its sweeping surveillance of international communications on the grounds that they only target foreigners. But contrary to the U.S. government's representations, Americans' communications are collected through programs authorized by the FISA Amendments Act. The NSA's procedures permit it to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.

In 2008, the ACLU filed a lawsuit challenging the constitutionality of the FISA Amendments Act. The lawsuit, *Amnesty International v. Clapper*, was filed on behalf of a broad group of attorneys and human rights, labor, legal and media organizations whose work requires them to engage in sensitive telephone and email communications with people outside the U.S. Those people include colleagues, clients, sources, foreign officials and victims of human rights abuses. The coalition included Amnesty International USA, Human Rights Watch, The Nation magazine, and the Service Employees International Union. In February 2013, the United States Supreme Court dismissed the lawsuit, on the grounds that our clients lacked standing to seek relief because they could not demonstrate with enough certainty that their communications would be intercepted under the program.

The NSA's Mass Call-Tracking Program

On June 5, 2013, *The Guardian* disclosed a previously secret Foreign Intelligence Surveillance Court order that compels a Verizon subsidiary to supply the government with records relating to every phone call placed on its network between April 25, 2013 and July 19, 2013. The order directed Verizon to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating to its customers' calls, both between the United States and abroad and wholly within the United States.

As many have noted, the order is breathtaking in its scope. It is as if the government had seized every American's address book—with annotations detailing which contacts she spoke to, when she spoke with them, and for how long.

We have since learned that the mass acquisition of Americans' call details extends to at least the country's three largest phone companies. We have also learned that the government has been collecting these telephone records for seven years.

The ACLU is itself a Verizon customer. On June 11, the ACLU filed a constitutional challenge to the mass call-tracking program on its own behalf, titled *ACLU v. Clapper*, alleging that this collection violates the ACLU's First and Fourth Amendment rights under the U.S. Constitution.

The U.S. Constitution's Fourth Amendment protects Americans against unreasonable searches and seizures. President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata

but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans' phone records, it clearly is. Call records can reveal personal relationships, medical conditions, and political and religious affiliations. As Professor Edward Felten explained in a declaration filed in support of our lawsuit challenging the program:

> Although it is difficult to summarize the sensitive information that telephony metadata about a single person can reveal, suffice it to say that it can expose an extraordinary amount about our habits and our associations. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations.[13]

Because the government's collection of Americans' call records supplies it with a rich repository of personal information, the U.S. Constitution requires that the collection be "reasonable" (or proportionate) in light of its aims. The call-records program is anything but, for it allows the government to conduct warrantless surveillance and because it allows the government to surveil every American in its pursuit of a discrete number of targets.

We have also argued that the program is unconstitutional under the First Amendment. The Supreme Court has recognized that government surveillance has an acute potential to stifle association and expression protected by the First Amendment. That is certainly the case for mass and long-term surveillance of organizations like the ACLU, whose employees routinely talk by phone with clients and potential clients about legal representation in suits against the government. Often, even the mere fact that ACLU employees have communicated with these individuals is sensitive or confidential. ACLU employees regularly receive calls from, among others, prospective whistleblowers seeking legal counsel and government employees who fear reprisal for their political views.

In addition to our lawsuit, we have joined with others to urge Congress to protect Americans' privacy by narrowing the scope of Section 215 of the Patriot Act. The ACLU has urged Congress to change the law so that the government may compel the production of records under the provision only where there is a close connection between the records sought and a foreign power or agent of a foreign power.

Conclusion

We hope that the Commission will carefully assess the human rights implications of the NSA's surveillance programs and the United States's international obligations with respect to the universal right to freedom of expression and related rights as recognized by the Inter-American system for the protection of human rights. Thank you again for the invitation to testify. The ACLU appreciates the Commission's attention to these issues.

[13] Declaration of Edward W. Felten ¶ 46, *ACLU v. Clapper*, No. 1:13-CV-3994 (S.D.N.Y. Aug. 26, 2013), https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.