



Testimony of

Catherine Crump  
Staff Attorney  
Speech, Privacy & Technology Project  
American Civil Liberties Union Foundation

Before  
Committee on Civil Liberties, Justice and Home Affairs  
Inquiry on Electronic mass surveillance of EU citizens

September 30, 2013

On behalf of the American Civil Liberties Union, I would like to thank the Committee for this opportunity to speak on electronic mass surveillance issues.

The ACLU is a nationwide civil society organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution and civil rights laws.

I understand that a goal of this hearing is to establish facts as regard the allegations reported by the media, such as the scope, legality, and proportionality of the U.S. government's mass surveillance programs. Given this, I will spend my time today identifying recently revealed programs of surveillance that are of particular concern to the ACLU, and describing the efforts undertaken by us and other civil society organizations to limit these programs. It is our hope that an understanding of the work U.S. civil society organizations are carrying out will aid this Committee's thinking in targeting its own efforts going forward.

### **Recent Revelations About Mass Surveillance By U.S. Agencies**

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 three months, it has become clear that the National Security Agency (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, the NSA is collecting the “telephone metadata” of every single phone call into, out of, and within the United States.
- Under Section 702 of the 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 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, Europeans should take note that mass data surveillance programs are not inherently limited to the arena of national security.

I am going to use the rest of my time to explain the ACLU’s advocacy efforts in some detail.

### **First, the NSA’s Collection of the Content of Internet Communications**

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 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 do not engage in the mass collection of communications content, and surreptitiously access content only in a targeted manner and when there is a strong reason to do so.

The U.S. government has suggested that Americans should be unconcerned with its content collections programs on the ground that they only target foreigners, but this argument should be rejected for a number of reasons.

First, while we're not naive about foreign intelligence surveillance—all countries engage in it—there's an important distinction between surveillance of other governments and large scale surveillance of foreign populations. And second, even if no law or treaty prohibits such mass surveillance, that doesn't mean governments should engage in it. Now that Snowden has pulled

back the curtain on the extent of these practices, we hope that citizens in democratic countries will speak out against the practices and demand that new limits be put in place.

Second, contrary to the U.S. government's representations, Americans' communications are collected through programs authorized by Section 702 of 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 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. It is impossible not to wonder if the case would have been decided differently had the Snowden revelations been known earlier.

### **Second, a few words about 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 the 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.<sup>1</sup>

---

<sup>1</sup> Charlie Savage, *A.C.L.U. Files Lawsuit Seeking to Stop the Collection of Domestic Phone Logs*, N.Y. Times (June 11, 2013), [http://www.nytimes.com/2013/06/12/us/aclu-files-suit-over-phone-surveillance-program.html?pagewanted=all&\\_r=1&](http://www.nytimes.com/2013/06/12/us/aclu-files-suit-over-phone-surveillance-program.html?pagewanted=all&_r=1&)

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 issues, and political and religious affiliations.

We also argue that the program is unconstitutional under the First Amendment. The Supreme Court has recognized that government surveillance can have 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**

Thank you again for the invitation to testify. The ACLU appreciates the Committee's attention to this set of issues.