Answers to Questions for the Record of
The Senate Judiciary Committee

Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy
Director, Washington Legislative Office
American Civil Liberties Union

Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs

August 22, 2013

QUESTIONS FROM THE CHAIRMAN

1. Your written testimony discusses the constitutional implications of the Section 215 phone records program. We have heard government witnesses state repeatedly that under the 1979 case of *Smith v. Maryland,* phone records and other digital data are not protected by the Fourth Amendment because we have already revealed them to a third party, and that only the contents of our communications are protected.

Q: Do you agree that the *Smith v. Maryland* case provides definitive guidance on the constitutional standard to be applied to the bulk collection of telephone metadata under the Section 215 program? Is there case law suggesting that courts are reconsidering this doctrine in the face of new technology?

Q: In today's world of technological convergence, social media, web browsing, and location-enabled devices, is it possible to draw a clear line between content that is protected by the Fourth Amendment, and non-content information that is not? What implications does this have for the constitutional analysis that is based on this distinction?

The government's reliance on *Smith v. Maryland*, 442 U.S. 735 (1979), is misplaced. The Supreme Court held in *Smith* that the government's use of a so-called "pen register" did not constitute a search under the Fourth Amendment, but the technology at issue in that case was very primitive—it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls. *Id.* at 741. The pen register was in place for less than two days, and it was directed at a single criminal suspect. *Id.* at 737 (noting that pen register was installed after woman who had been robbed began receiving threatening and obscene phone calls from man purporting to be robber). Moreover, the information the pen register yielded was not aggregated with information from other pen registers, let alone with information relating to hundreds of millions of innocent people. *Id.* Nothing in *Smith*—a case involving narrow surveillance directed at a specific criminal suspect over a very limited time period—remotely suggests that the Constitution would be indifferent to the government's mass collection of sensitive information about every single phone call made or received in the United States over a period of seven years. It is also important to remember that *Smith* was decided in 1979, when the government lacked the technological capability to conduct generalized surveillance of telephony metadata, to store the huge volumes of information that would be generated by it, or to analyze that information quickly.

The more relevant case is *United States v. Jones*, 132 S. Ct. 945 (2012), in which five Justices of the Supreme Court concluded that the government's long-term collection and aggregation of location information constituted a search. In *Jones,* the Supreme Court considered whether police had conducted a Fourth Amendment search when they attached a GPS tracking device to a vehicle and monitored its movements over a period of twenty-eight days. The Court held that the installation of the GPS device and the use

of it to monitor the vehicle's movements constituted a search because it involved a trespass "conjoined with . . . an attempt to find something or to obtain information." *Id.* at 951 n.5. In two concurring opinions, five Justices concluded that the surveillance constituted a search because it "impinge[d] on expectations of privacy." *Id*. at 964 (Alito, J., concurring); *accord id.* at 955 (Sotomayor, J., concurring). Justice Sotomayor explained:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.

Id. at 955–56 (citations and quotation marks omitted); *see also id.* at 964 (Alito, J., concurring).

What the five concurring Justices observed of long-term location tracking is equally true of the NSA's telephony metadata program. Call records can reveal personal relationships, medical issues, and political and religious affiliations. The government has sought to reassure the public that this program collects "only" metadata, not content, but metadata can be very rich, and the aggregation of metadata permits the government to assemble comprehensive maps of citizens' relationships to one another.

To the extent the government's argument is that individuals lack a constitutionally protected privacy interest in telephony metadata because that information has been shared with telecommunications companies, this argument, too, is mistaken. *Jones* makes clear that mere fact that a person has shared information with the public or a third party does not mean that the person lacks a constitutionally protected privacy interest in it. *Jones*, moreover, is only the most recent in a line of Supreme Court cases confirming that the so-called "third-party records doctrine" is more nuanced than the government contends it is. *See, e.g.*, *Florida v. Jardines*, 133 S. Ct. 1409 (2013) (odors detectable by police dog that emanate outside of a home); *Kyllo v. United States*, 533 U.S. 27 (2001) (thermal imaging available outside a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results in hospital); *Bond v. United States*, 529 U.S. 334, 338–39 (2000) (personal luggage in overhead bin on bus).

2. As an alternative to the government bulk collection of telephone metadata under Section 215, some have proposed requiring the telecommunications providers to retain these records for five years so the records can be searched when it is deemed necessary.

Q: Do you believe that such an arrangement would alleviate any privacy concerns that may exist with regard to the Section 215 bulk collection program?

The ACLU opposes legislative proposals that would compel telecommunications providers to create the same kinds of vast databases of Americans' most sensitive information that have until now been maintained by the government in secret. Housing this massive amount of Americans' information in private rather than government hands would not eliminate the potential for abuse and misuse; indeed, in some respects it would increase it. Moreover, the existence of massive databases of information relating to Americans' communications and interactions may have a chilling effect on the freedoms of speech and association even if the databases are in private rather than government hands. The problem with the call-records program is less about who is amassing and retaining those records than about the fact they are being amassed and retained for long periods in the first place.

Moreover, the government has simply not demonstrated that the long-term retention of this kind of sensitive information is actually necessary. As discussed further below, the government has been unable to supply evidence that the metadata program played a crucial role in any specific terrorism investigation or prosecution. The proper course of action for Congress is to end the program, not to repackage it.

QUESTIONS FROM THE RANKING MEMBER

1. Would ending the collection of telephone metadata in bulk under Section 215—and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected—affect the government's ability to protect national security by "connecting the dots" of terrorist plots? Why or why not?

There is no evidence that the metadata program has provided uniquely valuable intelligence information. Members of the Senate Select Committee on Intelligence, which oversees the call-tracking program, have made clear that they have seen no evidence either in a public or classified setting that substantiates the intelligence community's general claims about the program's effectiveness.[1] In addition, the Chairman of this Committee reviewed a classified list of terrorist events supposedly prevented by the call-tracking program and reported that the program had not played a role in the breakup of even "several" plots.[2] The intelligence community has many tools at its disposal to capture and consult call data when it has reason to suspect an individual of terrorism.

---

[1] Press Release, *Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs*, June 19, 2013, http://www.wyden.senate.gov/news/press-releases/wyden-udall-issue-statement-on-effectiveness-of-declassified-nsa-programs.

[2] Hearing on Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, S. Comm. on the Judiciary (July 31, 2013) (statement of Sen. Patrick Leahy, Chairman), https://www.leahy.senate.gov/press/senate-judiciary-committee-holds-oversight-hearing-on-government-surveillance-programs.

Those tools include court orders under FISA and Title III, pen-register orders, national-security letters, and subpoenas—in addition to non-bulk business-records orders under Section 215. All of these tools allow the government to seek information about suspected terrorists without needlessly invading the privacy rights of millions of Americans at the same time.

Some defenders of the call-tracking program have suggested that eliminating ongoing bulk collection under Section 215 would slow down investigations in which speed is paramount, but, again, the public record is devoid of any examples of cases in which the government's possession of years of Americans' phone-call data proved to be important, let alone critical, in timely identifying a phone number of counterterrorism value. Moreover, law enforcement already has the ability to seek emergency orders or administrative subpoenas when time is of the essence. Intelligence officials have repeatedly pointed to one criminal case, *United States v. Moalin*, to defend the utility of the call-records database. But Senator Wyden recently noted to *The Washington Post* that in that case (which involved efforts to send $8500 to the Somali terrorist group al-Shabaab) the government did not arrest the principal defendant until long after analysis of the call database helped identify him.[3]

2. Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. In your view, would such an arrangement resolve your concerns about the legality of the telephone metadata program under Section 215? Why or why not?

See above.

3. Has the one-year ban on challenging non-disclosure orders under Section 215 posed practical problems or difficulties for private companies, especially since those companies may challenge the underlying order requiring the production of business records immediately? If so, what are they? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

It is of course impossible to know the extent to which the one-year bar has dissuaded private companies from challenging gag orders and has deprived the public of important information about the government's surveillance activities. In an analogous context, however, the recipient of a national-security letter explained the way an FBI-imposed gag order had affected his ability to disclose crucial information to Congress:

> The inspector general's report makes clear that NSL gag orders have had even more pernicious effects. Without the gag orders issued on recipients of the letters, it is doubtful that the FBI would have been able to abuse the NSL power the way that it did. Some recipients would have

[3] Ellen Nakashima, *NSA Cites Case as Success of Phone Data-Collection Program*, Wash. Post, Aug. 8, 2013, http://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_print.html.

> spoken out about perceived abuses, and the FBI's actions would have been subject to some degree of public scrutiny. To be sure, not all recipients would have spoken out; the inspector general's report suggests that large telecom companies have been all too willing to share sensitive data with the agency—in at least one case, a telecom company gave the FBI even more information than it asked for. But some recipients would have called attention to abuses, and some abuse would have been deterred.
>
> I found it particularly difficult to be silent about my concerns while Congress was debating the reauthorization of the Patriot Act in 2005 and early 2006. If I hadn't been under a gag order, I would have contacted members of Congress to discuss my experiences and to advocate changes in the law. The inspector general's report confirms that Congress lacked a complete picture of the problem during a critical time: Even though the NSL statute requires the director of the FBI to fully inform members of the House and Senate about all requests issued under the statute, the FBI significantly underrepresented the number of NSL requests in 2003, 2004 and 2005, according to the report.
>
> I recognize that there may sometimes be a need for secrecy in certain national security investigations. But I've now been under a broad gag order for three years, and other NSL recipients have been silenced for even longer. At some point—a point we passed long ago—the secrecy itself becomes a threat to our democracy. In the wake of the recent revelations, I believe more strongly than ever that the secrecy surrounding the government's use of the national security letters power is unwarranted and dangerous. I hope that Congress will at last recognize the same thing.[4]

The danger of the one-year prohibition is that it may prevent an individual or business from disclosing important information to the public or to Congress until after the value of the information has diminished or disappeared. It is important to remember that most information in the public domain about the government's surveillance programs is provided by the government itself. Gag orders related to the government's use of these programs prevent the public from confronting concrete examples of how these programs affect Americans who are forced to comply with them. Indeed, one reason that the public and Congress have reacted so energetically to the revelations made just a few months ago is that they disclosed the existence of expansive and intrusive government powers that had remained almost entirely secret for many years. Nondisclosure provisions thwart meaningful and necessary discussion about the government's surveillance policies. As a result, they undermine the legitimacy of even properly drawn national-security policies. Wide-ranging and intrusive surveillance programs like the Section 215 call-tracking program require robust and fully informed debate. Gag orders stifle that debate.

---

[4] Anonymous, *My National Security Gag Order*, Wash. Post, March 23, 2007, http://wapo.st/XBX7g.

At the same time, removing the one-year bar would not jeopardize national security in any way. Removing the bar, after all, would not prevent the government from imposing a gag order; its only effect would be to require the government to defend certain gag orders to a court.

As explained in earlier submitted testimony, the one-year bar is not the only problem with Section 215's gag-order provisions.[5] Removing the one-year bar, however, should be part of a larger reform package.

4. Would the government's annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

a. How many FISA court orders were issued;
b. How many individuals' (foreign and U.S. persons) information was collected;
c. How many U.S. persons' information was collected; and
d. How many U.S. persons' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

5. Would the government's annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

a. How many FISA court orders were issued;
b. How many individuals' (foreign and U.S. persons) information was collected;
c. How many U.S. persons' information was collected; and

6. Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

[5] *See* Hearing on Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, S. Comm. on the Judiciary (July 30, 2013) (written testimony of Jameel Jaffer and Laura Murphy), http://1.usa.gov/18CuNpF (discussing, among other things, the requirement that reviewing courts defer to the government's determination of whether secrecy is necessary).

a. How many FISA court orders the company received;
b. The percentage of those orders the company complied with;
c. How many of their users' information they produced; and
d. How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

7. Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

a. How many FISA court orders the company received;
b. The percentage of those orders the company complied with; and
c. How many of their users' information they produced.

As we wrote in our earlier-submitted written testimony, the public should have access to basic statistics concerning the government's use of new surveillance authorities. Amendments to FISA made since 2001 have substantially expanded the government's surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of Congress and the public have learned more about domestic surveillance in last three months than in the last several decades combined.

We know of no practical reason why the government could not disclose the statistics listed above. If the government cannot say precisely how many U.S. persons' information was collected, Congress should require it to disclose an estimate. Neither Congress nor the public can evaluate the implications of the government's surveillance activities without knowing how broad those activities are.

Nor do we know of any reason why private corporations could not disclose the statistics listed above. Some private corporations have said they would like to disclose these statistics in order to help the public understand what steps they are taking to protect their customers' privacy.[6] Some of these corporations have said that the restrictions on their disclosure of these statistics puts them at a disadvantage vis a vis their competitors in other countries.[7] On June 18, 2013, Google and Microsoft separately petitioned the

[6] *See, e.g.*, Ted Ullyot, *Facebook Releases Data, Including All National Security Requests*, Facebook Newsroom, June 14, 2013, https://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests ("We will continue to be vigilant in protecting our users' data from unwarranted government requests, and we will continue to push all governments to be as transparent as possible.").

[7] *See, e.g.*, Ryan W. Neal, *NSA Surveillance Costing U.S. Businesses Billions: PRISM, XKeyScore Hurt American Cloud Companies*, Int'l Bus. Times, Aug. 9, 2013, http://www.ibtimes.com/nsa-surveillance-costing-us-businesses-billions-prism-xkeyscore-hurt-american-cloud-companies.

FISC arguing that the First Amendment permitted them to release aggregate statistics about two categories of national-security requests: those issued under Section 215 and Section 702.[8] (These companies already disclose broad approximations of the number of national-security letters they receive, but they have not been permitted to disclose the exact number, or the number of individuals whose privacy was implicated by these letters.[9]) More recently, a coalition of Internet companies including Google and Microsoft—as well as other technology giants like AOL, Apple, Facebook, Mozilla, Twitter, and Yahoo!—signed a public letter addressed to the President, this Committee, and others urging the government to allow regular reporting of statistics reflecting: (1) the number of government requests that they receive under surveillance authorities like Section 215, Section 702, and the national-security-letter statutes; (2) the number of individuals, accounts, or devices about which the government requested under each authority; and (3) the number of requests under each authority that sought communications content, subscriber information, or other information.[10] The companies also requested that the government itself publish a regular "transparency report" that aggregates the total number of requests the government makes under its surveillance authorities as well as the total number of individuals affected by those requests.

It is important to note that aggregate statistics alone would not allow the public to understand the reach of the government's surveillance powers. As we have seen with Section 215, one application may implicate the privacy of millions of people. It is crucial that Congress require the disclosure of richer statistical information as well as relevant decisions of the FISC.

The release of this information would not compromise national security. There may be a very narrow category of exceptions—for example, the release of certain information by a small Internet Service Provider could, in certain time-limited circumstances, tip off one of its clients about surveillance directed at it. But these exceptions will quite clearly be rare, and any rules surrounding statistical releases can be crafted in ways that avoid these kinds of problems. (One possibility would be to permit private corporations to disclose precise numbers only if they received more than ten demands under a given national-security provision, and otherwise to disclose only that they received between one and ten demands under that provision.)

---

[8] *See* Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders, *In re Motion for Declaratory Judgment*, Misc. 13-03 (FISC June 16, 2013), http://www.uscourts.gov/uscourts/courts/fisc/misc-13-03-motion.pdf; Microsoft Corporation's Motion for Declaratory Judgment or Other Appropriate Relief Authorizing Disclosure of Aggregate Data Regarding Any FISA Orders It Has Received, *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, Misc. 13-04 (FISC June 16, 2013), http://www.uscourts.gov/uscourts/courts/fisc/misc-13-04-motion.pdf.

[9] *See*, *e.g.*, Google, Transparency Report: User Data Requests, https://www.google.com/transparencyreport/userdatarequests/US/.

[10] Letter from Coalition to President Barack Obama *et al.* (July 18, 2013), https://www.aclu.org/files/assets/weneedtoknow-transparency-letter.pdf.

Again, the release of these statistics would permit a more informed debate about the government's surveillance activities. It would also increase the democratic legitimacy of practices that the country collectively chooses to endorse. In the long run, it could also restore the confidence of Americans and others in the American companies that hold so much sensitive information relating to their users.

8. When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

The ACLU generally supports proposals to make proceedings before the FISC adversarial. In particular, we support the FISA Court Reform Act of 2013 sponsored by Senators Blumenthal, Wyden, and Udall. That bill would create an Office of the Special Advocate (OSA) to advocate before the FISC for legal interpretations that minimize the scope of intrusion into individual privacy. The OSA would have the authority to appeal FISC decisions. The bill would also allow third parties to participate as amici in cases involving significant or novel issues of law. Finally, it would require the disclosure of significant legal opinions issued by the FISC and the FISCR.

As we stated in our earlier-submitted testimony, we believe that any reform to the FISC should be paired with reforms to the substantive surveillance laws. These laws, including Sections 215 and 702, are far too broad, and no structural reform will be meaningful if the substantive surveillance laws are not significantly narrowed.

9. Do you believe that the FISC is a rubber stamp for the government? If not, what explains the government's high success rate before it? Is that success rate in part the product of a "give and take" process by which the Court reviews the government's applications and provides feedback?

The true problems with the FISC are structural ones—meaning they are capable of being addressed by Congress. In a letter to the Chairman of this Committee dated July 29, 2013, Presiding Judge of the FISC, the Hon. Reggie B. Walton, explained the process by which FISC orders are approved and addressed several questions from the Chairman about the operation of the court.[11] Judge Walton described the work of the FISC as an essentially collaborative process between FISC judges, clerks, and staff and government attorneys.[12] He also generally outlined the procedures the court uses to approve regular

[11] *See* Letter from Hon. Reggie B. Walton, Presiding Judge, FISC, to Sen. Patrick Leahy, Chairman, Senate Judiciary Committee (July 29, 2013), http://www.scribd.com/doc/156993381/FISC-letter-to-Leahy.

[12] *See id.* at 5–7.

FISA orders, bulk-collection orders under Section 215, as well as Section 702 applications.[13] In doing so, Judge Walton noted the oft-cited statistic that final FISA applications are approved more than 99% of the time. And he provided a rare window into the operation of an extremely and unusually secretive judicial institution.

As Judge Walton's letter notes, the FISC was created to hear individualized surveillance applications, but its docket has changed quite dramatically in recent years. Thirty years ago, the FISC's principal task was to determine whether the government had, in any given case, demonstrated probable cause to believe that a specific surveillance target was an agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2). Today, the FISC addresses novel and complex statutory and constitutional questions in order to evaluate the lawfulness of broad surveillance programs that rely on complicated and quickly changing technology.

10. Does the Fourth Amendment or any other protections under the Bill of Rights apply to non-U.S. persons in foreign countries? Why or why not? What does this mean for orders issued under Section 702?

Orders issued under Section 702 must conform to the Fourth Amendment not because non-U.S. persons in foreign countries have Fourth Amendment rights but because Americans and others living in the United States have Fourth Amendment rights. Because Americans have a reasonable expectation of privacy in their international communications, surveillance that implicates those communications must conform to the Fourth Amendment's requirements.

This is not to say that Congress should be indifferent to the privacy rights of foreigners living outside the United States. The United States has obligations to respect and protect the rights to privacy and free expression under international instruments like the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It also has a political interest in respecting the privacy rights of foreigners outside the United States. As the Chairman of this Committee has said "repeatedly, . . . just because we have the ability to collect huge amounts of data does not mean that we should be doing so."[16] The damage to the credibility and moral authority of the United States that these surveillance programs has inflicted is plain, and the government's ability to apply pressure to other countries who engage in violations of human rights has been significantly diminished.

11. To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

Public access to the FISA Court's substantive legal reasoning is essential. Without it, some of the government's most far-reaching policies will lack democratic legitimacy.

---

[13] *See id.* at 1–5.

[16] *See* Statement of Sen. Patrick Leahy, *supra* note 2.

Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.[17] Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA's sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such opinions, some close to one hundred pages long.[18] We are hopeful that the release of several FISC opinions earlier this week signifies a new commitment on the part of the government to ensure that the public has access to crucial information about the government's surveillance policies.

[17] *See, e.g.*, Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, http://wapo.st/170VVSu.

[18] *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, http://nyti.ms/12beiA3.