



Testimony of

Jameel Jaffer

Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy

Director, Washington Legislative Office
American Civil Liberties Union

Before

The Senate Judiciary Committee

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

July 31, 2013

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting the ACLU to testify before the Committee.

Over the last two months it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans' telephone calls and electronic communications. These unconstitutional surveillance programs are the product of defects both in the law itself and in the current oversight system. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government's surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly

used procedural doctrines to place the NSA's activities beyond the reach of the Constitution.

To say that the NSA's activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance "threaten[ed] to undermine our democratic society and fundamentally alter its nature." This warning should have even more resonance today, because in recent decades the NSA's resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately.

First, it should amend relevant provisions of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA's so-called "business records" provision, and to the national security letter authorities.

Second, it should end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Third, it should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.

Thank you again for the invitation to testify. We appreciate the Committee's attention to this set of issues.

I. Metadata surveillance under Section 215 of the Patriot Act

On June 5, 2013, *The Guardian* disclosed a previously secret FISC order that compels a Verizon subsidiary, Verizon Business Network Services (VBNS), to supply the government with records relating to every phone call placed on its network between

April 25, 2013 and July 19, 2013.¹ The order directs VBNS to produce to the NSA “on an ongoing daily basis . . . all call detail records or ‘telephony metadata’” relating to its customers’ calls, including those “wholly within the United States.”² 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, for how long, and (possibly) from which locations.

News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans’ call details extends beyond customers of VBNS, encompassing subscribers of the country’s three largest phone companies: Verizon, AT&T, and Sprint.³ Members of the congressional intelligence committees have confirmed that the order issued to VBNS is part of a broader program under which the government has been collecting the telephone records of essentially all Americans for at least seven years.⁴

Intelligence officials have said that the government does not “indiscriminately sift through” the phone-record database. Instead, it queries the database “only when there is reasonable suspicion, based on specific and articulated facts, that an identifier is associated with specific foreign terrorist organizations.”⁵ According to a statement released by the government last month, “less than 300 unique identifiers met this standard and were queried” in 2012.⁶ But even if the government ran queries on only 300 unique identifiers in 2012, those searches implicated the privacy of millions of Americans. Intelligence officials have explained that analysts are permitted to examine the call

¹ See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, June 5, 2013, <http://bit.ly/13jsdlb>.

² Secondary Order, *In Re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc’n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), available at <http://bit.ly/11FY393>.

³ See Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, <http://on.wsj.com/11uD0ue> (“The arrangement with Verizon, AT&T and Sprint, the country’s three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total.”); Siobhan Gorman & Jennifer Valentino-DeVries, *Government Is Tracking Verizon Customers’ Records*, Wall St. J., June 6, 2013, <http://on.wsj.com/13mLm7c>.

⁴ Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place ‘Since 2006,’* Guardian, June 6, 2013, <http://bit.ly/13rfdxdu>; *id.* (Senator Saxby Chambliss: “This has been going on for seven years.”).

⁵ See, e.g., *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Intelligence Comm.*, 113th Cong. (June 18, 2013) (testimony of NSA Deputy Director John C. Inglis), <http://bit.ly/15kZ9wh>.

⁶ See, e.g., Ellen Nakashima, *Call Records of Fewer Than 300 People Were Searched in 2012, U.S. Says*, Wash. Post, June 15, 2013, <http://wapo.st/148Z7Wm>.

records of all individuals within three “hops” of a specific target.⁷ As a result, a query yields information not only about the individual thought to be “associated with [a] specific foreign terrorist organization[]” but about all of those separated from that individual by one, two, or three degrees. Even if one assumes, conservatively, that each person has an average of 40 unique contacts, an analyst who accessed the records of everyone within three hops of an initial target would have accessed records concerning more than two million people.⁸ Multiply that figure by the 300 phone numbers the NSA says that it searched in 2012, and by the seven years the program has apparently been in place, and one can quickly see how official efforts to characterize the extent and impact of this program are deeply misleading.

a. The metadata program is not authorized by statute

The metadata program has been implemented under Section 215 of the Patriot Act—sometimes referred to as FISA’s “business records” provision—but this provision does not permit the government to track all Americans’ phone calls, let alone over a period of seven years.

As originally enacted in 1998, FISA’s business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international terrorism investigations by making an application to the FISC. *See* 50 U.S.C. §§ 1861-62 (2000 ed.). Only four types of records could be sought under the statute: records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862 (2000 ed.). Moreover, the FISC could issue an order only if the application contained “specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power.” *Id.*

The business records power was considerably expanded by the Patriot Act.⁹ Section 215 of that Act, now codified in 50 U.S.C. § 1861, permitted the FBI to make an application to the FISC for an order requiring

the production of *any tangible things* (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities

50 U.S.C. § 1861(a)(1) (emphasis added).

⁷ *See* Pete Yost, *Congress Expresses Anger Over NSA Surveillance Program*, Boston Globe, July 18, 2013, <http://b.globe.com/17moqWU>.

⁸ *Id.*

⁹ For ease of reference, this testimony uses “business records provision” to refer to the current version of the law as well as to earlier versions, even though the current version of the law allows the FBI to compel the production of much more than business records, as discussed below.

No longer limited to four discrete categories of business records, the new law authorized the FBI to seek the production of “any tangible things.” *Id.* It also authorized the FBI to obtain orders without demonstrating reason to believe that the target was a foreign power or agent of a foreign power. Instead, it permitted the government to obtain orders where tangible things were “sought for” an authorized investigation. P.L. 107-56, § 215. This language was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b). Under the current version of the business records provision, the FBI must provide “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant*” to a foreign intelligence, international terrorism, or espionage investigation. 50 U.S.C. § 1861(b)(2)(A) (emphasis added).¹⁰

While the Patriot Act considerably expanded the government’s surveillance authority, Section 215 does not authorize the metadata program. First, whatever “relevance” might allow, it does not permit the government to cast a seven-year dragnet over the records of every phone call made or received by any American. Indeed, to say that Section 215 authorizes this surveillance is to deprive the word “relevance” of any meaning. The government’s theory appears to be that some of the information swept up in the dragnet might become relevant to “an authorized investigation” at some point in the future. The statute, however, does not permit the government to collect information on this basis. *Cf.* Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, Guardian, June 9, 2013, <http://bit.ly/18iDA3x> (“[B]ased on the scope of the released order, both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended.”). The statute requires the government to show a connection between the records it seeks and some specific, existing investigation.

Indeed, the changes that Congress made to the statute in 2006 were meant to ensure that the government did not exploit ambiguity in the statute’s language to justify the collection of sensitive information not actually connected to some authorized investigation. As Senator Jon Kyl put it in 2006, “We all know the term ‘relevance.’ It is a term that every court uses. The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation.”¹¹

As Congress recognized in 2006, relevance is a familiar standard in our legal system. It has never been afforded the limitless scope that the executive branch is

¹⁰ Records are presumptively relevant if they pertain to (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This relaxed standard is a significant departure from the original threshold, which, as noted above, required an individualized inquiry.

¹¹ Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court’s Redefinition of ‘Relevant’ Empowered Vast NSA Data-Gathering*, Wall St. J., July 8, 2013, <http://on.wsj.com/13x8QKU>.

affording it now. Indeed, in the past, courts have carefully policed the outer perimeter of “relevance” to ensure that demands for information are not unbounded fishing expeditions. *See, e.g., In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (“What is more troubling is the matter of relevance. The [grand jury] subpoena requires production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.”).¹² The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of “relevance.”¹³

b. The metadata program is unconstitutional

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. 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.

The Supreme Court’s recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual’s location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual’s movements over an extended period allows the government to generate a “precise, comprehensive record” that reflects “a wealth of detail about her familial, political, professional, religious, and sexual associations.” *Id.* (Sotomayor, J., concurring).

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles she reads, whom she corresponds with, and whom *those* people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in *Jones*. In fact, the surveillance held unconstitutional in *Jones* was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in *Jones* was meant to further a specific criminal investigation into a specific crime, and the

¹² *See also Hale v. Henkel*, 201 U.S. 43, 76-77 (1906).

¹³ The metadata program also violates Section 215 because the statute does not authorize the prospective acquisition of business records. The text of the statute contemplates “release” of “tangible things” that can be “fairly identified,” and “allow[s] a reasonable time” for providers to “assemble[]” those things. 50 U.S.C. § 1861(c)(1)-(2). These terms suggest that Section 215 reaches only business records already in existence.

government collected information about one person’s location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Some have defended the metadata program by reference to the Supreme Court’s decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in *Smith*, however, was very primitive—it tracked the numbers being dialed, but it didn’t indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country.

Another argument that has been offered in defense of the metadata program is that, though the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the *collection* of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans’ private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans’ private papers and communications in the first place.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government’s surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. *See, e.g., United States v. U.S. District Court*, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to “exacting scrutiny” where they substantially burden First Amendment rights. *See, e.g., Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government’s legitimate goals. *See, e.g., Press Release, Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks*, June 7, 2013, <http://1.usa.gov/19Q1Ng1> (“As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.”).

c. Congress should amend Section 215 to prohibit suspicionless, dragnet collection of “tangible things”

As explained above, the metadata program is neither authorized by statute nor constitutional. As the government and FISC have apparently found to the contrary, however, the best way for Congress to protect Americans’ privacy is to narrow the statute’s scope. The ACLU urges Congress to amend Section 215 to provide 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. Several bipartisan bills now in the House and Senate should be considered by this Committee and Congress at large. The LIBERT-E Act, H.R. 2399, 113th Cong. (2013), sponsored by Rep. Conyers, Rep. Justin Amash, and forty others, would tighten the relevance requirement, mandating that the government supply “specific and articulable facts showing that there are reasonable grounds to believe that the tangible things sought are relevant and material,” and that the records sought “pertain only to an individual that is the subject of such investigation.” A bill sponsored by Senators Udall and Wyden, and another sponsored by Senator Leahy, would also tighten the required connection between the government’s demand for records and a foreign power or agent of a foreign power. Congress could also consider simply restoring some of the language that was deleted by the Patriot Act—in particular, the language that required the government to show “specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power.”

II. Electronic surveillance under Section 702 of FISA

The metadata program is only one part of the NSA’s domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans’ electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008.¹⁴ Under this program, labeled “PRISM” in NSA documents, the government collects emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.¹⁵ The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it involves surveillance of foreigners outside the United States.¹⁶ This is misleading. The PRISM program involves the collection of Americans’ communications, both international and domestic, and for reasons explained below, the program is unconstitutional.

¹⁴ Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, <http://wapo.st/1888aNr>.

¹⁵ While news reports have generally described PRISM as an NSA “program,” the publicly available documents leave open the possibility that PRISM is instead the name of the NSA database in which content collected from these providers is stored.

¹⁶ James R. Clapper, DNI Statement on Activities Authorized Under Section 702 of FISA, Office of the Director of National Intelligence (June 6, 2013), <http://1.usa.gov/13JJdBE>; *see also* James R. Clapper, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), <http://1.usa.gov/10YY4tp>.

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.¹⁷ While leaving FISA in place for purely domestic communications, the FISA Amendments Act revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans’ international communications. Under the FISA Amendments Act, the Attorney General and Director of National Intelligence (“DNI”) can “authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. 1881a(a). The government is prohibited from “intentionally target[ing] any person known at the time of the acquisition to be located in the United States,” *id.* § 1881a(b)(1), but an acquisition authorized under the FISA Amendments Act may nonetheless sweep up the international communications of U.S. citizens and residents.

Before authorizing surveillance under Section 702—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a “mass acquisition order”). *Id.* § 1881a(a), (c)(2). A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year.

To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court “a written certification and any supporting affidavit” attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, “targeting procedures” reasonably designed to ensure that the acquisition is “limited to targeting persons reasonably believed to be located outside the United States,” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” *Id.* § 1881a(g)(2)(A)(i).

The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, “minimization procedures” that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted “guidelines” to ensure compliance with the limitations set out in

¹⁷ A description of electronic surveillance prior to the passage of the FISA Amendments Act, including the warrantless wiretapping program authorized by President Bush beginning in 2001, is available in Mr. Jaffer’s earlier testimony to the House Judiciary Committee. *See The FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security*, H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (written testimony of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union Foundation), available at <http://bit.ly/14Q61Bs>.

§ 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that “a significant purpose of the acquisition is to obtain foreign intelligence information.” *Id.* § 1881a(g)(2)(A)(iii)–(vii).

Importantly, Section 702 does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government’s certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. *Id.* § 1881a(g)(4).

Nor does Section 702 place meaningful limits on the government’s retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt “minimization procedures,” *id.* § 1881a, that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons,” *id.* §§ 1801(h)(1), 1821(4)(A). The Act does not, however, prescribe specific minimization procedures. Moreover, the FISA Amendments Act specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is “foreign intelligence information.” *Id.* § 1881a(e) (referring to *id.* §§ 1801(h)(1), 1821(4)(A)). The phrase “foreign intelligence information” is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs. *Id.* § 1801(e).

As the FISA Court has itself acknowledged, its role in authorizing and supervising surveillance under the FISA Amendments Act is “narrowly circumscribed.”¹⁸ The judiciary’s traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FISA Amendments Act is to issue advisory opinions blessing in advance broad parameters and targeting procedures, under which the government is then free to conduct surveillance for up to one year. Under Section 702, the FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not closely supervise the implementation of the government’s targeting or minimization procedures. In short, the role that the FISA Court plays under the FISA Amendments Act bears no resemblance to the role that it has traditionally played under FISA.

¹⁸ *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), available at <http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf>.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.¹⁹ The statute's defects include:

- *Section 702 allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored.*

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

- *Section 702 allows the government to conduct intrusive surveillance without meaningful judicial oversight.*

Under Section 702, the government is authorized to conduct intrusive surveillance without meaningful judicial oversight. The FISA Court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is initiating any particular surveillance program. The FISA Court's role is limited to reviewing the government's "targeting" and "minimization"

¹⁹ The ACLU raised many of these defects in a constitutional challenge to the FISA Amendments Act filed just hours after the Act was signed into law in 2008. The case, *Amnesty v. Clapper*, was filed on behalf of a broad coalition of attorneys and human rights, labor, legal and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and email communications with individuals located outside the United States. In a 5-4 ruling handed down on February 26, 2013, the Supreme Court held that the ACLU's plaintiffs did not have standing to challenge the constitutionality of the Act because they could not show, at the outset, that their communications had been monitored by the government. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). The Court did not reach the merits of plaintiffs' constitutional challenge.

procedures. And even with respect to the procedures, the FISA court’s role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time.

- *Section 702 places no meaningful limits on the government’s retention and dissemination of information relating to U.S. citizens and residents.*

As a result of the FISA Amendments Act, thousands or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is “targeted” at people abroad. Yet the law fails to place any meaningful limitations on the government’s retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt “minimization” procedures—procedures that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.” However, these minimization procedures must accommodate the government’s need “to obtain, produce, and disseminate foreign intelligence information.” In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is “foreign intelligence information.” Because “foreign intelligence information” is defined broadly (as discussed below), this is an exception that swallows the rule.

- *Section 702 does not limit government surveillance to communications relating to terrorism.*

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather “foreign intelligence information.” There are multiple problems with this. First, under the new law the “foreign intelligence” requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase “foreign intelligence information” has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the “foreign affairs of the United States.” Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

b. The NSA’s “targeting” and “minimization” procedures do not mitigate the statute’s constitutional deficiencies

Since the FISA Amendments Act was enacted in 2008, the government’s principal defense of the law has been that “targeting” and “minimization” procedures supply sufficient protection for Americans’ privacy. Because the procedures were secret, the government’s assertion was impossible to evaluate. Now that the procedures have

been published, however,²⁰ it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans’ communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans’ international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans’ privacy are weak and riddled with exceptions.

- *The NSA’s procedures permit it to monitor Americans’ international communications in the course of surveillance targeted at foreigners abroad.*

While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans’ communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans’ international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans’ communications that contain “foreign intelligence information” or evidence of a crime can be retained forever, and even communications that don’t can be retained for as long as five years. Despite government officials’ claims to the contrary, the NSA is building a growing database of Americans’ international telephone calls and emails.

- *The NSA’s procedures allow the surveillance of Americans by failing to ensure that the its surveillance targets are in fact foreigners outside the United States.*

The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA’s procedures fail to ensure that its surveillance targets are *in fact* foreigners outside the United States. This is because the procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

- *The NSA’s procedures permit the government to conduct surveillance that has no real connection to the government’s foreign intelligence interests.*

One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the

²⁰ See Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, Guardian, June 20, 2013, <http://bit.ly/105qb9B>.

FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather “foreign intelligence information.” As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even “the foreign affairs of the United States.” The NSA’s procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner’s address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA’s surveillance.

- *The NSA’s procedures permit the NSA to collect international communications, including Americans’ international communications, in bulk.*

On its face, Section 702 permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the FISA Amendments Act made clear that this was one of its principal purposes, and unsurprisingly, the procedures give effect to that design. While they require the government to identify a “target” outside the country, once the target has been identified the procedures permit the NSA to sweep up the communications of any foreigner who may be communicating “about” the target. The Procedures contemplate that the NSA will do this by “employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas,” by “target[ing] Internet links that terminate in a foreign country,” or by identifying “the country code of the telephone number.” However the NSA does it, the result is the same: millions of communications may be swept up, Americans’ international communications among them.

- *The NSA’s procedures allow the NSA to retain even purely domestic communications.*

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic.²¹ The Act should require the NSA to purge these communications from its databases, but it does not. The procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly.

²¹ Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in “significant and systemic” overcollection of such domestic communications. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, April 15, 2009, <http://nyti.ms/16AIq5O>.

- *The NSA's procedures allow the government to collect and retain communications protected by the attorney-client privilege.*

The procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

c. Congress should amend Section 702 to prohibit suspicionless, dragnet collection of Americans' communications

For the reasons discussed above, the ACLU believes that the FISA Amendments Act is unconstitutional on its face. There are many ways, however, that Congress could provide meaningful protection for privacy while preserving the statute's broad outline. One bill introduced by Senator Wyden during the reauthorization debate last fall would have prohibited the government from searching through information collected under the FISA Amendments Act for the communications of specific, known U.S. persons. Bills submitted during the debate leading up to the passage of the FISA Amendments Act in 2008 would have banned dragnet collection in the first instance or required the government to return to the FISC before searching communications obtained through the FISA Amendments Act for information about U.S. persons. Congress should examine these proposals again and make amendments to the Act that would provide greater protection for individual privacy and mitigate the chilling effect on rights protected by the First Amendment.

III. Excessive secrecy surrounds the government's use of FISA authorities

Amendments to FISA 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 two months than in the last several decades combined. While the Judiciary and Intelligence Committees have received some information in classified format, only members of the Senate Select Committee on Intelligence, party leadership, and a handful of Judiciary Committee members have staff with clearance high enough to access the information and advise their principals. Although the Inspectors General and others file regular reports with the Committees of jurisdiction, these reports do not include even basic information such how many Americans' communications are swept up in these programs, or how and when Americans' information is accessed and used.

Nor does the public have access to the FISC decisions that assess the meaning, scope, and constitutionality of the surveillance laws. 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 encompass millions of individual records. 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. 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.²² 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.²³ Executive officials testified before Congress several years ago that declassification review was already underway,²⁴ and President Obama directed the DNI to revisit that process in the last few weeks. If the administration refuses to release these opinions, Congress should consider legislation compelling their release.

Congress should also require the release of information about the type and volume of information that is obtained under dragnet surveillance programs. The leaked Verizon order confirms that the government is using Section 215 to collect telephony metadata about every phone call made by VBNS subscribers in the United States. That the government is using Section 215 for this purpose raises the question of what other “tangible things” the government may be collecting through similar dragnets. For reasons discussed above, the ACLU believes that these dragnets are unauthorized by the statute as well as unconstitutional. Whatever their legality, however, the public has a right to know, at least in general terms, what kinds of information the government is collecting about innocent Americans, and on what scale.

IV. National Security Letters

The ACLU has a number of serious concerns with the national security letter (NSL) statutes. In this testimony, we focus on only two. The first is that the NSL statutes allow executive agencies (usually the FBI) to obtain records about people who are not known or even suspected to have done anything wrong. They allow the

²² See, e.g., Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, <http://wapo.st/170VVSu>.

²³ See Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, <http://nyti.ms/12beiA3>.

²⁴ Prehearing Questions for Lisa O. Monaco Upon Her Nomination to be the Assistant Attorney General for National Security, Sen. Select Comm. on Intelligence, 112th Cong., at 12-13, available at <http://bit.ly/10V5Ion>.

government to collect information, sometimes very sensitive information, not just about suspected terrorists and spies but about innocent people as well. The second concern is that the NSL statutes allow government agencies (again, usually the FBI) to prohibit NSL recipients from disclosing that the government sought or obtained information from them. This authority to impose non-disclosure orders—gag orders—is not subject to meaningful judicial review. Indeed, as discussed below, the review contemplated by the NSL statutes is no more than cosmetic.²⁵

a. The NSL statutes invest the FBI with broad authority to collect constitutionally protected information pertaining to innocent people

Several different statutes give executive agencies the power to issue NSLs.²⁶ Most NSLs, however, are issued by the FBI under 18 U.S.C. § 2709,²⁷ which was originally

²⁵ The ACLU has a number of other concerns with the NSL statutes. First, the statutes do not significantly limit the retention and dissemination of NSL-derived information. *See, e.g.*, 18 U.S.C. § 2709(d) (delegating to the Attorney General the task of determining when, and for what purposes, NSL-derived information can be disseminated). Second, the statutes provide that courts that hear challenges to gag orders must review the government’s submissions *ex parte* and *in camera* “upon request of the government”; this language could be construed to foreclose independent consideration by the court of the constitutional ramifications of denying the NSL recipient access to the evidence that is said to support a gag order. 18 U.S.C. § 3511(e). *But see Doe v. Gonzales*, 500 F. Supp. 2d 379, 423-24 (S.D.N.Y. 2007) (construing statute more narrowly). Third, the statutes provide that courts that hear challenges to gag orders must seal documents and close hearings “to the extent necessary to prevent an unauthorized disclosure of a request for records”; this language could be construed to divest the courts of their constitutional responsibility to decide whether documents should be sealed or hearings should be closed. 18 U.S.C. § 3511(d). *But see Doe*, 500 F. Supp. 2d at 423-24 (finding that statute “in no way displaces the role of the court in determining, in each instance, the extent to which documents need to be sealed or proceedings closed and does not permit the scope of such a decision to be made unilaterally by the government”).

²⁶ For instance, under 12 U.S.C. § 3414(a)(5)(A), the FBI is authorized to compel “financial institutions” to disclose customer financial records. The phrase “financial institutions” is defined very broadly, and encompasses banks, credit unions, thrift institutions, investment banks, pawnbrokers, travel agencies, real estate companies, and casinos. 12 U.S.C. § 3414(d) (adopting definitions in 31 U.S.C. § 5312). Under 15 U.S.C. § 1681u, the FBI is authorized to compel consumer reporting agencies to disclose “the names and addresses of all financial institutions . . . at which a consumer maintains or has maintained an account,” as well as “identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment.” Under 15 U.S.C. § 1681v, executive agencies authorized to conduct intelligence or counterintelligence investigations can compel consumer reporting agencies to disclose “a consumer report of a consumer and all other information in a consumer’s file.” Still another statute, 50 U.S.C. § 436 empowers “any authorized investigative agency” to compel financial institutions and consumer reporting agencies to disclose records about agency employees.

enacted in 1986 as part of the Electronic Communications Privacy Act (“ECPA”).²⁸ Since its enactment, the ECPA NSL statute has been amended several times. In its current incarnation, it authorizes the FBI to issue NSLs compelling “electronic communication service provider[s]” to disclose “subscriber information,” “toll billing records information,” and “electronic communication transactional records.”²⁹ An “electronic communication service” is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”³⁰

Because most NSLs are issued under ECPA, this testimony focuses on that statute. All of the NSL statutes, however, suffer from similar flaws.

The ECPA NSL statute implicates a broad array of information, some of it extremely sensitive. Under the statute, an Internet service provider can be compelled to disclose a subscriber’s name, address, telephone number, account name, e-mail address, and credit card and billing information. It can be compelled to disclose the identities of individuals who have visited a particular website, a list of websites visited by a particular individual, a list of e-mail addresses with which a particular individual has corresponded, or the e-mail address and identity of a person who has posted anonymous speech on a political website. As the *Library Connection* case shows, the ECPA NSL statute can also be used to compel the disclosure of library patron records.³¹ Clearly, all of this information is sensitive. Some of it is protected by the First Amendment.³²

Because NSLs can reach information that is sensitive, Congress originally imposed stringent restrictions on their use. As enacted in 1986, the ECPA NSL statute permitted the FBI to issue an NSL only if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent.³³ Since 1986, however, the reach of the law has been extended dramatically. In 1993, Congress relaxed the individualized suspicion requirement, authorizing the FBI to issue an NSL if it could certify that (i)

²⁷ Dep’t of Justice, Office of Inspector General, *A Review of the FBI’s Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, (March 2008), (hereinafter “2008 OIG Report”), at 107, available at <http://1.usa.gov/17PO5aI>.

²⁸ See Pub L. No. 99-508, Title II, § 201(a), 100 Stat. 1848 (Oct. 21, 1986) (codified as amended at 18 U.S.C. § 2510 *et seq.*)

²⁹ 18 U.S.C. §§ 2709(a) & (b)(1).

³⁰ *Id.* § 2510(15).

³¹ See *Library Connection v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

³² Cf. *Mcintyre v. Ohio Elections Comm.*, 514 U.S. 334, 341-42 (1995) (“[A]n author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”); *Talley v. California*, 362 U.S. 60, 64 (1960) (“Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names.”).

³³ 18 U.S.C. § 2709 (1988).

the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that *either* (a) the subject of the NSL was a foreign power or foreign agent, *or* (b) the subject had communicated with a person engaged in international terrorism or with a foreign agent or power “under circumstances giving reason to believe that the communication concerned international terrorism.”³⁴ In 2001, Congress removed the individualized suspicion requirement altogether and also extended the FBI’s authority to issue NSLs in terrorism investigations. In its current form, the NSL statute permits the FBI to issue NSLs upon a certification that the records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”³⁵

The relaxation and then removal of the individualized suspicion requirement has resulted in an exponential increase in the number of NSLs issued each year. According to an audit conducted by the Justice Department’s OIG, the FBI’s internal database showed that the FBI issued 8,500 NSL requests in 2000, the year before the Patriot Act eliminated the individualized suspicion requirement.³⁶ By comparison, the FBI issued 39,346 NSL requests in 2003; 56,507 in 2004; 47,221 in 2005; and 49,425 in 2006.³⁷ These numbers, though high, substantially understate the number of NSL requests actually issued, because the FBI has not kept accurate records of its use of NSLs. The OIG sampled 77 FBI case files and found 22 percent more NSL requests in the case files than were recorded in the FBI’s NSL database.³⁸ Since 2007, the public has had only partial information about the FBI’s use of its NSL authorities. Neither the FBI nor the Department of Justice annually publish the total number of NSLs; instead, the Department of Justice reports statistics that omit NSLs concerning non-U.S. persons and NSLs strictly for subscriber information—making a true comparison impossible. These partial statistics indicate that the FBI issued 16,804 NSLs seeking information concerning U.S. persons in 2007; 24,744 in 2008; 14,788 in 2009; 24,287 in 2010; 16,511 in 2011; and 15,229 in 2012.³⁹

The statistics and other public information make clear that the executive branch is now using NSLs not only to investigate people who are known or suspected to present threats but also—and indeed principally—to collect information about innocent

³⁴ Pub. L. 103-142, 107 Stat. 1491 (Nov. 17, 1993).

³⁵ 18 U.S.C. § 2709(a) & (b)(1) (2006).

³⁶ See Dep’t of Justice, Office of Inspector General, *A Review of the Federal Bureau of Investigation’s Use of National Security Letters* (March 2007), (hereinafter “2007 OIG Report”), at xvi, available at <http://bit.ly/16woHoY>.

³⁷ See *id.* at xix; 2008 OIG Report at 9.

³⁸ 2007 OIG Report at 32.

³⁹ See Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Court Orders 1979-2012*, May 4, 2012, <http://bit.ly/cnSWP5> (compiling NSL statistics); Kim Zetter, *Federal Judge Finds National Security Letters Unconstitutional, Bans Them*, *Wired*, Mar. 15, 2013, <http://bit.ly/YzEtgG> (same).

people.⁴⁰ News reports indicate that the FBI has used NSLs “to obtain data not only on individuals it saw as targets but also details on their ‘community of interest’—the network of people that the target was in contact with.”⁴¹ Some of the FBI’s investigations appear to be nothing more than fishing expeditions. In two cases brought the ACLU, the FBI has abandoned its demand for information after the NSL recipient filed suit; that is, the FBI withdrew the NSL rather than try to defend the NSL to a judge.⁴² The agency’s willingness to abandon NSLs that are challenged in court raises obvious questions about the agency’s need for the information in the first place.

The ACLU believes that the current NSL statutes do not appropriately safeguard the privacy of innocent people. Congress should narrow the NSL authorities that allow the FBI to demand information about individuals who are not the targets of any investigation.

b. The NSL statutes allow the FBI to impose gag orders without meaningful judicial review

A second problem with the NSL statutes is that they empower executive agencies to impose gag orders that are not subject to meaningful judicial review.⁴³ Until 2006, the ECPA NSL statute categorically prohibited NSL recipients from disclosing to any person that the FBI had sought or obtained information from them.⁴⁴ Congress amended the statute, however, after a federal district court found it unconstitutional.⁴⁵ Unfortunately, the amendments made in 2006, while addressing some problems with the statute, made the gag provisions even more oppressive. The new statute permits the FBI to decide on a case-by-case basis whether to impose gag orders on NSL recipients but strictly confines the ability of NSL recipients to challenge such orders in court.

As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on

⁴⁰ The statistics also make clear that the FBI is increasingly using NSLs to seek information about U.S. persons. The percentage of NSL requests generated from investigations of U.S. persons increased from approximately 39 percent of NSL requests in 2003 to approximately 57 percent in 2006. 2008 OIG Report at 9.

⁴¹ Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. Times, Sept. 9, 2007; see also Barton Gellman, *The FBI’s Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, Wash. Post, Nov. 6, 2005 (reporting that the FBI apparently used NSLs to collect information about “close to a million” people who had visited Las Vegas).

⁴² See generally *Doe v. Mukasey*, 549 F.3d 861 (2d. Cir. 2008); *Library Connection v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

⁴³ All of the NSL statutes authorize the imposition of such gag orders.

⁴⁴ 18 U.S.C. § 2709 (2005).

⁴⁵ *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

any person or entity served with an NSL.⁴⁶ To impose such an order, the Director or his designee must “certify” that, absent the non-disclosure obligation, “there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person.”⁴⁷ If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from “disclos[ing] to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the [FBI] has sought or obtained access to information or records under [the NSL statute].”⁴⁸ Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a “certification” that the gag is necessary, the certification is not examined by anyone outside the executive branch. No judge considers, before the gag order is imposed, whether secrecy is necessary or whether the gag order is narrowly tailored.

The gag provisions permit the recipient of an NSL to petition a court “for an order modifying or setting aside a nondisclosure requirement.”⁴⁹ However, in the case of a petition filed “within one year of the request for records,” the reviewing court may modify or set aside the nondisclosure requirement only if it finds that there is “no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.”⁵⁰ Moreover, if a designated senior government official “certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations,” the certification must be “treated as conclusive unless the court finds that the certification was made in bad faith.”⁵¹

In December 2008, the Second Circuit issued a decision construing the NSL statute (1) to permit a nondisclosure requirement only when senior FBI officials certify that disclosure may result in an enumerated harm that is related to “an authorized investigation to protect against international terrorism or clandestine intelligence

⁴⁶ 18 U.S.C. § 2709(c).

⁴⁷ *Id.* § 2709(c)(1).

⁴⁸ *Id.*

⁴⁹ *Id.* § 3511(b)(1).

⁵⁰ *Id.* § 3511(b)(2).

⁵¹ *Id.* In the case of a petition filed under § 3511(b)(1) “one year or more after the request for records,” the FBI Director or his designee must either terminate the non-disclosure obligation within 90 days or recertify that disclosure may result in one of the enumerated harms. *Id.* § 3511(b)(3). If the FBI recertifies that disclosure may be harmful, however, the reviewing court is required to apply the same extraordinarily deferential standard it is required to apply to petitions filed within one year. *Id.* If the recertification is made by a designated senior official, the certification must be “treated as conclusive unless the court finds that the recertification was made in bad faith.” *Id.*

activities”; (2) to place on the government the burden of showing that a good reason exists to expect that disclosure of receipt of an NSL will risk an enumerated harm; and (3) to require the government, in attempting to satisfy that burden, to adequately demonstrate that disclosure in a particular case may result in an enumerated harm.⁵² The court also invalidated the subsection of the NSL statute that directs the courts to treat as conclusive executive officials’ certifications that disclosure of information may endanger the national security of the United States or interfere with diplomatic relations.⁵³

In addition, the Second Circuit ruled that the NSL statute is unconstitutional to the extent that it imposes a non-disclosure requirement on NSL recipients without placing on the government the burden of initiating judicial review of that requirement.⁵⁴ The court held that this deficiency, however, could be addressed by the adoption of a “reciprocal notice” policy.⁵⁵ Under this policy, the FBI must inform NSL recipients of their right to challenge gag orders. If a recipient indicates its intent to do so, the FBI must initiate court proceedings to establish—before a judge—that the gag order is necessary and consistent with the First Amendment.⁵⁶

Consistent with these judicial rulings, the ACLU supports congressional efforts to ensure that “gag orders” associated with national security letters and other surveillance directives are limited in scope, limited in duration, and imposed only when necessary.

V. Summary of recommendations

For the reasons above, Congress should amend relevant provisions of FISA to prohibit suspicionless, “dragnet” monitoring or tracking of Americans’ communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA’s so-called “business records” provision, and to the national security letter authorities.

Congress should also end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information

⁵² *Doe v. Mukasey*, 549 F.3d 861, 883 (2d. Cir. 2008).

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *See id.*

⁵⁶ A district court in the Northern District of California recently issued a similar decision, finding that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and that 18 U.S.C. § 3511(b)(2) and (b)(3) violate the First Amendment and separation of powers principles. *In re Nat'l Sec. Letter*, No. C 11-02173 SI, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013). The court enjoined the government from issuing NSLs under section 2709 or from enforcing the nondisclosure provision in that or any other case. *Id.*

about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Finally, Congress should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.