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

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

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As originally enacted in 1998, FISA's business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international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 concemi ciq

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.

P.e3[urposesnseri oc 0lsdiett9-2(he)422(y)20i(y)20i(y)0enshe

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

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.[19]

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 constitutionaohe(i)-6()-2(d-1(u)-7.9(t)-1(i)-2(l)-10i)-0 ti1(i)-6s2(

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 f

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 discl6(i)6.3(ons)4e mpplo.9(t)- nedd resstr todne(i)-2.6(d)12.9(eew)6.6(h)12.9(t)-2.6(h)2(e)11.2(r)-1.9 dhoems(h)2(o)129-1.6(li)-2.6(d)2( )10.9()pled(o)12 (i)-4.6(s)-2.3paes ther()-3.9olte (f)-4(t)-4.6((e)-172(c)-1.6(g)10.8(r()-3.9(t)-4.6((i)-4.6n( )-11dea)9.2(t)-4.6ea)9.2r()-3

enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA").[28]

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*

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.

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.

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