Nos. 13-15957 and 13-16731

UNDER SEAL

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNDER SEAL,

Petitioner-Appellee (No. 13-15957),

Petitioner-Appellant (No. 13-16731),

v.

ERIC H. HOLDER, JR., ATTORNEY GENERAL; UNITED STATES DEPARTMENT OF JUSTICE; and FEDERAL BUREAU OF INVESTIGATION,

Respondents-Appellants (No. 13-15957),

Respondents-Appellees (No. 13-16731).

On Appeal from the United States District Court
for the Northern District of California
Case No's. ll-cv-2173 SI & 13-mc-80089 SI
Honorable Susan Illston, District Court Judge

BRIEF *AMICI CURIAE* OF EXPERTS IN COMPUTER SCIENCE AND DATA SCIENCE IN SUPPORT OF APPELLANTS

Phillip R. Malone, CA Bar No. 163969
Michael Chen, CA Bar Student Cert. No. 34469
Emily Warren, CA Bar Student Cert. No. 34473
Rachel Yu, CA Bar Student Cert. No. 34474
JUELSGAARD INTELLECTUAL
PROPERTY & INNOVATION CLINIC
Mills Legal Clinic at Stanford Law School
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 725-6369

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, each of the amici listed in Exhibit A states that he or she is not a corporation that issues stock and has no parent corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Agency Publications, Reports and Opinions

U.S. Department of Justice Office of the Inspector General, *A Review of the FBI's Use of National Security Letters* 36 (2007) .... passim

U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 75 (2010**)** 11, 14, 15

Magazines, Newspapers and Blogs

Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, Wired (June 16, 2013 9:30 AM), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again 16, 27

The Economist, *Mining Social Networks: Untangling the Social Web*, (Sept. 2, 2010), http://www.economist.com/node/16910031 30

Dan Eggen, *Text 'Give' to Obama: President's Campaign Launches Cellphone Donation Drive*, Wash. Post (Aug. 23, 2012), http://www.washingtonpost.com/politics/text-give-to-obama-presidents-campaign-launches-cellphone-donation-drive/2012/08/23/5459649a-ecc4-11e1-9ddc-340d5efb1e9c_story.html 22

Barton Gellman, *NSA Statements to the Post*, Wash. Post, Aug 15, 2013, http://wapo.st/1ixchnm 18

Hal Hodson, *How Metadata Brought Down CIA Boss David Petraeus*, NewsScientist (Nov. 16, 2013 1:59 PM), http://www.newscientist.com/article/dn22511-how-metadata-brought-down-cia-boss-david-petraeus.html. 29

Mail & Guardian, *Story Tip-Offs*, http://mg.co.za/page/story-tip-offs 19

Jane Mayer, *What's the Matter With Metadata?*, New Yorker (June 6, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html 6, 16, 28, 32

New York Times, *Contact the Public Editor*, NYTimes.com, http://publiceditor.blogs.nytimes.com/contact-the-public-editor/ 18

Rebecca J. Rosen, *Stanford Researchers: It is Trivially Easy to Match Metadata to Real People*, The Atlantic (Dec. 24, 2013 1:50 PM), http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-real-people/282642 17

Internet Sources

Griffin Boyce and Brian Duggan, *The Real Reason Why Metadata Collecting Is Dangerous*, New America Foundation (June 17, 2013 4:54 PM), http://inthetank.newamerica.net/blog/2013/06/real-reason-why-metadata-collecting-dangerous 21

Childhelp, *Childhelp National Child Abuse Hotline*, http://childhelp.org/pages/hotline-hom**e** 18

Charles Duhigg, *How Companies Learn Your Secrets* (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp 33

Electronic Privacy Information Center, *National Security Letters*, http://epic.org/privacy/nsl/ 4

GLBT National Help Center, *Gay, Lesbian, Bisexual and Transgender National Hotline*, http://www.glbtnationalhelpcenter.org/hotline.................................... 18

IBM, *Analyst's Notebook*, http://www-03.ibm.com/software/products/en/analysts-notebook-family... 26

IBM, *Environmental Investigation Agency: IBM i2 Solution Help Combat the Illegal Tiger Trade* (2012) 26

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA Three-Hop, Web Policy* (Dec. 9, 2013), http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/ 13, 14, 18

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, Web Policy (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata 18, 20, 30, 33

MIT Media Lab, *Immersion*, https://immersion.media.mit.edu 25

STATEMENT OF INTEREST[1]

The amici listed in Exhibit A are professors of computer and data science at the country's leading educational institutions, and expert computer scientists, specializing in data and computer security, data analysis, cryptography, and privacy-enhancing technologies. Collectively, amici's research has significantly shaped the development of modern communications technology and data analysis techniques.

Amici offer this brief to emphasize for the Court the extraordinary sensitivity of the data that can be gathered through National Security Letters, notwithstanding its legal categorization as "non-content" data, and the personal, intimate, family, associational, political, health and medical, financial and other information that can be revealed by such data. Amici's expertise and familiarity with data analysis and communications technology offer a particularly informed perspective on the issues confronted in this case. The list of amici attached as Exhibit A includes a brief biography of each.

[1] Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for the amici and their counsel, has authored this brief in whole or in part, or contributed money towards its preparation. All parties have consented to the filing of this brief.

INTRODUCTION

Under the Electronic Communications Privacy Act (ECPA) National Security Letter (NSL) provisions of 18 U.S.C. § 2709(a)-(b), the FBI easily surveils ordinary Americans. NSLs can be obtained merely with the signature of any special agent in charge of any FBI field office, and there is no need for suspicion of wrongdoing. The data seized need only be considered "relevant" to a counterintelligence or counterterrorism investigation, and the person whose data are taken need not be in any way considered a suspect or target.

With no affirmative judicial approval of the NSL process and a low "relevance" standard that encompasses potentially millions of people per single NSL request, the government unreasonably invades the privacy of potentially every American. Through the hundreds of thousands of NSLs have already been issued, the FBI may have collected data on almost every person in the United States. And once collected, NSL data typically is stored in massive databases and can be accessed broadly—not just by top FBI officials.

While the government asserts that the information obtained by NSLs does not include the actual content of a communication, NSL information can nonetheless be incredibly revealing. Through even a relatively naïve analysis of information obtained by an NSL, the FBI can gather extensive information about a person's political contributions, intimate relationships, religious and community affiliations, medical conditions, financial records, and much more. The rise of "Big Data" and sophisticated analytical tools only compound this danger, giving the government unprecedented access to the sensitive information of American citizens.

ARGUMENT

I. NATIONAL SECURITY LETTERS GIVE THE FBI EXTENSIVE AUTHORITY TO SURVEIL ORDINARY AMERICANS

The current version of the substantive ECPA NSL provisions, codified at 18 U.S.C. § 2709(a)-(b), authorizes dozens of FBI agents around the country to issue national security letters without meaningful, affirmative judicial checks. These letters can compel the disclosure of all non-content data connected with phone calls, text messages, and emails—essentially, everything except for actual recordings and copies of the messages themselves. Agents can collect data pertaining to any entity that may be "relevant" to an investigation and have issued hundreds of thousands of requests for such data. Moreover, since "relevant" may be defined however the Bureau wishes, the standard offers it great discretion to collect data on nearly any American. Once collected, these data are stored in databases accessible by tens of thousands of people and are used to produce intelligence reports for dozens of agencies. Predictably but unfortunately, there is substantial evidence that the FBI has abused these expansive authorities.[2]

Though the type of data that the FBI may demand under § 2709(a)-(b) has not been fully litigated, public and private actors have interpreted the statute's key terms (subscriber information, toll billing records, and electronic transaction communication records) to include all of the following kinds of information[3]:

1. All phone numbers, email addresses, and screen names associated with an individual;
2. The individual associated with any phone number, email address, or screen name;
3. All mailing address, phone number, and billing information associated with an individual and the length of time an individual has subscribed to a service;

[2] The President's Review Group on Intelligence and Communications Technologies, *Final Report* 90 (2013).

[3] *See* Daniel Koffsky, *Requests for Information Under the Electronic Communications Privacy Act*, *in* 32 *Opinions of the Office of Legal Counsel* 2, 5 (2008); President's Review Group, *supra* note 2, at 90; Chris Soghoian, *US Surveillance Law May Poorly Protect New Text Message Services*, American Civil Liberties Union (Jan. 8, 2013, 9:44 AM), https://www.aclu.org/blog/national-security-technology-and-liberty/us-surveillance-law-may-poorly-protect-new-text; *National Security Letters*, Electronic Privacy Information Center (last visited Mar. 13, 2014, 4:35 PM), http://epic.org/privacy/nsl/; Decl. in Supp. of Pet. to Set Aside National Security Letter and Nondisclosure Requirement In re Matter of National Security Letters 5, 11, Mar. 14, 2013, ECF 13-1165; Declaration of Under Seal in Support of Petition to Set Aside National Security Letters and Nondisclosure Requirements Imposed in Connection Therewith, In re Matter of National Security Letters, No. CV-131165 (LB) (N.D. Cal. Mar. 14, 2013), Exhibit A.

4. All IP addresses from which a user has logged into an email account and the timeframes during which each was used;

5. A complete list of all phone calls ever associated with a phone number including, for each call, whether it was outgoing or incoming, the phone number contacted, how long the call lasted, and when it was made;

6. A complete list of all text messages ever associated with a phone number including, for each message, whether it was sent or received, the phone number contacted, and when it was sent; and

7. A complete list of all emails ever associated with a screen name, including, for each email, whether it was sent or received, the email address contacted, other email addresses that were copied, the size of the message, and when it was sent.

These NSL-obtained data, colloquially referred to as "metadata," generally are considered "non-content" under the definition of "contents" in 18 U.S.C. § 2510(8).[4] But the data demanded by NSLs, while legally non-content data, are in fact profoundly meaningful. As discussed further in section II, information from NSLs can expose details ranging from political beliefs and affiliations to the structure of grassroots organizations to reproductive choices to medical conditions

[4] *See* Decl. Set Aside 9, 15, ECF 13-1165.

and more. As former Google Senior Privacy Analyst and privacy/surveillance author Susan Landau stated in an interview: "The public doesn't understand . . . It's much more intrusive than content." The government gains expansive private information by studying "who you call, and who they call. If you can track that, you know exactly what is happening—you don't need the content."[5]

The ECPA NSL substantive provisions authorize the FBI to demand not only many kinds of substantive data, but also data relating to nearly any American. In contrast to older versions of the statute, the current "very low" relevance standard authorizes the FBI to demand data on individuals who are not investigation targets and eliminates any requirement to record particularized facts justifying why an individual's data are relevant.[6] The only limits on what can be deemed "relevant" are that investigations to which data are relevant must be authorized and that the FBI must be able to justify—almost always to itself rather than a court—that the request is motivated by more than a First Amendment-protected activity alone. § 2709(b). The administration has recently argued that "'relevance' is a broad standard that permits discovery of large volumes of data in

[5] Jane Mayer, *What's the Matter With Metadata?*, New Yorker (June 6, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html (quoting interview with Landau) (internal quotation marks omitted).

[6] President's Review Group, *supra* note 2, at 90.

circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated."[7]

The substantial lack of affirmative judicial approval in determining what is sufficiently relevant contrasts starkly with other provisions of ECPA and Section 215 of the Patriot Act, statutes governing the collection of similar data but requiring a court order or subpoena. 18 U.S.C. § 2703(c)(1); 50 U.S.C. § 1861. This contrast drove the President's Review Group on Intelligence and Communications Technologies to observe that it was "unable to identify a principled reason why NSLs should be issued by FBI officials" rather than by a court.[8]

In practice, the expansive relevance standard has facilitated the use of NSLs in "approximately one-third of all counterterrorism, counterintelligence, and cyber investigations" during 2006.[9] When the FBI issues these NSLs, they include one or more requests for either "toll billing records" (telephony and text-message data), "electronic communications transactional records" (email data), or subscriber

[7] *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act* 2 (Aug. 9, 2013).

[8] President's Review Group, *supra* note 2, at 93.

[9] U.S. Department of Justice Office of the Inspector General, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* 109 (2008).

information (names and other identifying data associated with an account). A response to any individual request will thus include hundreds to hundreds of thousands of individual observations—including, for example, a 26-minute call from a subscriber to a phone number the FBI has identified as belonging to his mother, at 10:35 PM six months ago.

As shown in Table I, even the limited unclassified information available indicates that the FBI has made over 300,000 NSL requests in the past decade, the "overwhelming majority" of which have been for ECPA NSL data.[10] Of these, the FBI has made almost 150,000 requests for non-subscriber information of U.S. persons, mostly toll billing or electronic transaction records, and over 165,000 requests (with estimates above 340,000)[11] for information about U.S. persons, including subscriber information. Including requests for information about non-

[10] U.S. Department of Justice Office of the Inspector General, *A Review of the FBI's Use of National Security Letters* 36 (2007); *accord* OIG (2008), *supra* note 9, at 60, 107; President's Review Group, *supra* note 2, at 90.

[11] The only public information about requests for subscriber-only information about U.S. persons are that such requests made up 56% of total requests for U.S. persons' information in 2006, Table I, and the majority of requests in 2012, President's Review Group, *supra* note 2, at 90. If subscriber-only requests for data about U.S. persons comprised 56% of all requests for data about U.S. persons in all years, as it did in 2006, then the FBI would have made 342,868 total requests for U.S. persons' data.

Americans, the FBI made over 304,000 requests (with estimates above 570,000).[12] Collectively, these requests have generated databases with millions of observations of phone calls, emails, and text messages.[13]

[12] To estimate total requests for persons of any nationality in years other than 2006, we assume that the proportion of total requests that were requests for U.S. persons' data in these years equaled that in 2006, 60%, OIG (2008), *supra* note 9, at 108. Combined with the data for 2006, this yields an estimate of 571,446 total requests.

[13] Though the precise size of the database is not public, it is possible to estimate. Table I shows that the FBI made 149,663 total requests for non-subscriber information pertaining to U.S. citizens. If the FBI made 228,579 requests for information about non-U.S. persons, *see* notes 2-3, *supra* (estimating 571,446 total requests of which 342,868 pertained to U.S. citizens), and 44% of these were for toll billing records or electronic transaction communications records, *see* Table I row 2006 (showing this proportion for U.S. persons' requests), then it made 99,775 requests for non-subscriber information pertaining to non-U.S. persons, yielding a total database of such information that would include 249,437 requests (149,663 + 99,775). If each request yielded an average of 1,000 observations then the database would have nearly 250 million observations.

TABLE I: NSL REQUESTS FROM 2003 TO 2012, BY REQUEST TYPE

Year	**For U.S. persons' non-subscriber information (mostly toll billing or electronic communications transactional records)**[14]	**For any U.S. persons' data, including subscriber information**[15]	**For non-U.S. persons' data of any type**[16]	**Total requests**[17]
2003	6,519	More than 6,519	Classified	39,346
2004	8,943	More than 8,943	Classified	56,507
2005	9,254	More than 9,254	Classified	47,221
2006	12,583	28,827	19,279	49,425
2007	16,804	More than 16,804	Classified	More than 16,804
2008	24,744	More than 24,744	Classified	More than 24,744
2009	14,788	More than 14,788	Classified	More than 14,788
2010	24,287	More than 24,287	Classified	More than 24,287
2011	16,511	More than 16,511	Classified	More than 16,511
2012	15,229	More than 15,229	Classified	More than 15,229
Total known	**149,662**	**More than 165,906**	**Classified**	**More than 304,862**
Estimated Totals[18]	**149,662**	**342,868**	**99,775**	**571,446**

The full set of individuals whose data the FBI could demand under the relevance standard likely comprises all Americans. Since the FBI uses NSLs to determine a target's "family members, associates, living arrangements, and contacts," an authorized agent may deem data pertaining to individuals far

[14] Data in this column for from 2003-2005 from 2007 OIG Report, *supra* note 9, at xx. Data for 2006-2012 from annual reports the FBI has made to Congress, *available at* https://www.fas.org/irp/agency/doj/fisa/#rept. Note that these data may include some additional requests for other types of NSL information authorized by statutes other than ECPA (see 2007 OIG Report at xx).

[15] Data in this column from 2008 OIG Report, *supra* note 9, at 108.

[16] Data in this column from 2008 OIG Report, *supra* note 9, at 108.

[17] Data in this column derived from OIG 2007 Report, *supra* note 9, at xvi, xix; OIG 2008 Report at 110. These figures include requests that the FBI failed to report to Congress but that the OIG found in its review of the FBI-OGC NSL database as of May 2006, May 2007.

[18] *See* notes 2-4, *supra*.

removed from an investigation target to be "relevant."[19] A 2010 OIG investigation found that the FBI has regarded the personal data of any individual within an investigation target's "community of interest" or "calling circle" to be relevant, though the definitions of these terms were redacted.[20] Revealingly, the 2007 OIG investigation could not find FBI guidance discouraging case agents from using NSLs to access the data of individuals "two or three steps removed" from an investigation target.[21] This is the same standard used by the NSA and means, for example, that if investigation target Adam called Betsy (step one), who emailed Caleb (step two), who texted Dwayne (step three), then Dwayne's data would be deemed "relevant" to the investigation of Adam.

Though three steps may seem trivial, some estimate that "[i]f the average person called 40 unique people, a three hop [or step] analysis would allow the government to mine the records of 2.5 million Americans when investigating one suspected terrorist."[22] Others have estimated that the FBI could deem "the phone

[19] OIG (2007), *supra* note 10, at xxiv.

[20] U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 75 (2010).

[21] OIG (2007), *supra* note 10, at 109.

[22] Pete Yost & Matt Apuzzo, *With 3 'Hops,' NSA Gets Millions of Phone Records*, Associated Press (Jul. 31, 2013 6:19 PM), http://bigstory.ap.org/article/senate-panel-looking-limits-surveillance.

records of a sizable proportion of the United States population" to be relevant to a single terrorism investigation under a three-steps rule.[23] Moreover, both of these estimates consider only steps among phone calls; the addition of texts and emails expands the circle of relevant individuals and businesses exponentially. Thus, with millions of Americans' data considered relevant to any investigation and thousands of investigations each year, a three-steps definition of relevance is a largely empty check on FBI discretion.

According to the 2007 OIG report, once the FBI receives data responding to an NSL request, that data is typically uploaded to a number of different databases. Electronic communications transactional records are uploaded to the Automated Case Support System, the FBI's centralized case management system. Roughly 34,000 individuals had access to this system in 2005. Toll billing records are uploaded to the Telephone Applications database. Some 19,000 individuals had access to this database in 2006.[24] In addition, information from NSL demands is stored separately in a number of classified databases about which no information

[23] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA Three-Hop, Web Policy* (Dec. 9, 2013), http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/.

[24] OIG (2007), *supra* note 10, at 28-30.

has been made public.[25] Supplementing these storage databases, the FBI also uses a data analysis application called the Investigative Data Warehouse, which can pull data from each of these databases and run analytic models to reveal data patterns that may be of interest to investigators.[26]

Thousands of non-FBI personnel also have direct access to these databases.[27] Others are often recipients of FBI-produced intelligence products, which are regularly derived from NSL-data analysis and provided to entities including the CIA, NSA, DIA, Joint Terrorism Task Forces at the federal, state, and local levels, foreign governments, U.S. Attorneys' offices, and the FISA Court.[28]

Given the vast authority the ECPA NSL provisions grant to the FBI to collect and store these massive amounts of data, it is unsurprising that reports have surfaced documenting the FBI's abuse of its NSL authority. Due to the low relevance standard, the FBI has relied upon the NSL process to conduct fishing

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.* at xxiii.

expeditions before it can support a subpoena or FISA court order.[29] In at least one instance, moreover, a FISA court twice *denied* the FBI access to data under Section 215, citing First Amendment concerns. In response to this denial, the FBI issued NSLs based on an identical factual predicate to the Section 215 order, gathering the same data outside the eyes of the FISA court, even though "NSLs have the same First Amendment caveat as Section 215."[30]

In others cases, NSL recipients have given the FBI information that exceeded the scope of the NSL, pertained to the wrong individuals, or covered the wrong time period, and the FBI failed to destroy the irrelevant data.[31] NSLs have been signed by individuals who were not authorized agents[32] and have been issued in connection with unauthorized investigations,[33] both in violation of the terms of 18 U.S.C. § 2709. Moreover, though a Presidential Order requires the FBI to report all such intelligence violations to the President's Intelligence Oversight Board, the FBI failed to report one or more violations in 22% of the cases in the OIG's

[29] *See* U.S. Department of Justice Office of the Inspector General (OIG), *A Review of the Federal Bureau of Investigation's Use of National Security Letters* xxiv (2007).

[30] U.S. Department of Justice Office of the Inspector General, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006* 5 (2008).

[31] OIG (2008), *supra* note 9, at 100.

[32] OIG (2010), *supra* note 20, at 75.

[33] OIG (2007), supra note 10, at 66-67.

sample.[34] Furthermore, between 2003-2005, the FBI also failed to report almost 4,600 NSLs to Congress—nearly all ECPA NSLs—as required by § 2709.[35]

Separate from but related to the NSL process, the FBI for many years issued so-called exigent letters, demanding the kinds of data available through NSLs but circumventing even the procedures for issuing NSLs. These letters were often structured to include a promise from the FBI of "legal process to follow," such as a subpoena or NSL.[36] In one instance, the FBI used an exigent letter to gather reporter and news organization telephone data following a media leak constituting protected First Amendment speech.[37] It entered these records into its NSL databases, where they remained for three years until discovered by the OIG.[38]

II. NSL DATA REVEAL DEEPLY SENSITIVE INFORMATION ABOUT INDIVIDUALS AND THEIR ASSOCIATIONS

The types of data that can be obtained by NLSs reveal a wide variety sensitive information about the individuals from which the information comes and their associations, beliefs, speech and activities. Despite government claims that the collected data is "just metadata" and do "not include any information about the

[34] *Id.*

[35] *Id.*

[36] OIG (2010), *supra* note 20, at 65.

[37] *Id.* at 89-122.

[38] *Id.* at 278.

content" of phone calls, text messages, and emails, NSL data often can reveal information of the same character as that which could be obtained by listening in on a phone call or reading a text or email.[39]

In many instances, "non-content" data, such as NSL data, may be of even more value to government officials than content data. Since substantial non-content data analysis can be automated, non-content data surveillance often yields substantive information cheaper and faster than approaches such as traditional wiretapping, which can be more labor intensive.[40] And unlike content data, the routine creation of non-content is often unavoidable and unprotectable. As computer scientist Matt Blaze noted, "we leave trails of metadata [non-content data] everywhere, anytime we reach out to another person." There is almost no existing way to dust these trails.[41] Due to § 2709's broad scope, the relatively low cost of analysis, and the unprotected nature of non-content data, the FBI can use NSLs to determine everything from individuals' actions, beliefs and religious and political affiliations to organizations' structures and strategic plans to much more.

[39] *Administration White Paper*, *supra* note 7, at 2.

[40] Jane Mayer, *supra* note 5.

[41] *See* Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, Wired (June 16, 2013 9:30 AM), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again.

A. Even a Single Call, Text, or E-mail Reveals Sensitive Information

Though each NSL request can include information on thousands of interactions, a single phone call, text message, or email can already disclose deeply private information.

In many instances, details about the content of a conversation can be deduced from the identity of the parties. Although data that the FBI receives does not explicitly state whom a subscriber has contacted—NSL requests contain telephone numbers or e-mail addresses, not names—it is trivially easy for the FBI to match these data to specific individuals. One way to do so is to issue another NSL. An even more straightforward approach is to conduct a search for a number or address either online or through a public database. Consider, for example, the phone number 916.446.5247, which a Google search can instantly connect to Planned Parenthood Affiliates of California. Or the email pacificregion@aa.org, which, even without a Google search, one could associate with Alcoholics Anonymous. More generally, research shows that the government can link identities associated with lesser-known phone numbers just as easily.[42]

[42] *See* Rebecca J. Rosen, *Stanford Researchers: It is Trivially Easy to Match Metadata to Real People*, The Atlantic (Dec. 24, 2013 1:50 PM), http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-real-people/282642; Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, Web Policy (Mar.

(continued on next page)

With just the identity of the other side of a record, the FBI can already learn sensitive information about an individual. For example, certain phone lines are reserved for a specific purpose: support hotlines for rape victims, domestic violence victims, people contemplating suicide, or "listening lines" for gay and lesbian youths.[43] Such hotlines exist for veterans, first responders, drug addicts, gambling addicts, and child abuse victims.[44] Similarly, almost every federal, state, and local agency, including the FBI, has established hotlines for reporting fraud and misconduct by both internal and external sources.[45] Likewise, some email addresses are allocated to particular objectives, such as tipping off reporters about a potential story.[46] A 30-minute call or a lengthy email to any of these hotlines

(footnote continued from previous page)

12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata (finding that simple Google searches and a cheap, consumer-oriented data tool could match 91% of a random sample of 100 phone numbers to specific individuals).

[43] *See, e.g.*, *Gay, Lesbian, Bisexual and Transgender National Hotline*, GLBT National Help Center (last visited Mar. 11, 2014), http://www.glbtnationalhelpcenter.org/hotline.

[44] *See, e.g.*, *Childhelp National Child Abuse Hotline*, Childhelp (last visited Mar. 14, 2014), http://childhelp.org/pages/hotline-home.

[45] *See, e.g.*, Barton Gellman, *NSA Statements to the Post*, Wash. Post, Aug 15, 2013, http://wapo.st/1ixchnm; *Reporting Income Tax Fraud*, State of California Franchise Tax Board (last visited Mar. 17, 2014), https://www.ftb.ca.gov/online/Fraud_Referral/important_information.asp.

[46] *See* New York Times, *Contact the Public Editor*, NYTimes.com (last visited Mar. 18, 2014), http://publiceditor.blogs.nytimes.com/contact-the-public-

(continued on next page)

reveals information that anyone would consider private. In each of these cases, even without knowing a single word of the phone conversation or email exchange, NSL data from the interaction discloses meaningful clues as to the underlying content. Though these hotlines and tip lines are meant to allow vital, anonymous expression, NSLs allow the FBI to strip away that safety and anonymity and expose both the individual and effectively the content of his or her speech.

In an empirical study highlighting the significance of NSL data in these situations, Stanford University researchers Jonathan Mayer and Patrick Mutchler demonstrated that substantial personal information could be revealed through a single phone call. Analyzing data from 546 volunteers' phone calls to 33,688 unique numbers, Mayer and Mutchler discovered that a large proportion of participants contacted "sensitive organizations" in their daily lives.[47] The table below shows the proportion of volunteers who made at least one call to an organization whose purpose revealed sensitive information about the caller:

(footnote continued from previous page)
editor/; Mail & Guardian, *Story Tip-Offs* (last visited Mar. 18, 2014), http://mg.co.za/page/story-tip-offs.

[47] Mayer & Mutchler, *supra* note 42 ("phone metadata is unambiguously sensitive, even in a small population and over a short time window. We were able to infer medical conditions, firearm ownership, and more, using solely phone metadata.").

Category	**Participants with ≥ 1 Calls**
Health Services	57%
Financial Services	40%
Pharmacies	30%
Veterinary Services	18%
Legal Services	10%
Recruiting and Job Placement	10%
Religious Organizations	8%
Firearm Sales and Repair	7%
Political Officeholders and Campaigns	4%
Adult Establishments	2%
Marijuana Dispensaries	0.4%

As several of these categories suggest, NSL data from a single interaction can reveal sensitive information about possible civil legal disputes or criminal activity. Sensitive information obtained through NSLs is shared with U.S. Attorney's Offices,[48] and a call to a marijuana dispensary, an email to CustomerService@GunsAmerica.com, or a text message to a known gang member, could all serve as reason to begin an investigation or as evidence in a later criminal case, even where the individual was not suspected of anything at the time of the NSL. Contacting a defense attorney may even indicate concerns about criminal activity.

Furthermore, how and when governmental authorities act on these potentially incriminating communications depends solely on their interpretation of

[48] OIG (2007), *supra* note 10, at xxiii.

the data. If the picture that NSL data paints is inaccurate or incomplete, it can lead to unnecessary arrests, unexplained detentions, or at the very least, a further invasion of an individual's privacy through additional searches.[49]

In the extreme, NSL data can reveal information even more sensitive than the actual contents of the communication itself. Consider, for instance, the case of text message donation hotlines. Set up as partnerships between wireless telephone carriers and non-profit organizations, these donation hotlines enable wireless subscribers to donate to charities through cellular text messages. By sending a message to a predetermined phone number, a subscriber triggers the wireless carrier to make a donation and add the amount to his monthly bill. In one such program to support of victims of the Haitian earthquake, the American Red Cross enabled thousands of subscribers to text HAITI to 90999 to donate $10.[50]

In recent years, text-message donation hotlines have gained popularity and expanded to numerous organizations such as churches, cancer research

[49] *See* Griffin Boyce and Brian Duggan, *The Real Reason Why Metadata Collecting Is Dangerous*, New America Foundation (June 17, 2013 4:54 PM), http://inthetank.newamerica.net/blog/2013/06/real-reason-why-metadata-collecting-dangerous.

[50] *See* Declaration of Edward W. Felten, ACLU v. Clapper, No. 13-cv-03994 (WHP) (S.D.N.Y. Aug. 23, 2013), ECF No. 27 ("Felten Decl."), 16.

foundations, and reproductive services organizations like Planned Parenthood.[51] After a policy change by the Federal Election Commission in 2012, these programs have even invaded electoral campaigns. Candidates such as Barack Obama and Mitt Romney raised money directly via text messages.[52]

In these interactions, the significant information—the identity of the recipient organization and size of the donation—is contained in the NSL data, not in the content of text messages such as "HAITI." The NSL data alone is sufficient to determine whether the sender was donating (and how much) to a church, Planned Parenthood, or a particular political campaign.

B. Patterns of Calls, Texts, and Emails Reveal Even More Sensitive Information

In addition to inferences from a single communication, the FBI can gain a far richer and more deeply revealing picture of the contours of a person's life using data-analysis techniques that assess patterns of activity—who an individual contacts, how frequently, and when. By analyzing the hundreds to hundreds of thousands of data points returned in response to each NSL request, the FBI can

[51] *See Donate by Text*, Susan G. Komen for the Cure (last visited Mar. 11, 2014), http://ww5.komen.org.

[52] *See, e.g.*, Dan Eggen, *Text 'Give' to Obama: President's Campaign Launches Cellphone Donation Drive*, Wash. Post (Aug. 23, 2012), http://www.washingtonpost.com/politics/text-give-to-obama-presidents-campaign-launches-cellphone-donation-drive/2012/08/23/5459649a-ecc4-11e1-9ddc-340d5efb1e9c_story.html.

learn an individual's religion, sleep patterns, work habits, hobbies, number and location of friends, and even civil and political affiliations. By combining data from multiple requests about multiple individuals, the FBI can deduce the nature and function of entire organizations, and how the people within them interact.

1. Social Graph and Predictive Modeling Techniques are Easy to Implement and Immensely Informative

The recent evolution of two tools, social graphs and predictive modeling, add particular potency to the aggregation of data gathered through NSLs. With respect to the first, publicly available software packages can generate social graphs from datasets such as the FBI's NSL database. These software packages take a dataset of non-content data and output a graphical image of an individual's patterns of communication or of communications among members of a group. Consider two such software packages: MIT's Immersion and IBM's i2 Analyst's Notebook.

MIT's Immersion uses the "From, To, Cc and Timestamp" fields of a person's emails—all included in response to NSL requests for electronic transaction communications records—to create a "people-centric view" of that person's life. In under a minute, the software churns through thousands of emails and spits out a network of individuals and organizations with which the user has communicated, highlighting key contacts and linking contacts with each other. By tracking interactions across time, Immersion can also trace the development of relationships. Based on the frequency of the emails exchanged, the software visualizes a growth or contraction of connections between not only the original user, but also other individuals in his network, detailing his "personal and professional history."[53]

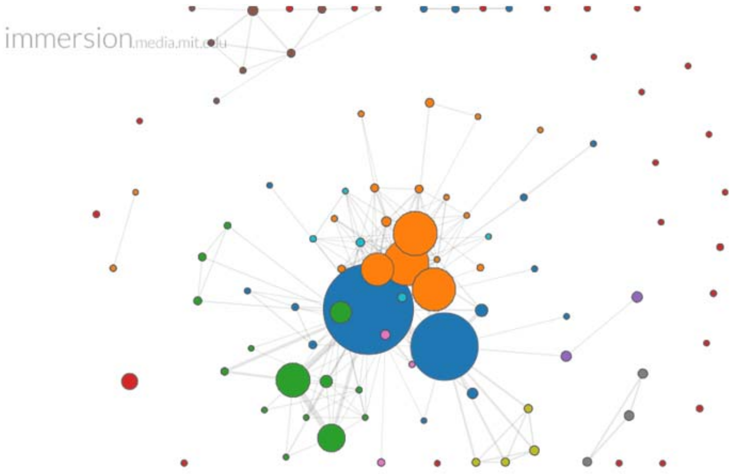

Figure 1: An Immersion user's network, visualized as a social graph

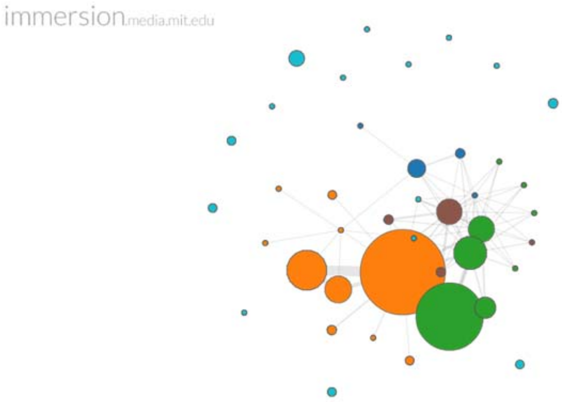

Figure 2: The Immersion user's network a week earlier. The expansion and contraction of circles provide a visual interpretation of relationship development between individuals in the network.

[53] *See Immersion*, MIT Media Lab (last visited Mar. 17, 2014), https://immersion.media.mit.edu.

IBM's more sophisticated i2 Analyst's Notebook software uses the same basic ideas to identify key people, events, and connections in networks described by much larger datasets.[54] For example, the Environmental Investigation Agency used Analyst's Notebook to process non-content data from undercover investigations in order to accurately map out a criminal international tiger trafficking network.[55]

Either in conjunction with or independent of social graphs, the FBI can also use predictive modeling to derive sensitive information about individuals and groups from the data it has gathered through NSLs. Predictive models allow analysts to use known patterns of activity to make specific and highly accurate predictions about individual and organizational attributes, such as race, religion, or leadership structure. For example, happily married couples often call each other many times a week. If an analyst applied a predictive model based on this pattern to a set of toll billing records for an individual who had called her spouse infrequently for many months, the model might indicate that she had between a predictable chance of filing for divorce within one year.

[54] *See Analyst's Notebook*, IBM (last visited Mar. 17, 2014), http://www-03.ibm.com/software/products/en/analysts-notebook-family.

[55] *See* IBM, *Environmental Investigation Agency: IBM i2 Solution Help Combat the Illegal Tiger Trade* (2012).

The larger the dataset a researcher has upon which to build a predictive model, the more precise the model will be. If a certain calling pattern is only seen in a few married couples, then applying a model based on that pattern to new data will yield only weak inferences. But if the same pattern is seen in 5,000 couples, a model based on the pattern will offer opportunities to ask nuanced queries and make inferences with confidence. For instance, a researcher could query the likelihood of divorce in six months and in two years, and the confidence intervals around results might be plus or minus 5% rather than 10%. Given the vast data set that NSLs provide—including hundreds of millions of observations, as estimated above—it is almost certain that FBI researchers have created sophisticated and highly precise predictive models. Even if they have not, there is an extensive public literature on predictive modeling upon which the Bureau can draw.

Though the FBI has developed its data-analysis tools in order to improve its terrorism and espionage investigations, these dual-use tools are even easier to apply to ordinary Americans. As Matt Blaze argues, "[t]he better understood the patterns of a particular group's behavior, the more useful it is. This makes using metadata [non-content data] to identify lone-wolf Al Qaeda sympathizers (a tiny minority about whose social behavior relatively little is known) a lot harder than, say, rooting out Tea Partiers or Wall Street Occupiers, let alone the people with whom we share our beds."[56]

2. NSL Data Reveal Extensive Private Personal, Political, Associational, Religious, Corporate, Medical, and Financial Information

As we lack access to the FBI's massive database of NSL data, we cannot say with precision what applying social graphs and predictive models to this data would reveal. But even relatively naïve analyses of this data yields information on medical conditions, religious affiliations, relational and political networks, corporate structures, and finances. Comprehensively applying social graphs and predictive modeling to millions of observations would only increase the sensitivity of many of these inferences.

First, information obtained through NSLs can reveal substantial information about the operations of political groups. A social graph derived from NSL data can reveal an association's otherwise anonymous membership, donors, political supporters, and confidential sources. As former NSA official William Binney has stated, the government could use data analysis to "monitor the Tea Party, or reporters, whatever group or organization you want to target. . . It's exactly what

[56] Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, Wired (June 16, 2013 9:30 AM), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again.

the Founding Fathers never wanted."[57] Even a cursory analysis of the frequency of communications among members could distinguish who within a grassroots movement is an ardent organizer and who is a casual participant. With more detailed study, as Susan Landau noted, non-content data can even show "if opposition leaders are meeting, who is involved, where they gather, and for how long."[58]

Second, NSL data disclose a great deal about the strength of personal relationships. Generally, a person one calls once a week is more likely to be a close friend than someone one calls once a year.[59] More specifically, consider an NSL request made with regards to a man in an illicit intimate relationship. The data returned in reply to this request might show he makes long, frequent calls to his mistress late at night, in contrast to the short, sparse calls made to his wife. Eventually, the affair may end, and the frequency of the calls to the mistress might drop or end entirely. Or, perhaps the affair continues and he begins to communicate frequently with an attorney specializing in divorce. Precisely in this vein, it was FBI analysis of non-content data similar to NSL data that ultimately

[57] Jane Mayer, *supra* note 5 (quoting interview with Binney) (internal quotation marks omitted).

[58] Jane Mayer, *supra* note 5 (quoting interview with Susan Landau).

[59] *See* Felten Decl., 17.

revealed former CIA director David Petraeus's affair with Paula Broadwell. While looking into allegations of another sort, the FBI linked together multiple email addresses used by Broadwell to uncover the affair that ended both participants' public careers.[60]

Third, the FBI can easily infer religious affiliation and association from information gained ghrough NSLs. On the most basic level, adherents of particular religions likely call organizations affiliated with their religion more often than they call organizations affiliated with other religions. Relying only on "the naïve assumption" that this is true, Mayer and Mutchler accurately identified the religion of 73% of participants.[61]

Additionally, adherents of different religions may exhibit notable patterns of phone calls, emails, and text messages. For example, the NSL data of an individual who strictly observes the Sabbath would show no communications on Saturdays, while that of an individual who regularly attends church on Sunday mornings would show little activity at that time. NSL data of an individual who is Muslim

[60] *See* Hal Hodson, *How Metadata Brought Down CIA Boss David Petraeus*, NewsScientist (Nov. 16, 2013 1:59 PM), http://www.newscientist.com/article/dn22511-how-metadata-brought-down-cia-boss-david-petraeus.html.

[61] Mayer & Mutchler, *supra* note 42.

and recites the Isha prayer nightly might show more activity between dawn and dusk if that individual communicates with others before or after prayers.

Furthermore, on an organizational level, a social graph of email data could disclose a network of friends who frequent the same religious services. An evolution of this social graph over time could reveal when an individual changed faiths or began to frequent a different place of worship. It could also show who manages the religious social community, which members are most active, and to whom certain members turn for advice at critical moments.

Fourth, NSL data can reveal internal or external dynamics within the corporate sector. For example, NSL data can reveal the relative power of employees within a firm. As *The Economist* observed: "People at the top of the office or social pecking order often receive quick callbacks [and] do not worry about calling other people late at night."[62] The lengths of phone calls can also be indicative: "Influential [people] reveal their clout by making long calls, while the calls they receive are generally short."[63]

NSL data can also expose valuable information about a company's future. Multiple calls among a subset of the members of a board of directors over a short

[62] *Mining Social Networks: Untangling the Social Web*, Economist (Sept. 2, 2010), http://www.economist.com/node/16910031.

[63] *Id.*

period of time and soon before a board meeting might evince intentions to stage a corporate takeover. Correspondence by executives at a smaller firm with those at a larger competing firm, and then investment banks and attorneys who specialize in acquisitions, could indicate a coming sale of the company.

Fifth, NSL data can reveal substantial information about someone's personal finances. As noted above, Mayer and Mutchler found that over half of individuals in their sample called at least one of their financial institutions over only the few-month time horizon of their study. An individual in debt would have frequent contact with entities identifiable as debt collectors and might contact payday loan services or an attorney who specializes in Chapter 7 bankruptcy filings. Someone who provides funds to a relative abroad might receive more emails from Western Union than is typical and might contact foreign banking organizations. Moreover, NSL data obtained through ECPA's provisions is only one subset of all NSL data that the FBI can collect. Other statutes provide authority to demand full credit reports, for example, data that could quickly corroborate evidence derived from ECPA NSLs.

Finally, patterns in data obtained through FBI use of NSLs can reveal an enormous amount of sensitive information about medical conditions. Consider, for instance, the inferences derived from personal records showing "a call to a gynecologist, and then a call to an oncologist, and then a call to close family members."[64] Mayer and Mutchler's study empirically documents this possibility. Relying on patterns of phone calls to certain kinds of doctors, laboratories, pharmacies, and home-reporting hotlines, Mayer and Mutchler deduced that one participant in their study suffered from cardiac arrhythmia and another from relapsing multiple sclerosis. For a third, they observed that the participant had a long morning call with her sister, then two days later placed a series of calls to the local Planned Parenthood clinic, placed additional calls to the clinic two weeks later, and then made a final call a month afterwards.[65]

In a different context, a recent, widely reported incident involving Target illustrates how predictive models can enhance these inferences. Using extensive customer data, Target determined that pregnant women are more likely to buy certain products at different stages of pregnancy. To capitalize on this trend, Target used its database to create a "pregnancy prediction" score upon which it based an advertisement campaign offering targeted coupons to women in different trimesters. In so doing, Target discovered incredibly private information about its customers' reproductive choices and, in at least one case, determined that a teenage girl was pregnant and sent her pregnancy related coupons before even her father

[64] Jane Mayer, *supra* note 5 (quoting Susan Landau) (internal quotation marks omitted).

[65] *See* Mayer & Mutchler, *supra* note 42.

found out.[66] These types of patterns that can easily be discerned from aggregated information are often far more revealing than one might ever imagine from any individual piece of data.

CONCLUSION

The reach of NSL demands for information into the private lives of ordinary Americans is nearly limitless. Contradicting government claims that NSL data does not include content, simple analysis of NSL data can reveal a wide variety of any American's otherwise anonymous political activity or beliefs, close relationships, religious affiliations, personal or community associations, medical records, financial data and more. The FBI can learn deeply sensitive information about the daily life of almost every person in this country without meaningful, affirmative judicial approval.

DATED: March 28, 2014

Respectfully submitted,

JUELSGAARD INTELLECTUAL
PROPERTY & INNOVATION CLINIC
Mills Legal Clinic at Stanford Law School

By: /s/ Phillip R. Malone
Phillip R. Malone
Counsel for Amici Curiae

[66] *See* Charles Duhigg, *How Companies Learn Your Secrets*, NYTimes.com (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp.

STATEMENT OF RELATED CASES

Consolidated cases *Under Seal v. Holder, et al.*, No's. l3-15957 and 13-16731, and *Under Seal v. Holder, et al.*, No. l3-16732, which involve the same legal issues but different NSL recipients, are related. This Court has ordered that No's. l3-15957 and 13-16731 be briefed separately from, but on the same briefing and oral argument schedule as, No. l3-16732.

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) and 29(d) because this brief contains 6,925 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word for Mac 2011, the word processing system used to prepare the brief, in 14 point Times New Roman font.

I declare under penalty of perjury that this Certificate of Compliance is true and correct and that this declaration was executed on March 28, 2014.

By: /s/Phillip R. Malone
Phillip P. Malone

JUELSGAARD INTELLECTUAL
PROPERTY & INNOVATION CLINIC

Counsel for Amici Curiae

EXHIBIT A

EXHIBIT A

List of *Amici* and Short Biographies[1]

Harold Abelson is a Professor in the Department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. A fellow at the Institute of Electrical and Electronic Engineers (IEEE), he was awarded the 2011 Association for Computing Machinery (ACM) Special Interest Group on Computer Science Education Award for Outstanding Contribution to Computer Science Education and the 2012 ACM Karl V. Karlstrom Outstanding Educator Award. Professor Abelson's research interests focus on information technology and policy; he is also an advocate of intellectual property reform, innovation, and an open Internet. His publications include *Access Control is an Inadequate Framework for Privacy Protection* and *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*.

Andrew W. Appel is the Chair of and a Professor in Princeton University's Computer Science Department. He was named an ACM Fellow in 1998 and received the 2002 ACM Special Interest Group on Programming Languages (SIGPLAN) Distinguished Service Award. Professor Appel is active in issues related to the intersection between law and technology, focusing his research

[1] Amici file this brief in their individual capacities, not as representatives of the institutions with which they are affiliated.

primarily on program verification, computer security, programming language semantics, and compilers. His publications include Compiling with Continuations and Security Seals on Voting Machines: A Case Study.

Steven M. Bellovin is a Professor in the Computer Science Department at Columbia University. He was elected to the National Academy of Engineering in 2001 and awarded the NIST/NSA National Computer Systems Security Award in 2006. Professor Bellovin's research focuses on networks, security, and the tensions between the two. Examples of his publications include Firewalls and Internet Security: Repelling the Wily Hacker, Facebook and privacy: It's complicated, and When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning.

Matthew A. Blaze is an Associate Professor in the Computer and Information Science Department at the University of Pennsylvania where he also directs the Distributed Systems Lab Research. He implemented the Crytographic File System for Unix in 2002, which remains in use today. Professor Blaze's research interests center cryptography and its applications, trust management, human scale security, secure systems design, and networking and distributed computing. Several recent publications include Going Bright: Wiretapping Without Weakening Communication Infrastructure and Notes on Theoretical Limitations and Practical Vulnerabilities of Internet Surveillance Capture.

Fernando J. Corbato is Professor Emeritus in the Department of Electrical Engineering and Computer Science at M.I.T. He has achieved wide recognition for his pioneering work on the design and development of multiple-access computer systems. He was associated with the M.I.T. Computation Center from its organization in 1956 until 1966. In 1963 he was a founding member of Project MAC, the antecedent of CSAIL. In 1990, Prof. Corbato received the Turing Award, "for his pioneering work in organizing the concepts and leading the development of the general-purpose, large-scale, time-sharing and resource-sharing computer systems." At his retirement in 1996, Prof. Corbato held a Ford Professor of Engineering Chair.

Lorrie Faith Cranor is an Associate Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. She is also the director of the CyLab Usable Privacy and Security Laboratory. Professor Cranor was the 2006 Phase 1 Winner of the Tor Graphical User Interface Design Competition and 2004 IBM Best Academic Privacy Faculty Award. Her work has been widely recognized, most recently being awarded the Future of Privacy Forum Privacy Papers for Policy Makers 2012 award for Leading Paper. Her research interests focuses on usable privacy and security, with recent publications including The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification and Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences.

David Farber is the Distinguished Career Professor of Computer Science and Public Policy in the School of Computer Science at Carnegie Mellon University. He has been a major contributor to the development of computer networking and computer programming languages. Professor Farber served as Chief Technologist to the FCC from 2000 to 2001 and received the 1995 ACM Special Interest Group on Data Communications Award for lifelong contributions to the computer communications field. His publications include A Secure and Reliable Bootstrap Architecture and Recoverability of Communication Protocols—Implications of a Theoretical Study.

Edward W. Felten is is the Robert E. Kahn Professor of Computer Science and Public Affairs, and the Director of the Center for Information Technology Policy, at Princeton University. He has published more than 100 papers in the research literature. In 2011-12 he served as the first Chief Technologist at the Federal Trade Commission. He has testified before Congressional hearings on topic including surveillance and privacy. He is a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

Michael J. Freedman is an Associate Professor in the Computer Science Department at Princeton University. His research broadly focuses on distributed systems, security, and networking, and has led to commercial products and deployed systems reaching millions of users daily. His privacy-related research has developed techniques for untrusted and encrypted cloud services, anonymous communication systems, and secure multi-party computation. A recipient of the Presidential Early Career

Award for Scientists and Engineers (PECASE), Freedman has also been recognized by a National Science Foundation CAREER Award, the Office of Naval Research's Young Investigator Award, membership in DARPA's Computer Science Study Group, an Alfred P. Sloan Fellowship, and multiple conference award publications.

Matthew D. Green is an Assistant Research Professor in the Department of Computer Science at Johns Hopkins University. He received the 2007 Award for Outstanding Research in Privacy Enhancing Technologies. Professor Green's research interests include privacy-enhanced information storage, anonymous payment systems, and bilinear map-based cryptography as well as cryptographic engineering. His publications include *Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage* and *Security Analysis of a Cryptographically-Enabled RFID Device*.

J. Alex Halderman is an Assistant Professor of Electrical Engineering and Computer Science at the University of Michigan. His work has won numerous distinctions, including two best paper awards from the USENIX Security conference. Professor Halderman's research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. His publications include Telex: Anticensorship in the Network Infrastructure and Lest We Remember: Cold-Boot Attacks on Encryption Keys.

Robert Harper is a Professor of Computer Science at Carnegie Mellon University, where he has been a member of the faculty since 1988. His research focuses on the application of constructive type theory, a computationally based foundation for mathematics, to programming languages and program□verification. He was elected as an ACM Fellow in July of 2006. He is the co- recipient of the 2006 Most Influential Paper Ten Years Later Award from the ACM Conference on Programming Language Design and Implementation and of the 2007 Test of Time Award from the IEEE Conference on Logic in Computer Science. He is a past editor of the Journal of the ACM, and is currently a member of the editorial board for the Journal of Functional Programming, Information and Computation, and Mathematical Structures in Computer Science. He was honored with the Allen E. Newell Award for Excellence in Research, and the Herbert A. Simon Award for Excellence in Teaching, both at Carnegie Mellon University.

David Mazieres is associate professor of Computer Science at Stanford University, where he leads the Secure Computer Systems research group. Prof. Mazieres received a BS in Computer Science from Harvard in 1994 and Ph.D. in Electrical Engineering and Computer Science from MIT in 2000. Prof. Mazieres's research interests include Operating Systems and Distributed Systems, with a particular focus on security. Prof. Mazieres has several awards including a Sloan award (2002), USENIX best paper award (2001), NSF CAREER award (2001), MIT Sprowls best thesis in computer science award (2000), and fast-track journal papers at OSDI (2000), SOSP (1995), and SOSP (2005).

Greg Morissett is the Allen B. Cutting Professor of Computer Science at Harvard University, where he also served as the Associate Dean for Computer Science and Engineering from 2007-2010. Prof. Morrisett has received a number of awards for his research on programming languages, type systems, and software security, including a Presidential Early Career Award for Scientists and Engineers, an IBM Faculty Fellowship, an NSF Career Award, and an Alfred P. Sloan Fellowship. He was recently made a Fellow of the ACM. He currently serves on the editorial board for The Journal of the ACM and as co-editor-in-chief for the Research Highlights column of Communications of the ACM. In addition, Prof. Morrisett has served on the DARPA Information Science and Technology Study (ISAT) Group, the NSF Computer and Information Science and Engineering (CISE) Advisory Council, Microsoft Research's Technical Advisory Board, and Microsoft's Trusthworthy Computing Academic Advisory Board.

James Purtilo is an Associate Professor of Computer Science at the University of Maryland, College Park, where he specializes in software producibility and product assurance. Purtilo has published on software formal methods, rapid prototyping and testing, most recently with a focus on mechanisms for intrusion detection and prevention in secure systems. At the University of Maryland, he has served as director of the Master of Software Engineering Program on his campus, Associate Dean in his college and Chair of CS Department's undergraduate program.

Ronald L. Rivest is a Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. A founder of RSA Security and Peppercoin, Professor Rivest was received the 2012 National Cyber Security Hall of Fame and 2005 Massachusetts Innovation & Technology Exchange (MITX) Lifetime Achievement Award. His research primarily focuses on cryptography and computer and network security. His recent publications include *Introduction to Algorithms* and *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*.

Avi Rubin is a Professor of Computer Science at Johns Hopkins University and Technical Director of the Johns Hopkins Information Security Institute. He was the Director of the USENIX Association from 2000 to 2004 and a recipient of the 2007 Award for Outstanding Research in Privacy Enhancing Technologies. His research primarily focuses on computer security. His recent publications include *Charm: A Framework for Rapidly Prototyping Cryptosystems* and *Security and Privacy in Implantable Medical Devices and Body Area Networks*.

Barbara Simons is retired from IBM Research. She is the only woman to have received the Distinguished Engineering Alumni Award from the College of

Engineering of U.C. Berkeley. A fellow of the American Association for the Advancement of Science (AAAS) and a fellow and former president of the Association for Computing Machinery (ACM), she has also received the Computing Research Association Distinguished Service Award. An expert on electronic voting, Simons recently published Broken Ballots: Will Your Vote Count?, a book on voting machines co-authored with Douglas Jones. She was appointed to the Board of Advisors of the U.S. Election Assistance Commission in 2008, and she was a member of the workshop, convened at the request of President Clinton, that produced a report on Internet Voting in 2001.

Eugene H. Spafford is a Professor in the Department of Computer Science at Purdue and serves as the Executive Director of Purdue's Center for Education and Research in Information Assurance and Security. He was an advisor to the National Science Foundation (NSF) and is the Editor-in-Chief of the Elsevier journal, Computers & Security. Professor Spafford was inducted into the Cybersecurity Hall of Fame in 2013 and received the 2007 ACM President's Award. His research focuses on preventing, detecting, and remedying information system failures and information security. He has published many articles and books including *Practical UNIX and Internet Security* and *Web Security, Privacy & Commerce*.

Daniel S. Wallach is a Professor of Computer Science and a Rice Scholar at the Baker Institute for Public Policy at Rice University. A member of the USENIX Association Board of Directors, he received the 2013 Microsoft Faculty Research Award, 2009 Google Research Award, and 2000 NSF CAREER Award. Professor Wallach's research primarily focuses on computer security and has touched on issues include web browsers and servers, peer-to-peer systems, smartphones, and voting machines. His publications include VoteBox: A Tamper-evident, Verifiable Electronic Voting System and Secure Routing for Structured Peer-to-Peer Overlay Networks.

CERTIFICATE OF SERVICE

I certify that I caused the foregoing **BRIEF *AMICI CURIAE* OF EXPERTS IN COMPUTER SCIENCE AND DATA SCIENCE IN SUPPORT OF APPELLANTS** to be delivered to the court by placing the same for Federal Express next-business-day delivery on March 31, 2014, addressed as follows:

Susan Soong, Chief Deputy Clerk - Operations
U.S. Court of Appeals for the Ninth Circuit
95 7th Street
San Francisco, CA 94103

I am informed and believe that the court will effect service on the parties.

Dated: March 31, 2014

/s/ Lynda F. Johnston
LYNDA F. JOHNSTON