14-42

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

AMERICAN CIVIL LIBERTIES UNION, NEW YORK CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs-Appellants,

v.

JAMES R. CLAPPER, IN HIS OFFICIAL CAPACITY AS DIRECTOR OF NATIONAL INTELLIGENCE, KEITH B. ALEXANDER, IN HIS OFFICIAL CAPACITY AS DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE, ERIC H. HOLDER, JR., IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES, CHARLES T. HAGEL, IN HIS OFFICIAL CAPACITY AS SECRETARY OF DEFENSE, ROBERT S. MUELLER, III, IN HIS OFFICIAL CAPACITY AS DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION,

Defendants-Appellees.

On Appeal From The United States District Court
For The Southern District of New York
Case Nos. 13-cv-03994 (WHP)
Honorable William H. Pauley, III, District Judge

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

Cindy Cohn
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
cindy@eff.org
Counsel for Amici Curiae

TABLE OF CONTENTS

STATEMENT OF INTEREST 1

LIST OF AMICI CURIAE 2

INTRODUCTION 4

ARGUMENT 5

I. METADATA REVEALS HIGHLY PERSONAL AND SENSITIVE INFORMATION 5

A. Telephony Metadata Reveals Sensitive Information, Even in Limited Quantities. 8

B. In the Aggregate, Telephony Metadata Is Even More Revealing 10

C. Creating a Trail of Sensitive Metadata Is an Unavoidable Byproduct of Modern Life 15

II. THE GOVERNMENT'S LIMITATIONS ON METADATA COLLECTION AND USE DO NOT MITIGATE THE PRIVACY CONCERNS 21

CONCLUSION 25

TABLE OF AUTHORITIES

Federal Cases

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted],
No. BR 13-109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013) 7, 10

In re Application of the FBI for an Order Requiring the Production of Tangible Things,
No. BR 14-01 (FISA Ct. Feb. 5, 2014) 22, 23

Smith v. Maryland,
442 U.S. 735 (1979) 6, 15

United States v. Jones,
565 U.S. __, 132 S. Ct. 945 (2012) 4

Federal Statutes

18 U.S.C. § 2703 21

18 U.S.C. § 2709 21

Other Authorities

Bayesian Spam Filtering, Wikipedia
https://en.wikipedia.org/wiki/Bayesian_spam_filtering 14

Carter Jernigan and Behram Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, First Monday (Oct. 5, 2009),
http://firstmonday.org/article/view/2611/2302 19

Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.....20

Corrina Cortes, *et al*., *Communities of Interest*, AT&T Shannon Research Labs, *available at* http://www.research.att.com/~volinsky/papers/portugal.ps.....14

Eunjoon Cho, *et al.*, *Friendship and Mobility: User Movement In Location-Based Social Networks* (2011), *available at* http://roke.eecs.ucf.edu/Reading/Papers/Friendship%20and%20Mobility%20User%20Movement%20In%20Location-Based%20Social%20Networks.pdf....19

Haim Kaplan, *et al.*, *Just the Fax – Differentiating Voice and Fax Phone Lines Using Call Billing Data*, AT&T Labs, http://bit.ly/19Aa8Ua 14

Hui Zang & Jean Bolot, *Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study*, (2011), *available at* http://paloalto.thlab.net/uploads/papers/Mobicom_2011_-_Anonymization_of_location_data_does_not_work_-_Zang_Bolot.pdf 21

Immersion, https://immersion.media.mit.edu.....18

James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times (Sep 28, 2013), *available at* http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html 17

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA's Got Your Number* (Dec. 23, 2013), http://webpolicy.org/2013/12/23/metaphone-the-nsas-got-your-number.....21, 24

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2013), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata.....9, 14

Kieran Healy, *Using Metadata to Find Paul Revere* (June 9, 2013), http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere.....12

Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.....11, 17, 24

Machine Learning for Antivirus Software, About Data Mining (Apr. 24, 2013), http://www.aboutdm.com/2013/04/machine-learning-for-anti-virus-software.html.....14

Matt Blaze, *Phew, NSA is Just Collecting Metadata. (You Should Still Worry)*, Wired (Jun. 19, 2013), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again 10

Michael Kosinski, *et al.*, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l. Acad. Sci 5803 (2013), *available at* http://www.pnas.org/content/early/2013/03/06/1218772110.abstract 19

Michael Pearson, *Obama: No one listening to your calls*, CNN (Jun 9, 2013), http://www.cnn.com/2013/06/07/politics/nsa-data-mining. 4

Nat'l Research Council of the Nat'l Acad. of Sci., *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (2008) 17

Privacy and Civil Liberties Oversight Bd., Report on the Telephone Records Program (Jan. 23, 2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf 23, 24

Siobhan Gorman, *et al.*, *U.S. Collects Vast Data Trove*, Wall St. J. (June 7, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922 10

Steven M. Bellovin, *Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the § 215 and § 702 Surveillance Programs* (July 31, 2013), *available at* https://www.cs.columbia.edu/~smb/papers/PCLOB-statement.pdf 16

Transcript: Diane Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program, Wash. Post (June 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program...5

Yaniv Altshuler, *et al.*, *Incremental Learning with Accuracy Prediction of Social and Individual Properties from Mobile-Phone Data* (2012), *available at* http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6406354&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6406354 19

Yves-Alexandre de Montjoye, *et al*., *Unique in the Crowd: The Privacy Bounds of Human Mobility* (2013), *available at* http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html 20

STATEMENT OF INTEREST[1]

Amici are leading computer and data science experts from across the United States, specializing in data and computer security, data analysis, cryptography, and privacy-enhancing technologies. Most *amici* are professors of computer science at the country's leading educational institutions; others have enjoyed distinguished careers in the private sector. Collectively, *amici*'s research and technological contributions have significantly shaped the development of modern communications technology.

Amici offer this brief to emphasize for the Court the extraordinary sensitivity of communications metadata. *Amici*'s expertise and familiarity with data analysis and communications technology offer a particularly informed perspective on the issues confronted in this case.

Amici base this brief on the Declaration of Professor Edward W. Felten submitted in the District Court below. They write to reassure this Court that Professor Felten's conclusions are sound and widely shared across the field of computer science, and to provide additional information in support of his

[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.

conclusions and those of the Appellants. A list of *amici* appears below. Short professional biographies of the *amici* are attached as Exhibit A.

LIST OF AMICI CURIAE[2]

Harold Abelson
Professor of Electrical Engineering and Computer Science,
Massachusetts Institute of Technology

Andrew W. Appel
Professor of Computer Science and Department Chair,
Princeton University

Steven M. Bellovin
Professor of Computer Science,
Columbia University

Matthew A. Blaze
Associate Professor of Computer and Information Science,
University of Pennsylvania

Lorrie Faith Cranor
Associate Professor of Computer Science and of Engineering & Public Policy,
Carnegie Mellon University

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy,
Carnegie Mellon University

Michael J. Freedman
Associate Professor of Computer Science,
Princeton University

Matthew D. Green
Assistant Research Professor of Computer Science,
Johns Hopkins University

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

J. Alex Halderman
Assistant Professor of Electrical Engineering and Computer Science,
University of Michigan

Robert Harper
Professor of Computer Science,
Carnegie Mellon University

Nadia Heninger
Assistant Professor of Computer and Information Science,
University of Pennsylvania

Ronald L. Rivest
Professor of Electrical Engineering and Computer Science,
Massachusetts Institute of Technology

Avi Rubin
Professor of Computer Science and Technical Director of the Johns Hopkins Information University Security Institute,
Johns Hopkins University

Bruce Schneier
Fellow at the Berkman Center for Internet & Society,
Harvard University

Barbara Simons
IBM Research (retired) and Former President of the Association for Computing Machinery (ACM)

Eugene H. Spafford
Professor of Computer Science and Executive Director of Purdue Center for Education and Research in Information Assurance and Security,
Purdue University

Daniel S. Wallach
Professor of Computer Science,
Rice University

INTRODUCTION

It is not *just* metadata.

Telephony metadata reveals private and sensitive information about people. It can reveal political affiliation, religious practices, and people's most intimate associations. It reveals who calls a suicide prevention hotline and who calls their elected official; who calls the local Tea Party office and who calls Planned Parenthood. The aggregation of telephony metadata—about a single person over time, about groups of people, or with other datasets—only intensifies the sensitivity of the information. Aggregated metadata "generates a precise, comprehensive record" of people's habits, which in turn "reflects a wealth of detail about [their] familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. __, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). The call records collected by the government are not *just* metadata—they are intimate portraits of the lives of millions of Americans.

Amici, leading computer and data science experts, write to emphasize that when telephone records are collected in bulk, it is cold comfort that the government is not "listening to [our] telephone calls."[3] The telephony metadata the

[3] *See, e.g.*, Michael Pearson, *Obama: No one listening to your calls*, CNN (Jun 9, 2013), http://www.cnn.com/2013/06/07/politics/nsa-data-mining. ("Nobody is listening to your telephone calls.").

government collects can yield as much information (and oftentimes more) than our actual conversations.

Amici write to reaffirm the views presented in Professor Edward W. Felten's Declaration submitted in the court below;[4] to emphasize that those views are broadly shared throughout the field of computer science; to provide further examples of the revelatory power of metadata and metadata analysis; and to urge this Court to afford sensitive, personal information, like the telephony metadata collected here, the law's full protection.

ARGUMENT

I. METADATA REVEALS HIGHLY PERSONAL AND SENSITIVE INFORMATION.

In an attempt to alleviate concerns about the NSA's call record collection program, Senator Dianne Feinstein, the Chairwoman of the Senate Select Committee on Intelligence, said: "As you know, this is just metadata. There is no content involved."[5] Her position echoes that of President Obama[6] and of the

[4] 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.").

[5] *Transcript: Diane Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program*, Wash. Post (June 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program.

[6] *Transcript of President Obama's Jan. 17 Speech on NSA Reforms, Wash. Post* (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-

government in the court below.[7] Implicit in this view is the suggestion that "content" is sensitive (and its collection worthy of concern), but "metadata" is less so (and should raise no alarms). *Amici* hope to disabuse the Court of this notion. The pool of telephony metadata collected by the government reveals a wealth of deeply personal and intimate information about millions of Americans. Its sensitivity cannot be discounted.

At the outset, it bears emphasizing that there is nothing sacred or particularly profound about defining specific sets of communications data as "metadata" as opposed to "content." In communications technology, "metadata" is often defined by what it is not: it is not the "content" (or "payload") of a communication. Although the law may try to draw hard and fast distinctions between the two, *see, e.g., Smith v. Maryland*, 442 U.S. 735, 741 (1979), the reality is far murkier and typically depends on context. A change in technical protocols or standards can cause information traditionally regarded as metadata to be treated as content, and vice-versa. But the task here is not to define "metadata," nor do *amici* believe it practical or useful to do so in a categorical way. Rather, this brief will only discuss

---

9556-4a4bf7bcbd84_story.html. *(*"Let me repeat what I said when this story first broke. This program does not involve the content of phone calls or the names of people making calls. Instead, it provide [*sic*] a record of phone numbers and the times and length of calls, metadata . . . .").

[7] Gov. Brief at 24-30, *ACLU v. Clapper*, No. 13-3994 (WHP) (S.D.N.Y. Oct. 1, 2013), ECF No. 61.

the *sensitivity* of the information—"telephony metadata"—collected by the government.

Under the call records collection program, the "telephony metadata" collected includes (at least[8]) the following information:

> [C]omprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, Internal Mobile station Equipment Identity (IMEI) number, etc.), International Mobile Subscriber Identity (IMSI) number, trunk identifier, telephone calling card numbers, and time and duration of call.

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *1 n.2 (FISA Ct. Aug. 29, 2013) ("BR 13-109"). IMSI and IMEI numbers are unique numbers that identify the user or device that is making or receiving a call. In conjunction with originating and terminating telephone numbers, for the vast majority of telephone users, these numbers can be used to identify a specific user and device. A "trunk identifier" provides information about how a call is routed through the phone network, revealing general information about the parties' location. The other data

[8] The government has also now admitted to collecting cell site location data on a test basis under Section 215. *See* Letter from Nat'l Sec. Agency Legislative Affairs Office to Senate Select Committee on Intelligence, (Dec. 1, 2010), *available at* http://www.dni.gov/files/documents/1118/CLEANED010.%20RFI%20Response_SSCI%20Gottte...es%201%20December%202010-Sealed.pdf. Additional information may be collected as well.

collected includes the calling card number used (if one is used), and the time and duration of a call.

As explained more fully below, this information reveals deeply personal information about Americans' habits, interests, beliefs, and relationships.

A. Telephony Metadata Reveals Sensitive Information, Even in Limited Quantities.

Although the "telephony metadata" obtained by the government may, on its face, appear innocuous, it is anything but: telephony metadata is revealing—even at the level of individual calls. We will not attempt to catalogue every possible way in which metadata can reveal sensitive information about an individual; however, a few brief examples help illustrate this point.

A call to a hotline or another type of dedicated, single-purpose phone line provides perhaps the starkest demonstration of the power of metadata to reveal deeply private and sensitive information about a single call or caller. An hour-long call at 3 A.M. to a suicide prevention hotline; a thirty-minute call to an alcohol addiction hotline on New Year's Eve; or a fifteen-minute call to a phone-sex service—the "metadata" from those calls, even in the absence of the "content" of

the conversation, still reveals information that virtually anyone would consider exceptionally private.[9]

Setting aside the example of hotlines, disclosure of metadata from even a few calls can yield equally sensitive information about a caller. For example: a person makes a series of calls—first, to an HIV testing service; then, a doctor; and then, an insurance company. A likely narrative emerges—an individual coping with a new diagnosis of HIV—that is apparent even without examining the content of any communication.

The revelatory nature of even a relatively limited sample of call records is not merely hypothetical. In one short-term study of only a few months of mobile telephony metadata, researchers identified one plausible inference of a subject obtaining an abortion; one subject with a heart condition; one with multiple sclerosis; and one owner of a specific brand of firearm.[10]

As these examples illustrate, metadata from even a tiny sample of calls can provide an intimate lens into a person's life.

---

[9] Indeed, metadata about a single call can reveal *more* information than the "content" of the call itself. For example, many wireless telephone companies allow subscribers to donate to charities by sending a text message to a specified "short code," corresponding to the charity. *See* Felton Decl. ¶¶ 43-45. The metadata about these texts reveals that the subscriber has donated to a specific charity or cause, while the content of the message contains at most a donation amount. *Id.* ¶ 45.

[10] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2013), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata.

B. In the Aggregate, Telephony Metadata Is Even More Revealing.

While telephony metadata is revealing, even in limited samples, it is even more so in the aggregate. Indeed, and although seemingly counterintuitive, telephony metadata may actually be *more* informative and revealing than the "content" of conversations, especially when collected *en masse*. This is so for two reasons: first, the aggregation of metadata can reveal context beyond what is revealed in a conversation.[11] Second, the structured nature of telephony metadata lends itself more readily to powerful data analysis.

As an initial matter, there can be no dispute that the quantity of telephony metadata collected under the program is vast. *See* BR 13-109, at *1 (noting that the government obtains "a very large volume of each company's call detail records"). The government apparently collects the metadata on a daily basis for all calls originating or terminating in the United States and carried by the nation's three largest telecommunication carriers.[12] NSA then retains this data for five years.[13]

---

[11] *See* Matt Blaze, *Phew, NSA is Just Collecting Metadata. (You Should Still Worry)*, Wired (Jun. 19, 2013), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again ("Metadata is our *context*. And that can reveal far more about us—both individually and as groups—than the words we speak.").

[12] *See* Siobhan Gorman, *et al.*, *U.S. Collects Vast Data Trove*, Wall St. J. (June 7, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922.

[13] *Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies* 97 (2013) ("President's Review Grp."), *available at*

Thus, even under extraordinarily conservative estimates, the government maintains a database of at least billions of call records containing the details of the most sensitive, intimate, and personal aspects of the lives of millions of Americans.

Once such a large database of telephony metadata is compiled, the government is capable of discerning patterns of sensitive information using relatively unsophisticated methods of analysis. Aggregation demonstrates how metadata provides context and information that is not always apparent from the "content" of a communication. Again, although impossible to comprehensively describe the ways telephony metadata reveals private information, two simple examples from Professor Felten's declaration demonstrate the sensitivities associated with aggregation of just one individual's metadata.

First, "[t]wo people in an intimate relationship may regularly call each other, often late in the evening. If those calls become less frequent or end altogether, metadata will tell us that the relationship has likely ended as well—and it will tell us when a new relationship gets underway." Felten Decl. ¶ 49. Likewise, "a single telephone call to a bookie may suggest that a [person] . . . plac[ed] a bet, [but] analysis of metadata *over time* could reveal that the person has a gambling

---

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

problem, particularly if the call records also reveal a number of calls made to payday loan services." *Id.* ¶ 53.

Like its revelatory power for particular individuals, aggregated telephony metadata allows analysts to create "social graphs" that map the network of connections between individuals and social groups. Using aggregated metadata, an analyst could determine the membership, structure, or participants in an organization like ACLU, or a political party like the Tea Party, or social movement like Occupy Wall Street. Similarly, analysis of telephony metadata over time could provide an estimate of the number of people attending a particular church or political meeting and can map the associations of individuals, revealing friendships, business relationships, and social and political connections.[14]

Finally, the metadata acquired through the government's program is particularly revealing because it is uniformly structured which, in turn, facilitates its processing by powerful data-mining programs. Telephone, IMSI, and IMEI numbers are standardized and expressed in a fixed and predictable format; times,

[14] Analysts can also apply algorithms designed to look more systematically for correlations as well as abnormalities in large sets of metadata. For example, the sociologist Kieran Healy transcribed data compiled by the historian David Hackett Fischer regarding the membership of 260 men in seven Boston-area organizations just prior to the Revolutionary War. Kieran Healy, *Using Metadata to Find Paul Revere* (June 9, 2013), http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere. Using relatively unsophisticated social network analysis to visualize the connections between the men, Healy identified Paul Revere as a central figure in the Boston organizations. *Id.*

dates, and durations of calls are also stored in particular, standardized ways. This standardization and predictability make the data simple to aggregate, store, and analyze using powerful data analysis programs.[15]

Structured data, such as telephony metadata, is ideally suited for analysis using automated data mining, machine learning, and link-analysis tools. Advances in data storage capacity over the past thirty years have made the maintenance of vast troves of data—like five years of calling information on millions of Americans—trivial. The expansion in storage capacity has lead to a parallel growth in the sophistication of computing tools for the analysis of large datasets. These tools can identify patterns and relationships among the data, in turn revealing personal details, habits, and behaviors.

Employing these tools, researchers have been able to mine large pools of metadata, yielding observations of an even deeper and more revealing nature. Professor Felten's declaration recites a number of such studies: "Researchers have discovered that individuals have unique calling patterns, regardless of which

[15] In contrast, the content of a given telephone conversation is far more unstructured. Human speech is not mechanical, and its myriad variations make it more difficult for computers to accurately process. Although voice-recognition software has made significant advances, it is still a difficult, time-consuming, and error-prone process. And, even if the *transcription* process is accurate, the *meaning* of a conversation must still be deciphered. Natural language processing remains an imperfect process, and computer programs have only recently begun to seriously grapple with interpreting figures of speech, sarcasm, innuendo, and other qualities common to everyday human speech.

telephone they are using,[16] . . . developed algorithms capable of predicting whether the phone line is used by a business or for personal use,[17] identified callers by social group (workers, commuters, and students) based on their calling patterns,[18] and even estimated the personality traits of individual subscribers." Felten Decl. ¶ 61. Other research has shown that it is possible to automatically identify whether an individual is in a relationship and, if so, with whom, solely based on telephone metadata pattern analysis.[19]

"Machine learning" is another powerful technique that has matured in the past two decades using simple statistical models and large datasets to sort complex but well-organized datasets (such as metadata) into simple categories.[20] Machine learning is potent not only because it can predict sensitive facts about people captured in a dataset, but also because it can accurately estimate these facts for

---

[16] Corrina Cortes, *et al*., *Communities of Interest*, AT&T Shannon Research Labs, *available at* http://www.research.att.com/~volinsky/papers/portugal.ps.

[17] Haim Kaplan, *et al*., *Just the Fax – Differentiating Voice and Fax Phone Lines Using Call Billing Data*, AT&T Labs, http://bit.ly/19Aa8Ua.

[18] Corinna Cortes & Daryl Pregibon, *Giga-Mining*, AT&T Labs-Research, http://bit.ly/153pMcI.

[19] Mayer & Mutchler, *supra* note 10.

[20] Indeed, machine learning protects our computers against viruses and sorts the spam out of our inboxes. *See Machine Learning for Antivirus Software*, About Data Mining (Apr. 24, 2013), http://www.aboutdm.com/2013/04/machine-learning-for-anti-virus-software.html; *Bayesian Spam Filtering*, Wikipedia https://en.wikipedia.org/wiki/Bayesian_spam_filtering.

every single person in the dataset. Metadata classifiers are an especially potent method for analyzing bulk records of the sort obtained under this program.

In sum, the metadata collection program operated by the government is a far cry from the limited capabilities of the pen register, used to track a single number for a matter of days, that the Supreme Court addressed in *Smith*. *See* 442 U.S. at 737. Metadata collected about one person over a long period of time—here the government claims to be keeping the information for at least five years—is more revealing than over a short one; and the aggregation of data about many people—again the government is collecting all metadata from at least several large telephone carriers—is yet more revealing, particularly with respect to previously unrevealed connections between individuals. This information should be afforded the law's highest protection.

C. Creating a Trail of Sensitive Metadata Is an Unavoidable Byproduct of Modern Life.

Nor can the collection of telephony metadata be considered in a vacuum. Looking beyond telephone records demonstrates the great risk to privacy in accepting the government's proffered bright line between "content" and "metadata."[21] Even without the contents of communications, the government can,

[21] Indeed, and regardless of the wisdom of the content/non-content distinction for telephony, its application to other kinds of data is not straightforward. For example, a website URL entered by a user could be

by collecting and aggregating large amounts of metadata, potentially learn or infer much private information about individuals. This is not surprising—metadata is truly ubiquitous.

Individuals create metadata about themselves as a byproduct of simply existing in a digital world. Metadata is generated through the innumerable and near-continuous digital transactions and interactions attendant to modern life. A report by the National Academy of Sciences on privacy and national security cataloged the forms of metadata and data created about individuals, including:

> financial transactions, medical records, travel, communications, legal proceedings, consumer preferences, Web searches, and, increasingly, behavioral and biological information. This is the essence of the information age—it provides us with convenience, choice, efficiency, knowledge, and entertainment; it supports education, health care, safety, and scientific discovery. Everyone leaves personal digital tracks in these systems whenever he or she makes a purchase, takes a trip, uses a bank account, makes a phone call, walks past a security camera, obtains a prescription, sends or receives a package, files

---

considered a form of metadata, since it is part of a routing request by the user to receive the contents of the website located at the URL address. Yet, quite obviously, the URL itself conveys information about the contents of the site. Just as dialing the San Francisco Suicide Prevention hotline can reveal information about the caller's conversation, so too can visiting the hotline's online live chat page, http://www.sfsuicide.org/get-help/livechat. For further discussion of the technical nuance required to define metadata, *see* Steven M. Bellovin, *Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the § 215 and § 702 Surveillance Programs* 5-7 (July 31, 2013), *available at* https://www.cs.columbia.edu/~smb/papers/PCLOB-statement.pdf.

> income tax forms, applies for a loan, e-mails a friend, sends a fax, rents a video, or engages in just about any other activity.[22]

Because of the ubiquity and diversity of the data generated by individuals, estimates of scale are difficult to generate. By way of example, the New York Times reported that under an NSA program, the Agency is equipped to collect 94 different metadata "entity types" for a total of 20 billion "record events" each day.[23] Crucially, nearly all of this metadata is created as a result of an individual's interactions with third parties. As a result, the metadata almost universally resides with these third parties; telecommunications and Internet service providers retain Internet routing information, location data, and other browsing data, while banks store financial records, retailers store credit card transaction data, and so on. In addition, the types of information created in Internet communications continues to grow; for example, when the transition to Internet Protocol Version 6 is completed, "web communications will include roughly 200 data fields, in addition to the underlying content."[24]

---

[22] Nat'l Research Council of the Nat'l Acad. of Sci., *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* 3 (2008).

[23] James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times (Sep 28, 2013), *available at* http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html.

[24] President's Review Grp. at 121.

It is very difficult, and in practice often impossible, for an individual to avoid creating metadata or to disguise one's particular digital traces. As Professor Felten's declaration describes, technologies exist to encrypt or otherwise protect the contents of communications. Felten Decl. ¶¶ 31-33. However, the metadata about these communications is much harder to obscure. Although some tools, most notably the Tor Project, seek to hide metadata trails on the Internet, these tools are imperfect and do not yet work for real-time communication. *Id.* ¶¶ 34-35.

And, just as the aggregation and analysis of telephony metadata is more revealing than a single call record, the analysis of other sets of metadata is likewise more revealing in the aggregate. As with call records, other forms of metadata are usually stored in formats that permit efficient aggregation and bulk analysis.

For example, while telephone records are a common means to produce social graphs, other metadata can be useful for this purpose as well. A recent project at MIT Media Lab called Immersion accesses volunteers' email metadata and produces a detailed visualization of their social graph.[25] Based on little more than intuition and common sense, someone viewing a volunteer's user patterns can make educated guesses about which people are central to the volunteer's professional, romantic, and social life. Similarly, two studies of social graph

[25] *See* Immersion, https://immersion.media.mit.edu ("Immersion collects only the metadata (*From, To, Cc* and *Timestamp*) of emails. Immersion does not access the subject or body of any of your emails.")

records from Facebook have shown that it is easy to predict sensitive facts about people's personal lives, such as their sexual preferences, from such metadata.[26]

Like telephony metadata, the analysis of other types of metadata can also lead to predictive insight about individuals' future behavior or private information that they have not shared publicly. Location data, created by mobile devices as they connect to cell towers, has been shown to be a particularly rich source for predictive inference. In one study involving location data, researchers developed a model to accurately guess individuals' future movements based on the movements of their friends.[27] Another study presented a predictive model for ethnicity and relationship status based solely on location.[28] A third found that the correlation of

---

[26] *See* Carter Jernigan and Behram Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, First Monday (Oct. 5, 2009), http://firstmonday.org/article/view/2611/2302; Michael Kosinski, *et al*., *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l. Acad. Sci 5803 (2013), *available at* http://www.pnas.org/content/early/2013/03/06/1218772110.abstract. The patterns of relationships exposed by Facebook friendships and patterns of calling or texting are likely to have very similar revelatory structures.

[27] Eunjoon Cho, *et al*., *Friendship and Mobility: User Movement In Location-Based Social Networks* (2011), *available at* http://roke.eecs.ucf.edu/Reading/Papers/Friendship%20and%20Mobility%20User%20Movement%20In%20Location-Based%20Social%20Networks.pdf.

[28] Yaniv Altshuler, *et al*., *Incremental Learning with Accuracy Prediction of Social and Individual Properties from Mobile-Phone Data* (2012), *available at* http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6406354&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6406354.

as few as four points in time and place were enough to positively identify nearly all individuals in a location dataset.[29]

Similarly, retailers use predictive models based on metadata about customers' purchasing history. In a well-known example, Target developed a model to identify shoppers who were likely in their second trimester of pregnancy based solely on purchases of items like lotion, cotton balls, and vitamin supplements, in order to send them relevant offers.[30] The New York Times reported that the father of a pregnant teenaged girl first learned of his daughter's pregnancy when she received coupons from Target for baby clothes.[31] More prosaically, providers like Amazon and Netflix use data mining and machine learning algorithms to make accurate recommendations to their customers.

As these examples show, metadata is a byproduct of our modern lives. Any decision about the legal protection afforded telephony metadata will have broad privacy effects. Thus, the ubiquity and revealing nature of these other forms of metadata cannot be ignored when deciding what legal protections are appropriate to apply to the metadata at issue here.

---

[29] Yves-Alexandre de Montjoye, *et al.*, *Unique in the Crowd: The Privacy Bounds of Human Mobility* (2013), *available at* http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.

[30] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[31] *Id.*

II. THE GOVERNMENT'S LIMITATIONS ON METADATA COLLECTION AND USE DO NOT MITIGATE THE PRIVACY CONCERNS.

As a final point, *Amici* seek to address the practical significance of the government's claimed limitations on its collection and use of telephony metadata.

Most prominently, the government claims that the fact that it does not collect the names of those associated with the telephone numbers it collects is a privacy safeguard. It is not. The additional step of associating a name with an individual's metadata is trivial. First, the government, like all Americans, has ready access to public and commercial databases that match telephone numbers to actual names.[32] The government also has a number of legal tools, such as criminal subpoenas and National Security Letters, at its disposal to compel production of a phone subscriber's name. *See* 18 U.S.C. §§ 2703, 2709.

More generally still, a significant body of research has demonstrated that so-called "anonymized" datasets, including call records,[33] movie viewing habits,[34] and

---

[32] *See, e.g.*, Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA's Got Your Number* (Dec. 23, 2013), http://webpolicy.org/2013/12/23/metaphone-the-nsas-got-your-number (discussing identifying phone numbers using public and commercially available databases).

[33] Hui Zang & Jean Bolot, *Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study*, (2011), *available at* http://paloalto.thlab.net/uploads/papers/Mobicom_2011_-_Anonymization_of_location_data_does_not_work_-_Zang_Bolot.pdf.

[34] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1720-22 (2010).

anonymous social network users[35] can often be re-identified using statistical analysis. It is practically impossible to reliably anonymize a set of metadata where the data retains enough elements to distinguish among the anonymized individuals.[36] Ultimately, the absence of names from the call records database provides no meaningful privacy enhancement.

Additionally, the government suggests the intrusiveness of the call records program is limited because searches of the call records databases are conducted only when there is reasonable, articulable suspicion that a number is associated with international terrorism. *See* Order at 3, *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, No. BR 14-01 (FISA Ct. Feb. 5, 2014) ("BR 14-01").[37] A full understanding of the agency's process for searching the database undermines its claim.

First, a single search of the call records database has the capacity to sweep in thousands—if not millions—of Americans' call records. As the Privacy and Civil

---

[35] Gilbert Wondracek, *et al*., *A Practical Attack to De-Anonymize Social Network Users* 2010), *available at* http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5504716&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5504716.

[36] *See* Arvind Narayanan & Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information*," 53 Communications of the ACM 24, 24-26, (2010), *available at* http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf.

[37] *Available at* http://www.uscourts.gov/uscourts/courts/fisc/br14-01-order.pdf.

Liberties Board (PCLOB) explained, after starting with a single "seed" telephone number, the NSA's software:

> searches the records obtained by the agency under Section 215 and returns those records that are within one "hop" of the seed (*i.e.*, all of the telephone numbers directly in contact with the seed). The analyst may then review the telephone numbers found to be in contact with a first-hop number (*i.e.*, within two hops of the seed) and the telephone numbers found to be in contact with a second-hop number (*i.e.*, within three hops of the seed).[38]

Thus, a single search extends broadly and can affect large numbers of Americans' call records. As PCLOB noted, if "a seed number has seventy-five direct contacts . . . and each of these first-hop contact has seventy-five new contacts of its own," then each query would yield 5,625 telephone numbers.[39] If "each of those second-hop numbers has seventy-five new contacts of its own, a single query would result in a batch of calling records involving over 420,000 telephone numbers."[40] Ultimately, this is likely a conservative estimate: because many individuals are linked together through certain specific and well-known numbers, a

[38] Privacy and Civil Liberties Oversight Bd., Report on the Telephone Records Program 28-29 (Jan. 23, 2014) ("PCLOB Report"), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. The government has now modified its search procedures to only use two "hops," rather than three. *See* BR 14-01 at 4.

[39] PCLOB Report at 29.

[40] *Id*.

single query can sweep in far more numbers than the above estimate suggests.[41] For example, if a "seed" number called a company's customer service hotline, then every other person to contact that customer service line would come within the NSA's search results. Even if the NSA "only" performs 300 of these queries annually,[42] an exceedingly high number of Americans' call records will likely be swept into the NSA's searches.

Second, metadata responsive to an NSA search is then placed into the agency's "corporate store," where the data is not subject to the FISC-imposed limitations on search.[43] Rather, the NSA may apply the "full range" of signals analytic tradecraft to *all* records within the "store."[44] There is no reason to suspect the NSA does not apply powerful algorithmic analyses, to these stored records.

Thus, neither the absence of names nor the limitation on the initial search provides meaningful privacy protections for the sensitive information on millions of Americans contained within the government's repositories.

---

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

[42] *See* President's Review Grp. at 102.

[43] PCLOB Report at 30. By PCLOB's estimate, this "corporate store" contains records involving over 120 million telephone numbers.

[44] *Id*.

CONCLUSION

As described above, it is not *just* metadata. The massive quantity of data the government has collected provides a window into the thoughts, beliefs, traits, habits, and associations of millions of Americans. The Court should reject any contrary suggestion.

Given the detailed portrait that can be drawn from metadata alone—and given the especially revealing nature of large quantities of metadata—the collection of this sensitive information requires the highest protection of law and the Constitution.

Dated: March 13, 2014

Respectfully submitted,

/s/ Cindy Cohn
Cindy Cohn
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amici Curiae

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 Amicus Curiae In Support Of Appellee complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,351 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 2011, in 14 point Times New Roman font.

Dated: March 13, 2014

Respectfully submitted,

/s/ *Cindy Cohn*
Cindy Cohn

EXHIBIT A

Short Biographies of *Amici*

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 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*.

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 J. 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*.

Michael J. Freedman is an Associate Professor in the Computer Science Department at Princeton University. A 2011 Alfred P. Sloan Foundation Fellow, he received the 2011 Presidential Early Career Award for Scientists and Engineers (PECASE). Professor Freedman primarily researches on distributed systems, networking, and security. His publications include *Tarzan: A Peer-to-Peer Anonymizing Network Layer* and *The Free Haven Project: Distributed Anonymous Storage Service*.

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.

Nadia Heninger is an assistant professor in the Computer and Information Science department at the University of Pennsylvania. Her research interests include computer security, cryptography, and privacy-enhancing technologies. Recent publications include *Optimally Robust Private Information Retrieval*" and *Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices*.

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*.

Bruce Schneier is a Fellow at Harvard Law School's Berkman Center for Internet & Society and a Program Fellow at the New America Foundation's Open Technology Institute. A security technologist, Mr. Schneier regularly contributes to The Guardian and Wired Magazine and has published several books including *Applied Cryptography*, *Cryptography Engineering*, and *Secrets and Lies: Digital Security in a Networked World*.

Barbara Simons is retired from IBM Research and a former President of the Association for Computing Machinery (ACM), the world's largest educational and scientific computing society. 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 ACM and of the American Association for the Advancement of Science, she has received numerous awards, including the Computing Research Association Distinguished Service Award and the Electronic

Frontier Foundation Pioneer Award. She is a member of the Board of Advisors of the U.S. Election Assistance Commission. She co-authored the recently published *Broken Ballots: Will Your Vote Count?* and is Board Chair of Verified Voting.

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*.