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,

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,

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Eunjoon Cho, ., (2011) http://roke.eecs.ucf.edu/Reading/Papers/Friendship%20and%20Mobility%20User%20Movement%20In%20Location-Based%20Social%20Networks.pdf....19
!
Haim Kaplan, .,

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
!

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

write to reaffirm the views presented in Professor Edward W. Felten's Declaration submitted in the court below;[4]

the 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

the conversation, still reveals information that virtually anyone

B.

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 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." ¶ 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, a

Metadata classifiers are an especially potent

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 is very difficult, and in practice often impossible, for an individual to

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, t

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

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

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

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 (., 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 (., within two hops of the seed) and the telephone numbers found to be in contact with a second-hop number (., 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

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 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] , Jonathan Mayer & Patrick Mutchler, (Dec. 9, 2013), http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop.

[42] 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]

CONCLUSION

As described above, it is not 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,

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

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

and

semantics, and compilers. His publications include

and .

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

, , and

and

communications field. His publications include

and

.

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

and

.

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

and

.

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

and .

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-

Director of the USENIX Association from 2000 to 2004 and a recipient of the

issues include web browsers and servers, peer-to-peer systems, smartphones, and voting machines. His publications include

and

.