May 11, 2015

Majority Leader Mitch McConnell
United States Senate

Minority Leader Harry Reid
United States Senate

Chairman Charles Grassley
Senate Judiciary Committee

Chairman Richard Burr
Senate Select Committee on Intelligence

Ranking Member Patrick Leahy
Senate Judiciary Committee

Vice Chairman Dianne Feinstein
Senate Select Committee on Intelligence

We, the undersigned, write to oppose any data retention mandates that would require any company to retain user data for a defined length of time. Indiscriminate data retention mandates intrude upon privacy, chill freedom of expression and association, needlessly expose users to risks of data theft or misuse, and significantly increase operating costs for small and large businesses. For more information, please see the attached letter, signed by nearly two dozen noted technological experts and academics in the fields of data security, data protection, and privacy.

Respectfully,

Access
Advocacy for Principled Action in Government
American Library Association
Center for Democracy and Technology
Constitutional Alliance
The Constitution Project
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
Electronic Frontier Foundation
Fight for the Future
New America's Open Technology Institute
OpenTheGovernment.org
Silent Circle
Sonic
TechFreedom

Jon Callas
Chip Pitts

attachment: https://s3.amazonaws.com/access.3cdn.net/3cfd02d301093805f9_v3m6bxrzz.pdf

September 18, 2014

Chairman Dianne Feinstein
U.S. Senate Select Committee on Intelligence
Washington, DC 20510

Vice Chairman Saxby Chambliss
U.S. Senate Select Committee on Intelligence
Washington, DC 20510

Chairman Patrick J. Leahy
U.S. Senate Committee on the Judiciary
Washington, DC 20510

Ranking Member Chuck Grassley
U.S. Senate Committee on the Judiciary
Washington, DC 20510

Dear Chairman Feinstein, Vice Chairman Chambliss, Chairman Leahy, and Ranking Member Grassley,

We write to urge you to pass the USA FREEDOM Act without a data retention mandate. At the moment, the bill introduced by Senator Leahy takes steps to improve the legitimacy, transparency, accountability, and proportionality of U.S. intelligence practices.[1] Any mandate requiring internet service providers or phone companies to retain customer data, including metadata, for any length of time would undermine this progress.

As we set out below, data retention mandates deputize private corporations as government agents, bringing their conduct within the ambit of constitutional regulations without improving security. Moreover, a mandate to gather and retain vast amounts of personal data on a completely indiscriminate basis would violate Fourth Amendment rights recognized by the Supreme Court,[2] chill freedom of expression and association, and needlessly expose consumers to risks of data theft or misuse.

Repercussions and Risks

Judges and scholars have highlighted the grave constitutional implications of public-private collusion to gather, store, and analyze large quantities of personal and consumer data. In an almost 70-page opinion, Judge Richard Leon held that the expectation of privacy in metadata is not only reasonable, but "very significant."[3] As a result, the "systematic and high-tech collection and retention of personal data" violates the Fourth Amendment's basic purpose to protect against indiscriminate and arbitrary invasions of

[1] *See* S. 2685, 113th Cong. (2014).
[2] *See* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012).
[3] Klayman v. Obama, 957 F. Supp. 2d 1, 32 (D.D.C. 2013).

privacy by licensing a twenty-first century version of general warrants.[4] Judge Leon's judgment echoes concerns advanced by Professors David Gray and Danielle Citron, who argue that personal privacy must be protected from the "indiscriminate and invasive governmental practices that are characteristic of a surveillance state."[5] Animated by comparable concerns, courts and legislatures around the world have rejected data retention mandates on similar grounds.[6]

By infringing on privacy, data retention chills freedom of expression, association, and the press.[7] Data related to phone and email times, dates, locations, and recipients can reveal a tremendous amount of personal information, including one's occupation, religion, race, sexual orientation, medical condition, or political affiliation.[8] Easy access to this wealth of information makes it less likely that individuals and groups will communicate freely with each other. Civic groups, religious institutions, and advocacy organizations have already observed direct impacts on their ability to communicate with and serve their members and clients as a result of bulk surveillance.[9] Repackaging surveillance as data retention and delegating responsibility to unwilling agents only perpetuates the harm to ordinary people, treating all Americans as suspected criminals.

---

[4] *Id.* at 39.

[5] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 69 (2013).

[6] *See e.g.*, *The Court of Justice Declares the Data Retention Directive to be Invalid*, CJEU (Apr. 8, 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf; *Czech Constitutional Court Rejects Data Retention Law*, EDRI (Mar. 31, 2011), http://edri.org/czech-decision-data-retention; *German Court Orders Stored Telecoms Data Deletion*, BBC (Mar. 2, 2010, 2:57 PM), http://news.bbc.co.uk/2/hi/europe/8545772.stm; *Bulgarian Court Annuls a Vague Article of the Data Retention Law*, EDRI (Dec. 17, 2008), http://history.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention.

[7] In 2008, the Forsa Institute in Germany found that European data retention laws led individuals to avoid using mobile or online communications in certain circumstances. *Meinungen der Bundesburger zur Vorratsdatenspeicherung*, FORSA INST. (June 2, 2008), http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf. *See also Riley*, 134 S. Ct. at 2490 (discussing the amount of personal information that can be determined from certain types of metadata); *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

[8] In fact, metadata often reveals more than content. *See Continued Oversight of the Foreign Intelligence Surveillance Act, Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 4-12 (2013) (statement of Edward Felten, Professor, Princeton University); 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; Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA's Got Your Number*, WEB POLICY (Dec. 23, 2013), http://webpolicy.org/2013/12/23/metaphone-the-nsas-got-your-number.

[9] *See* First Amended Complaint, First Unitarian Church of Los Angeles v. National Security Agency, No. 3:13-cv-03287 (N.D.C.A. Sept. 10, 2013). For declarations from the organizations that filed suit, see *First Unitarian Church of Los Angeles v. NSA*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa (last visited Sept. 12, 2014).

This erosion of civil liberties is much too high a price to pay for no established security benefit. Bulk surveillance has not been proven to prevent terrorist attacks,[10] nor has it had any demonstrated impact on solving crime.[11] Both the Attorney General and the Director of National Intelligence have conceded that the intelligence community does not need a data retention mandate, arguing that the current version of the USA FREEDOM Act "will accommodate operational needs while providing appropriate privacy protections."[12]

By contrast, a data retention mandate would compromise security. Amassing the personal data of every person in the United States exposes that data to misuse, abuse, breaches,[13] and theft[14] by telecom employees[15] as well as the government—as a recent FISC ruling makes clear.[16] In that ruling, Judge Walton found that extending the time limit on data retention under Section 215 of the USA Patriot Act "would further infringe on the privacy interests of United States persons."[17] The judgment noted that data retention "increases the risk that information about United States persons may be improperly used or disseminated,"[18] especially considering that "the great majority of

---

[10] *See* Peter Bergen, et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AM. FOUND. (Jan. 2011), http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf; *see also Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, PCLOB (Jan. 23, 2014), http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

[11] Jennifer Baker*, German Crime Stats Deal Blow to EU's Data Retention Laws*, CSO (June 9, 2011), http://www.csoonline.com/article/2128756/data-protection/german-crime-stats-deal-blow-to-eu-s-data-retention-laws.html.

[12] Letter from Eric Holder, Attorney General, and James Clapper, Dir. Nat'l Intelligence, to Patrick Leahy, Sen. (Sept. 2, 2014), http://images.politico.com/global/2014/09/04/clapperholderleahyltr.pdf.

[13] For examples of recent breaches, see Dave Lewis, *iCloud Data Breach: Hacking and Celebrity Photos*, FORBES (Sept. 9, 2014), http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos; Shelly Banjo & Danny Yardon, *Home Depot Confirms Data Breach*, WALL ST. J. (Sept. 8, 2014), http://online.wsj.com/articles/home-depot-confirms-data-breach-1410209720.

[14] *See* Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight against Terrorism*, DEP'T OF DEF. (March 2004), https://cdt.org/files/security/usapatriot/20040300tapac.pdf.

[15] *See* Robert Faturechi, *Snowden Leaks Prompt Firms to Focus Cyber Security on Insider Threats*, L.A. TIMES (Aug. 10, 2014), http://www.latimes.com/business/technology/la-fi-tn-insider-threat-def-con-corporate-cybersecurity-20140810-story.html ("Employees can hack their systems to elevate their login credentials or install malware such as keystroke loggers to get around those controls. And the data thieves aren't just being paid by rival companies. A large chunk of in-house bad actors are believed to be getting paid off by organized crime.").

[16] *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, BR-1401 (FISA Ct. 2014), http://www.emptywheel.net/wp-content/uploads/2014/03/14-01_Opinion.pdf.

[17] *Id.* at 11.

[18] *Id.* at 6.

these individuals have never been the subject of investigation"[19] for intelligence purposes.

Along with creating lucrative targets for malicious actors,[20] data retention mandates pose significant costs. Telecom executives have voiced concerns over standardizing their datasets to match government needs.[21] Datasets would have to be held well beyond their business purpose,[22] creating significant liability risks and negative externalities: a company's international reputation would suffer for its association with domestic surveillance regimes,[23] while its energy-wasting datacenters contribute to environmental harms.[24] Ultimately, these costs would be passed onto consumers, detracting from current initiatives to create an affordable and efficient communications infrastructure while hamstringing the United States' global competitiveness and stifling innovation. [25]

Data retention causes adverse impacts on constitutional rights and economic innovation, while increasing data insecurity. Companies must be allowed to minimize retention because, as the Cato Institute put it, "Data destroyed cannot be misused."[26]

Guiding Principles

Mass and indiscriminate data retention is incompatible with privacy and security. Intelligence gathering practices must be necessary and proportionate, as the UN

---

[19] *Id.* at 11.
[20] Nigel Brew, *Telecommunications Data Retention—An Overview*, PARLIAMENT OF AUSTL. DEP'T OF PARLIAMENTARY SERV. (Oct. 24, 2012), http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/1998792/upload_binary/1998792.pdf.
[21] Marcy Gordon & Martha Mendoza, *AT&T, Verizon And Sprint Push Back Against The NSA, Too*, THE HUFF. POST (Mar. 3, 2014), http://www.huffingtonpost.com/2014/03/03/att-verizon-sprint-nsa_n_4891533.html.
[22] *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the Comm. on the Judiciary*, 112th Cong. (2011) (statement of Kate Dean, U.S. Internet Serv. Provider Assoc.).
[23] *Foreign Intelligence Surveillance Act (FISA) Reforms: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. (2014) (statement of Michael Woods, Vice President and Assoc. Gen. Counsel, Verizon Commc'ns).
[24] James Glans, *Power, Pollution, and the Internet*, N.Y. TIMES (Sept. 22, 2012), http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html.
[25] *Comprehensive Revision of Telecommunications (Interception and Access) Act of 1979: Hearing Before the S. Standing Comm. on Legal and Legis. Affairs*, 44th Parliament (2014) (Austl.); President Barack Obama, Remarks by the President at Mooresville Middle School at Mooresville, N.C. (Jun. 6, 2013), http://www.whitehouse.gov/the-press-office/2013/06/06/remarks-president-mooresville-middle-school-mooresville-nc.
[26] James Plummer, *Data Retention: Costly Outsourced Surveillance,* CATO INST. (Jan. 22, 2007), http://www.cato.org/publications/techknowledge/data-retention-costly-outsourced-surveillance.

Human Rights Committee's recent remarks to the U.S. government indicated.[27] Accordingly, the U.S. should look to the principles enshrined in the International Principles on the Application of Human Rights Law to Communications Surveillance.[28] Crafted and endorsed by hundreds of civil society groups, the International Principles reflect the universal understanding that interference with personal privacy is only consistent with human rights when supported by legal authority, triggered by necessity, and tailored to a specific and legitimate aim. Mandatory data retention fails on all counts.[29]

Conclusion

Over the past year, organizations like Target, Neiman Marcus, AOL, Adobe, the Internet Governance Forum, and eBay have experienced major data breaches, affecting millions of people and almost half of all American adults.[30] Mandatory data retention under the USA FREEDOM Act or in any other law will only compound the problem of insecure databases, increasing the vulnerability of consumer data and leading to more large-scale breaches and greater costs down the line. Retention will also corrode civil liberties while threatening the internet's vital role as a trusted space for free expression, innovation, and economic exchange.

Rather than watering down constitutional rights and impairing data security without a demonstrable benefit to national security, Congress should pursue comprehensive reform that protects the privacy of all people. The USA FREEDOM Act can help bring us one step closer to that goal, if it is passed without a data retention provision. We call upon you to reject any proposals mandating data retention or similar approaches, in the USA FREEDOM Act or any future legislation.

Respectfully,[31]

---

[27] *Concluding Observations on the Fourth Periodic Report of the United States of America*, U.N. Human Rights Committee, 110th Sess., March 10–28, 2014, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014).
[28] *International Principles on the Application of Human Rights Law to Communications Surveillance* (May 2014), https://en.necessaryandproportionate.org/text.
[29] *The Right to Privacy in the Digital Age*, U.N. High Comm. for Human Rights, 27th Sess., U.N. Doc. A/HRC/27/37 (June 30, 2014), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.
[30] James Pagliery, *Half of American Adults Hacked this Year*, CNN (May 28, 2014, 9:25 AM), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/index.html.
[31] All institutions are listed for identification purposes only and the signatories do not speak for or on behalf of their respective institutions.

Steven M. Bellovin
Professor
Department of Computer Science
Columbia University

Danielle Keats Citron
Lois K. Macht Research Professor & Professor of Law
University of Maryland School of Law

Joshua Dressler
Distinguished University Professor & Frank R. Strong Chair in Law
Ohio State University Moritz College of Law

Susan Freiwald
Professor of Law
University of San Francisco School of Law

David Gray
Professor of Law
University of Maryland School of Law

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

Woodrow Hartzog
Samford University Cumberland School of Law
Affiliate Scholar
The Center for Internet & Society
Stanford Law School

Peter Jan Honigsberg
Professor of Law
University of San Francisco

Anil Kalhan
Associate Professor of Law
Drexel University School of Law

Margot Kaminski
Assistant Professor
Ohio State University Moritz College of Law
Affiliated Fellow
Information Society Project
Yale Law School

Geoffrey King
Lecturer
University of California, Berkeley

Issa Kohler-Hausmann
Associate Professor of Law
Yale Law School

Arnold H. Loewy
George Killam Professor of Criminal Law
Texas Tech School of Law

Deirdre K. Mulligan
Associate Professor of Law
University of California, Berkeley, School of Information
Co-Director
Berkeley Center for Law and Technology

Paul Ohm
Associate Dean & Associate Professor
University of Colorado Law School

Neil Richards
Professor of Law
Washington University in St. Louis School of Law

Cesare P.R. Romano
Professor of Law & W. Joseph Ford Fellow

Loyola Law School, Los Angeles

Jonathan Simon
Adrian A. Kragen Professor of Law
Faculty Director, Center for the Study of Law & Society
University of California, Berkeley School of Law

Christopher Slobogin
Milton R. Underwood Chair in Law
Director, Criminal Justice Program
Vanderbilt Law School

Katherine J. Strandburg
Alfred B. Engelberg Professor of Law
New York University School of Law

Connie de la Vega
Professor & Academic Director of International Programs
University of San Francisco School of Law

Stephen I. Vladeck
Professor of Law
American University Washington College of Law