August 4, 2015

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW,
Washington, DC 20554

RE: Petition to Repeal 47 C.F.R. § 42.6 ("Retention of Telephone Toll Records")

Dear Secretary Dortch,

We, the undersigned consumer rights, human rights, and civil liberties organizations, along with members of the EPIC Advisory Board, petition the Federal Communications Commission ("FCC") to repeal 47 C.F.R § 42.6 ("Retention of Telephone Toll Records") because the rule requiring mass retention of phone records exposes consumers to data breaches, stifles innovation, reduces market competition, and threatens fundamental privacy rights.[1]

Mass Retention Requirements for Telecommunications Carriers Threatens Consumer Privacy

The FCC's data retention mandate implicates substantial privacy and civil liberties interests for millions of Americans. It states:

> Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.[2]

It is not necessary or effective.[3] It should end.

[1] This is a petition under the Administrative Procedure Act 5 U.S.C. § 553(e) and 47 C.F.R. §§ 1.401(a) – (c).
[2] FCC Retention of Telephone Toll Records, 47 C.F.R. § 42.6.
[3] *Accord* Official Statement, Office of the Director of National Intelligence, Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA Patriot Act (July 27, 2015) http://icontherecord.tumblr.com/post/125179645313/statement-by-the-odni-on-retention-of-data.

In 1985, when data was retained for only six months, the FCC initiated a rulemaking to remove this burdensome record-keeping requirement.[4] In response to the FCC's proposal, the Department of Justice ("DOJ") petitioned the Commission to extend the retention period from 6 to 18 months,[5] claiming "telephone toll records are often essential to the successful investigation and prosecution of today's sophisticated criminal conspiracies . . . ."[6] Telecommunications providers objected to the DOJ's proposal, noting that the elimination of the retention period would permit telephone companies to "develop cost efficient recordkeeping systems."[7] The companies also stated that "a six month retention period would seem adequate for most records."[8] Finally, they said, law enforcement agencies could request that records be maintained "for individuals under investigation without requiring that all toll records be retained."[9] The Department of Justice prevailed. Telephone records were retained, and the privacy interests of American telephone customers were placed at risk.

Many years later, it is abundantly clear that the 18-month data retention rule serves no purpose. As the DOJ itself acknowledged in 2006, "the efficacy of the Commission's current Section 42.6 requirement to meet law enforcement needs has been significantly eroded."[10] The

---

[4] Preservation of Records of Communications Common Carriers, 50 Fed. Reg. 31,395, 31,395 (proposed Aug. 2, 1985) [hereinafter Preservation of Records 1985]. *See also* Preservation of Records of Communication Common Carriers, 28 Fed. Reg. 13,200, 13,209 (Dec. 5, 1963) [hereinafter Preservation of Records 1963] (in which the FCC orders the 6-month retention to provide the "basis of charges to subscribers.").
[5] Preservation of Records 1985, *supra* note 4, at 31,395.
[6] *Id.* at 31,397.
[7] *In the Matter of: Revision of Part 42, Pres. of Records of Commc'n Common Carriers*, 60 Rad. Reg. 2d (P & F) ¶ 1529 at 3 (F.C.C. Aug. 22, 1986) [hereinafter *In the Matter of: Revision of Part 42*].
[8] Preservation of Records 1985, *supra* note 4, at 31,396.
[9] *In the Matter of: Revision of Part 42, supra* note 7, at 5.
[10] Dept. of Justice and Homeland Security, Comment Letter on Notice of Rulemaking In the Matter of Implementation of the Telecommunications Act of 1996, at 10 (Apr. 28, 2006), CC Docket No. 96-115 [hereinafter, DOJ CPNI Petition].

regulation is based on an outdated model since carriers have "moved away from classic billing models, in which charges are itemized," and instead use "non-measured, bundled, and flat-rate service plans," such that "some carriers have claimed that call records under such new plans are not covered by Section 42.6 because they are not 'toll records.'"[11]

Not only is the rule ineffectual in assisting law enforcement, it also stifles innovation and market competition. As explained above, carriers opposed the proposal to retain toll records for 18 months because moving away from toll recordkeeping would allow them to develop more cost efficient recordkeeping systems.[12] Furthermore, the toll recordkeeping is out of sync with the market demands of "bundled" packages that provide consumers with more comprehensive billing structures.[13] And the requirement prevents companies from competing on privacy, which many believe is the market-based solution to the enormous privacy challenge confronting the nation today.[14] These inefficiencies reveal that this program is no longer necessary or reliable in meeting the original goal of "forming basis of charges to subscribers and others"[15] or "supporting successful investigations."[16]

---

[11] *Id.* at 11-12; *See also* Fed. Bureau of Investigation Memorandum Opinion for the General Counsel on Information Under the Elec. Comm. Privacy Act (Nov. 5, 2008) at 6 (explaining the historical definition and difference between "local" and "long distance toll" within the communication industry).

[12] *In the Matter of: Revision of Part 42, supra* note 7, at 3.

[13] *See* DOJ CPNI Petition, *supra* note 10, at 11-12.

[14] *See, e.g.*, Tom Wheeler, Chairman, Fed. Commc'n Comm'n, Remarks at the RSA Conference (Apr. 21, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-333127A1.pdf ("We are also continuing to examine how the concept of cybersecurity intersects with other aspects of the FCC's statutory mission. For instance, the FCC has explicit responsibilities to protect the privacy of data that communications providers collect from their customers in the everyday course of business. Consumers have a right to expect that this information will be protected from disclosure. Failure to do so can have a chilling effect on free expression and the virtuous cycle of network investment and innovation.").

[15] Preservation of Records 1963, *supra* note 4, at 13,209.

[16] *In the Matter of: Revision of Part 42, supra* note 7, at 10.

Mass Retention of Telecommunications Data Implicates Substantial Privacy and Associational Freedom Interests

Section 42.6 requires telecommunication carriers to retain sensitive information on all of their customers, including the name, address, and telephone number of the caller, telephone number called, date, time and length of the call.[17] These telephone records not only show who consumers call and when, but can also reveal intimate details about consumers' daily lives.[18] These records reveal close contacts and associates, and confidential relationships between individuals and their attorneys, doctors, or elected representatives.[19]

Justice Stewart recognized the significant privacy interests implicated through phone surveillance in his dissent in *Smith v. Maryland*. He wrote,

> [t]he role played by a private telephone is . . . vital, and since *Katz* it has been abundantly clear that telephone conversations carried on by people in their homes or offices are fully protected by the Fourth and Fourteenth Amendments. As the Court said in *United States v. United States District Court,* "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[20]

Justice Marshall expressed similar concern when he wrote in *Smith,* "In my view, whether privacy expectations are legitimate within the meaning of Katz depends not on the risks

[17] 47 C.F.R. § 42.6.
[18] *See Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2013) (statement of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University).
[19] *See* Letter regarding Ending Renewal of the Section 215 Bulk Telephony Metadata Program from 28 Privacy & Civ. Liberties Organizations to President Barak Obama and Eric Holder, U.S. Attorney Gen. (June 17, 2014), https://www.epic.org/privacy/Coalition-Ltr-to-End-NSA-Bulk-Collection.pdf; *Mobile Technology Fact Sheet*, PEW RESEARCH CENTER, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/(last visited July 16, 2015) (stating that as of 2014, 90% of American adults own a cell phone).
[20] *Smith v. Maryland*, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting) (quoting *U.S. v. U.S. District Court*, 407 U.S. 297, 313 (1972)).

an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."[21]

Following the decision in *Smith v. Maryland,* the United States Congress took steps to safeguard telephone record information and overturned the Court's decision.[22] The House Committee report that accompanied the Electronic Communications Privacy Act of 1986 explained:

> As a general matter telephone companies maintain a record of calls placed from a telephone for billing purposes. These business records are primarily used by the telephone company for its own purposes. At the federal level the government can legally obtain access to such records based on a grand jury or trial subpoena or through the use of an administrative summons authorizing a specific federal agency to obtain records. Such government access is usually in connection with an ongoing criminal or civil investigation.[23]

The call toll records currently retained under the FCC Section 42.6 are not specifically tailored or limited to a particular investigation; carriers are required to retain data for 18 months for all subscribers. Since 90% of American adults have a cell phone, this equates to sensitive data being retained for nearly every American adult, even when they are under no suspicion of wrongdoing.[24] Such mass retention of sensitive data of the American people, and subsequent access by the government has a chilling effect.

As Justice Sotomayor recently stated in *United States v. Jones*, "[a]wareness that the Government may be watching chills associational and expressive freedoms."[25] And although telephone records may be a useful resource in the investigations of crimes,[26] law enforcement

---

[21] *Id.* at 749.
[22] Electronic Communications Privacy Act, Pub.L. 99-508, codified at 18 U.S.C. 3121 *et seq*. ("General prohibition on pen register and trap and trace device use; exception").
[23] H. REP. NO. 99-647, at 26 (1986) (internal citations omitted).
[24] *Mobile Technology Fact Sheet*, *supra* note 19.
[25] *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[26] DOJ CPNI Petition, *supra* note 10, at 5-6.

agencies could request that records be maintained "for individuals under investigation *without requiring that all toll records be retained*," as carriers have previously suggested.[27] Simply put, "[i]t is simply not possible that every phone record in the possession of a telecommunications firm could be relevant to an authorized investigation."[28]

A federal district court recently found that the bulk collection of telephone "*do*[*es*] implicate the interests of cell phone subscribers when their service providers are producing metadata about their phone communications to the Government . . . ."[29] Similarly, the FCC must recognize the significant privacy interests implicated by retaining toll data. The 42.6 program should end.

The European Court of Justice Struck Down the Data Retention Directive Because It Violated the Fundamental Right to Privacy

The Court of Justice of the European Union has determined that the routine mandated retention of telephone data violates the fundamental right to privacy. The decision is binding on the provision of telecommunications services across the European Union, a market larger than the United States telecommunications market.[30] Echoing views expressed by Justices Stewart, Marshall, and Sotomayor, the Court of Justice found:

> Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life,

[27] *In the Matter of: Revision of Part 42, supra* note 7, at 5 (emphasis added).
[28] Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari at 3, In re EPIC, *cert. denied*, 134 S. Ct. 638 (2013), 2013 WL 3484365.
[29] *Klayman v. Obama*, 957 F.Supp.2d 1, 22 (D.D.C. 2013). *See also Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015) ("The more metadata the government collects and analyzes, furthermore, the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals.").
[30] The EU and US programs differ in two key respects. The EU data retention requirements are typically broader in scope than the data that is lawfully obtained in the US under the FISA. However, EU telephone companies are not required to routinely provide customer information to the government as are US telephone companies.

> permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.[31]

With the decision, the CJEU "made clear that the unbounded retention of telephone records for national security purposes is not necessary, appropriate or proportionate in a democratic society."[32]

The CJEU decision bears on the FCC's continuing the mandate of Section 42.6. The routine compelled retention of telephone records is not necessary or proportionate for a democratic society.

Recent Data Breaches Reveal the Inherent Risks of Maintaining Unnecessary Records

In recent months, there have been a large number of high profile data breaches that illustrate the severity of the risks associated with data retention. For example, in April 2015, the Office of Personnel Management ("OPM") discovered that the personal data of 4.2 million current and former Federal government employees had been stolen. Subsequently in June 2015, OPM discovered that additional information had been compromised: including the background investigation records of current, former, and prospective Federal employees and contractors, totaling 21.5 million individuals.[33]

The FCC itself has brought data breach actions against companies that fail to safeguard the personal information of their customers. The agency recently proposed "a $10 million fine

---

[31] Press Release No 54/14, Court of Justice of the European Union, The Court of Justice Declares the Data Retention Directive to be Invalid (Apr. 8, 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf. Similar views were expressed by Justice Potter Stewart in dissent in *Smith v. Maryland*, 742 U.S. at 746.

[32] *See* Letter Concerning European Court of Justice Opinion on Data Retention and Privacy from Privacy Advocates, to John Podesta, Counsel to the President, and Nicole Wong, Deputy Chief Tech. Officer, Office of Science & Tech. Pol'y (Apr. 16, 2014), http://privacycoalition.org/Priv-Coal-to-WH-on-ECJ-Opinion.pdf.

[33] *Information About OPM Cybersecurity Incidents*, OPM.GOV, https://www.opm.gov/cybersecurity/ (last visited July 16, 2015).

against two telecommunications carriers for failing to protect the personal information of up to 305,000 consumers."[34] According to the FCC:

> The Commission alleges that the carriers' failure to reasonably secure their customers' personal information violates the companies' statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act, given that their data security practices lacked "even the most basic and readily available technologies and security features and thus creates an unreasonable risk of unauthorized access."[35]

The risk of breaches will increase as more sensitive data is retained.[36] The best strategy to reduce the risk of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset.[37] Furthermore, the risk of a breach can be reduced by deleting call records after they are no longer needed for billing or dispute purposes, or if law enforcement has not lawfully requested retention of call records for specific individuals. Section 42.6 stands in opposition to a critical strategy to safeguard consumer privacy.

Request for Agency Action

The mandatory retention of call toll records under Section 42.6 violates the fundamental right to privacy. It exposes consumers to data breaches, stifles innovation, and reduces market competition. It is outdated and ineffective. It is not necessary or proportionate for a democratic society.

The public should be given the opportunity to comment on the ongoing necessity of this provision in light of its ineffectiveness and the corresponding privacy threats. Further, the

---

[34] Press Release, Fed. Trade Commission, FCC Plans $10 Million Fine for Carriers that Breached Consumer Privacy (Oct. 24, 2014) https://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy.
[35] *Id.*
[36] *A Bill to Require Greater Protection or Sensitive Consumer Data and Timely Notification in Case of Breach*: Hearing on H.R. ___ *Before the Subcomm. on Commerce, Manufacturing, & Trade, H. Comm. on Energy & Commerce*, 112th Cong. 3 (2011) (statement of Marc Rotenberg, Executive Director, EPIC).
[37] *Id.* at 4.

undersigned organizations and privacy experts petition the FCC to repeal 47 C.F.R. § 42.6 in its entirety.

Contact: Marc Rotenberg and Khaliah Barnes, EPIC 1718 Connecticut Ave., NW, Suite 200, Washington, DC 20009. +1 202-483-1140.

Respectfully submitted,

Organizations

Access
American-Arab Discrimination Committee (ADC)
American Consumer Institute for Citizen Research
American Library Association
Benton Foundation
Bill of Rights Defense Committee
Campaign for Liberty
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Citizen Outreach
Constitutional Alliance
Consumer Action
Consumer Watchdog
Council on American-Islamic Relations
Cyber Privacy Project
Defending Dissent Foundation
DownsizeDC.org, Inc.
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Freedom of the Press Foundation
Government Accountability Project
Liberty Coalition
Niskanen Center
PEN American Center
Privacy Rights Clearinghouse
Restore the Fourth
TechFreedom

EPIC Advisory Board

Alessandro Acquisti
David Banisar
Ann Bartow
Rod Beckstrom
Colin Bennett
Danielle Citron
Simon Davies
Whitfield Diffie
Cynthia Dwork
Dave Farber
Addison Fischer
David Flaherty
A. Michael Froomkin
Deborah Hurley
Ian Kerr
Chris Larsen
Harry Lewis
Anna Lysyanskaya
Gary T. Marx
Mary Minow
Eben Moglen
Pablo Molina
Peter G. Neumann
Helen Nissenbaum
Deborah Peel
Stephanie Perrin
Chip Pitts
Ron Rivest
Pam Samuelson
Bruce Schneier
Barbara Simons
Nadine Strossen
Frank Tuerkheimer
Sherry Turkle

By:

Marc Rotenberg
EPIC President
Electronic Privacy Information Center
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
(202) 483-1140

For Petitioners
Filed August 4, 2015