May 10, 2016

Senator Jeff Flake, Chairman
Senator Al Franken, Ranking Member
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Hearing on "Examining the Proposed FCC Privacy Rules"

Dear Chairman Flake and Ranking Member Franken:

We write to you regarding the upcoming hearing on "Examining the Proposed FCC Privacy Rules." Your attention to this issue is critical, as threats to the privacy of online communications from Internet-based services are increasing dramatically.[1]

EPIC is a non-profit research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. We have worked closely with both the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC") for more than twenty years to safeguard consumer privacy. In EPIC's view, the FCC's proposed privacy rules are too narrow, but the FTC lacks adequate authority to safeguard consumer privacy. For the reasons set out below, we therefore urge the Senate Judiciary Committee to develop a comprehensive approach to privacy protection.

The Scope of the Problem

The unregulated collection of personal data has led to staggering increases in identity theft, security breaches, and financial fraud.[2] Communications data is collected and used for purposes never intended by the consumer. Additionally, the use of personal information to make automated decisions based on secret, imprecise, and oftentimes impermissible factors presents

[1] Associated Press, *Comcast Agrees to Pay $33 Million in California Privacy Breach*, LA TIMES (Sep. 18, 2015), http://www.latimes.com/business/la-fi-comcast-california-settlement-20150918-story.html; Ryan Knutson, *Verizon to Pay $1.35 Million to Settle FCC Probe of 'Supercookies'*, WALL ST. J. (Mar. 7, 2016), http://www.wsj.com/articles/verizon-to-pay-1-35m-to-settle-fcc-probe-of-supercookies-1457372226; Cecilia Kang, *Google Tracks Consumers' Online Activities Across Products, and Users Can't Opt Out*, WASH. POST (Jan. 24, 2012), https://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html; Tracey Lien, *Facebook Will Have to Face Lawsuit Over Scanning of Users' Messages*, LA TIMES (Dec. 24, 2014), http://www.latimes.com/business/technology/la-fi-tn-facebook-messages-lawsuit-20141224-story.html.

[2] *See, e.g.,* Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* (Feb. 2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.

clear risks to fairness and due process.[3] Far too many organizations collect detailed personal information and use it with too little regard for the consequences.

The United States has been slow to update its privacy laws, and companies have been reluctant to implement privacy enhancing technologies. Thus, neither an appropriate legal nor technical framework has been implemented to consistently safeguard individual privacy. Many of the current laws are no longer suited to protect the privacy of American consumers in the digital age. It is critical that privacy protections for communications keep pace with advances in technology.

The American public supports updating U.S. privacy safeguards. According to a recent study by the Pew Research Center, 91% of Americans believe they have lost control of how companies collect and use their personal information.[4] The overwhelming majority want that control, with 74% of Americans saying it is "very important" to control who gets their information and 65% saying it is "very important" to control what information gets collected.[5] Americans also consistently express a lack of confidence in the privacy and security of their online communications.[6]

The consequences of inadequate data protection in the U.S. implicate the interests of U.S. consumers and businesses.[7] The competitiveness of American technology companies in the global market also requires strong U.S. legal protections for communications privacy.[8] Communications officials in Europe are reviewing the "ePrivacy Directive" as users of Internet-based services in Europe face challenges similar to those faced by American consumers.[9] A

---

[3] *See* Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion?* (Jan 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[4] Lee Rainie, *The State of Privacy in America: What We Learned*, PEW RESEARCH CENTER (Jan. 20, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

[5] *Id*.

[6] *Id.*

[7] *See* Marc Rotenberg, Testimony before the U.S. House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (Nov. 3, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.

[8] *See* Aarti Shahani, *A Year After Snowden, U.S. Tech Losing Trust Overseas*, NPR (June 5, 2014), http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas; Claire Caine Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, NY TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[9] *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, European Commission (June 10, 2015), https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data. Other relevant international privacy frameworks include: Art. 12, Universal Declaration of Human Rights, United Nations, http://www.un.org/en/universal-declaration-human-rights/index.html; Art. 17, International Covenant on Civil and Political Rights, The Office of the United Nations High Commissioner for Human Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; Art. 7, Charter of Fundamental Rights of the European Union, http://ec.europa.eu/justice/fundamental-

framework approach to communications privacy protection may provide a good starting point to build a common approach to online privacy and to avoid the dramatic divergence that has arisen.[10]

The Important Role of the FCC in Safeguarding Consumer Privacy

As former FCC Chairman Julius Genachowski has recognized, "The right to privacy is a core American value, and the Federal Communications Commission, at the direction of Congress, has worked for years to implement laws that protect the privacy of consumers when they use communications networks."[11] The FCC implements and enforces a variety of legal protections for consumer privacy, and EPIC has supported the Commission's important work in this field on many occasions.

Section 222 of the Telecommunications Act of 1996 places certain obligations on telecommunications providers to protect the confidentiality of Customer Proprietary Network Information ("CPNI").[12] In 2007, in response to a petition by EPIC,[13] the FCC issued additional rules regarding CPNI compliance to strengthen the privacy and security of consumers' phone records.[14] EPIC filed an amicus brief in *NCTA v. FCC* in support of the FCC's rules, which were upheld by the D.C. Circuit Court of Appeals.[15] EPIC also filed comments in support of the FCC's move to apply CPNI rules to information stored on mobile devices.[16]

The Cable Communications Policy Act of 1984 ("Cable Act") provides strong protections for cable subscriber privacy. The subscriber privacy provision of the Cable Act establishes a comprehensive statutory framework to safeguard cable subscribers' "personally identifiable information," ensuring that cable operators collect only the user data needed to operate the service, keep the data secure while it is in use, and delete the data once it has served its purpose.[17] The subscriber privacy provision also gives cable consumers the right to access

---

rights/charter/index_en.htm; *Madrid Privacy Declaration: Global Privacy Standards for a Global World*, The Public Voice (Nov. 3, 2009), http://thepublicvoice.org/madrid-declaration/.

[10] EPIC, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*, EPIC (Nov. 3, 2015) https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.

[11] Julius Genachowski, Chairman, Fed. Commc'n Comm., Testimony before the U.S. House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology, *Internet Privacy: The Views of the FTC, the FCC and NTIA* (July 14, 2011), https://apps.fcc.gov/edocs_public/attachmatch/DOC-308403A1.pdf.

[12] 47 U.S.C. § 222.

[13] EPIC Petition to FCC, *Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information* (Aug. 30, 2005), https://epic.org/privacy/iei/cpnipet.html.

[14] Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36 (Mar. 13, 2007), https://apps.fcc.gov/edocs_public/attachmatch/FCC-07- 22A1.pdf.

[15] *See* EPIC, *NCTA v. FCC*, https://epic.org/privacy/nctafcc/.

[16] *See* EPIC Comments to FCC, *Privacy and Security of Information Stored on Mobile Communications Devices* (July 13, 2012), https://epic.org/privacy/location_privacy/EPIC-FCC-Mobile-Privacy-Comments.pdf.

[17] 47 U.S.C. § 551.

their data.[18] The private right of action set out in this provision is an important means of enforcing the terms of the law and upholding subscribers' privacy rights. The Cable Act rules are an effective model for privacy law in the commercial sector, particularly concerning the collection of data about cable programming.[19]

The Telephone Consumer Protection Act ("TCPA") prohibits invasive business practices and extends consumer control over personal information by requiring business to obtain meaningful consent from subscribers before subjecting them to automated or prerecorded calls.[20] In 2015, the FCC issued an order and declaratory ruling, interpreting the TCPA to provide greater privacy protections for consumers.[21] EPIC and six other consumer privacy groups filed an amicus brief in *ACA International v. FCC* urging the D.C. Circuit Court of Appeals to uphold the FCC's order safeguarding consumers.[22]

Regarding this particular rulemaking, EPIC has encouraged the FCC to use the full extent of its rulemaking authority to protect consumers' online privacy. But the Commission must go further to fully apply Fair Information Practices ("FIPs")[23] to online communications and to address the full range of communications privacy issues facing U.S. consumers in the digital age.[24] The broader issues raised in this rulemaking underscore the imperative for meaningful, comprehensive safeguards for consumer privacy. As it stands, the FTC is simply not equipped to provide these much-needed protections for numerous reasons.

The FTC Enforcement Approach is Insufficient to Protect Communications Privacy

Some have suggested that the FTC approach to privacy enforcement is sufficient to protect communications privacy. Although EPIC has worked with the FTC for over 20 years to develop the Commission's authority to protect consumer privacy and is responsible for several of

---

[18] *Id*.
[19] *See, e.g*., Marc Rotenberg, Testimony before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, *Privacy in the Commercial World* (Mar. 1, 2001), https://epic.org/privacy/testimony_0301.html; EPIC Comments to FCC, *In the Matter of Digital Broadcast Copy Protection* (Dec. 6, 2002), https://epic.org/privacy/drm/broadcastflagcomments.html; Letter from EPIC to FCC Chairman Michael K. Powell on VOIP Privacy (Dec. 15, 2003), https://epic.org/privacy/voip/fccltr12.15.03.html.
[20] 47 U.S.C. § 227.
[21] *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 30 FCC Rcd. 7961 (2015).
[22] See EPIC, *ACA International v. FCC (2015 TCPA Order Litigation)*, https://epic.org/amicus/acaintl/.
[23] U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, computers, and the Rights of Citizens viii* (1973). *See also* EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.
[24] *See* Memo from EPIC to Interested Persons on FCC Communications Privacy Rulemaking (Mar. 18, 2016), https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf; Letter from EPIC to FCC Chairman Tom Wheeler on Communications Privacy (Jan 20, 2016), https://epic.org/privacy/consumer/EPIC-to-FCC-on-Communications-Privacy.pdf.

its leading privacy settlements,[25] it is emphatically not our view that the FTC has the ability to safeguard communications privacy.

The FTC's emphasis on a "notice and choice" approach fails to effectively protect consumer privacy. Research shows that consumers rarely read privacy policies; when they do, these complex legal documents are difficult to understand. Moreover, emphasizing notice or disclosure favors the interests of businesses over consumers and fails to establish meaningful privacy safeguards. Nor can industry self-regulatory programs provide realistic privacy protections when they are not supported by enforceable legal standards.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[26] The Commission has never required compliance with the Consumer Privacy Bill of Rights ("CPBR"),[27] a basic set of privacy requirements, under its Consent Orders even when companies are found to violate Section 5 of the FTC Act.[28] And the Commission rarely incorporates public comments into its proposed settlements, which is contrary to public policy and the interest of American consumers. Moreover, American consumers whose privacy has been violated by unfair or deceptive trade practices do not have a private right of action to obtain redress. Only enforceable privacy protections create meaningful safeguards, and the lack of FTC enforcement has left consumers with little recourse.

Fundamentally, the FTC is not a data protection agency. Without regulatory authority, the FTC is limited to reactive, after-the-fact enforcement actions that largely focus on whether companies honored their own privacy promises. Because the United States currently lacks

---

[25] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[26] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).

[27] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; *see also* EPIC, *White House Sets Out Consumer Privacy Bill of Rights,* https://epic.org/privacy/white_house_consumer_privacy_.html.

[28] EPIC has recommended compliance with the CPBR in numerous settlement proceeding where the FTC has asked for public comment. *See, e.g.*, EPIC Comments, FTC Project No P114506 (Jul. 11, 2012), https://epic.org/privacy/ftc/FTC-In-Short-Cmts-7-11-12-FINAL.pdf; EPIC Comments, FTC Docket No. 102 3058 (Jun. 8, 2012), https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; EPIC Comments, FTC Project No P114506 (May 11, 2012), https://epic.org/privacy/ftc/EPIC-FTCAd-Disclosures-FINAL.pdf; EPIC Comments, FTC Docket No. 092 3184 (Dec. 17, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf; EPIC Comments, FTC Docket No. 102 3136 (May 2, 2011), https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

comprehensive privacy legislation or an agency dedicated to privacy protection, there are very few legal constraints on business practices that impact the privacy of American consumers. In light of the increasing threats to the privacy of online communications, it is imperative that Congress acts to fill this void.

The Senate Judiciary Committee Has Promoted Many Landmark Privacy Bills

This Committee has sponsored many landmark privacy laws that continue to provide important protections for Americans in the digital age. For example, the Electronic Communications Privacy Act ("ECPA") of 1986 updated federal wiretap law to address the rise of electronic mail and personal data stored on remote servers.[29] The Video Privacy Protection Act of 1988 ("VPPA") helped ensure the protection of personal data arising from the transition to digital video services.[30] The VPPA continues to play a key role safeguarding Internet users who stream video content on the Internet.

These bipartisan statutes represent carefully crafted privacy laws that addressed competing concerns, while setting out principles that were technology-neutral and forward-looking. Importantly, these statutes all provide for a private right of action to individuals whose privacy rights are violated. This mechanism is essential to ensuring robust enforcement of the terms of the law, and for providing meaningful redress to injured parties.

The Judiciary Committee should consider communications privacy legislation based on the FIPS and the CPBR. Consumer Privacy Bill of Rights ("CPBR"). Grounded in the FIPs, the CPBR grants consumer rights and places obligations on private companies collecting consumer information. The CPBR offers seven technology-neutral principles for consumer privacy: (1) Individual Control, (2) Transparency, (3) Respect for Context, (4) Security, (5) Access and Accuracy, (6) Focused Collection, and (7) Accountability.[31] This is a critical policy framework that provides a blueprint for protecting privacy in the modern age.

This framework would establish baseline safeguards for the development of innovative services that take advantage of technology while safeguarding privacy. It would also establish a common regulatory approach for the protection of communications data from the consumer's perspective.

Only enforceable privacy protections create meaningful safeguards, so an effective communications privacy framework must include a private right of action. The Committee should ensure this right is included in privacy legislation.[32]

---

[29] 18 U.S.C. § 2510 *et seq*.
[30] 18 U.S.C. § 2710.
[31] EPIC, *White House Sets Out Consumer Privacy Bill of Rights,* https://epic.org/privacy/white_house_consumer_privacy_.html.
[32] For example, the Justice for Telecommunications Consumers Act of 2016 would end ineffective arbitration schemes that prevent meaningful enforcement of consumer rights. Justice for Telecommunications Consumers Act, S. 2897, 114th Cong. (2016).

The U.S. should strengthen and update its communications privacy law because it is long overdue, because it is widely supported, and because the ongoing failure to modernize our privacy law is imposing an enormous cost on American consumers and businesses.

Thank you for your continuing commitment to consumer privacy protection. We look forward to working with you to develop rules to provide meaningful and much-needed protections for consumer privacy.

Sincerely,

Marc Rotenberg
EPIC President

Khaliah Barnes
EPIC Associate Director

Alan Butler
EPIC Senior Counsel

Claire Gartland
EPIC Consumer Protection Counsel

cc: Senator Chuck Grassley, Chairman, Senate Committee on the Judiciary
Senator Patrick J. Leahy, Ranking Member, Senate Committee on the Judiciary