January 20, 2016

Tom Wheeler, Chairman
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

RE: Communications Privacy Rulemaking

Dear Chairman Wheeler and FCC Commissioners:

EPIC writes to you in support of the recommendation from other organizations that the FCC undertake a rulemaking on consumer privacy. We support this recommendation. The threats to consumers from new Internet-based services are increasing dramatically.[1] We urge you to move quickly on a proposal to undertake a rulemaking consistent to protect the communications privacy of consumers.

For more than 20 years EPIC has worked with the FCC to promote consumer privacy in the communications field.[2] We write to you also to recommend that the FCC take this opportunity to address the full range of communications privacy issues facing US consumers. From government access to CPNI, to the use of email content for

[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; David Lazarus, *Verizon's Super-Cookies are a Super Privacy Violation*, LA Times (Feb. 2, 2015), http://www.latimes.com/business/la-fi-lazarus-20150203-column.html; Cecilia Kang, *Google Tracks Consumers' Online Activities Across Products, and Users Can't Opt Out*, Washington 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* (Dec. 24, 2014), http://www.latimes.com/business/technology/la-fi-tn-facebook-messages-lawsuit-20141224-story.html.

[2] EPIC Comments to FCC, *A National Broadband Plan for Our Future* (June 8, 2009), https://epic.org/privacy/pdf/fcc_broadband_6-8-09.pdf; Amicus Curiae Brief of EPIC, *NCTA v. FCC*, No. 07-1312 (D.C. Cir. May 6, 2008), https://epic.org/privacy/nctafcc/epic-ncta-050608.pdf; 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; Marc Rotenberg, Testimony before the U.S. House of Representatives Judiciary Committee, Subcommittee on Courts and Intellectual Property, *Communications Privacy*, (March 26, 1998, https://epic.org/privacy/internet/rotenberg-testimony-398.html

advertising, to the interception of wireless communications, it is clear that there are a broad range of communications privacy issues within the jurisdiction of the FCC that could be addressed in the context of this new rule making.

We are also aware that communications officials in Europe are reviewing the "ePrivacy Directive" as users of Internet-based services in Europe face challenges similar to those faced by US consumers.[3] For this reason, we believe that a framework approach to communications privacy protection may provide a good starting point to build a common framework for e-privacy and avoid the dramatic divergence that has arisen for consumer privacy.[4]

In this letter we outline several preliminary recommendations for your considerations as well as principles for communications privacy.

EPIC Recommendations for Communications Privacy Regulations

Apply Consumer Privacy Bill of Rights to Communications Data

The FCC must implement a communications privacy architecture based on the Fair Information Practices ("FIPs")[5] and the Consumer Privacy Bill of Rights ("CPBR").[6]

---

[3] ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, European Commission (June 10, 2015) *available at* https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data. Other relevant international privacy frameworks for communication privacy include: Art. 12, Universal Declaration of Human Rights, United Nations, *available at* 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, *available at* http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; Art. 7, Charter of Fundamental Rights of the European Union, *available at* http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm; *Madrid Privacy Declaration: Global Privacy Standards for a Global World*, The Public Voice (Nov. 3, 2009), available at http://thepublicvoice.org/madrid-declaration/; EU Human Rights Guidelines on Freedom of Expression Online and Offline, Council of the European Union (May 12, 2014).

[4] Editorial, *How European Privacy Concerns Could Hurt U.S. Tech Firms*, LA Times (Oct. 8, 2015), http://www.latimes.com/opinion/editorials/la-ed-europe-data-privacy-20151007-story.html.

[5] 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, The Code of Fair Information Practices, EPIC, https://epic.org/privacy/consumer/code_fair_info.html.

[6] 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 [hereinafter White House,

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. This is a critical policy framework that provides a blueprint for protecting privacy in the modern age.

Establish Data Minimization Requirements

The Commission must adopt data minimization requirements based on those described by the CPBR. Service providers should "collect only as much personal data as they need to accomplish purposes specified under the respect for context principle," and "should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise."[7] The FCC's regulations should explicitly limit collection of data to accomplishing a business purpose that is clearly specified.

In addition to limiting the collection of data, it is important that the FCC require service providers to have reasonable data retention and disposal policies. EPIC strongly opposes mandatory statutory data retention, and currently has a petition pending before the FCC urging an end to mandatory retention of phone records.[8] In the same vein, EPIC urges to the FCC to ensure that service providers retain consumer data for the shortest duration possible.

Promote Privacy Enhancing Technologies (PETs)

The FCC must also promote genuine Privacy Enhancing Technologies that limit or eliminate the collection of personally identifiable information.[9] Jeff Jonas, Chief Scientist for the IBM Analytics Groups, describes the need to "bake in" privacy protection by, for example, "the ability to anonymize the data at the edge, where it lives in the host system, before you bring it together to share it and combine it with other data."[10] A "Do Not Track" mechanism is another example of a beneficial privacy-enhancing technology.

CPBR]; *see also White House Sets Out Consumer Privacy Bill of Rights*, EPIC, https://epic.org/privacy/white_house_consumer_privacy_.html.

[7] White House, CPBR.

[8] EPIC, *Petition to Repeal 47 C.F.R. § 42.6 ("Retention of Telephone Toll Records")* (Aug. 4, 2015), available at https://www.epic.org/privacy/fcc-data-retention-petition.pdf.

[9] Herbert Burkert, "Privacy-Enhancing Technologies: Typology, Critique, Vision" in Technology and Privacy: The New Landscape 125 (Philip E. Agre and Marc Rotenberg eds. 1998)

[10] Alec Foege, *IBM's Jeff Jonas on Baking Data Privacy into Predictive Analytics, Data Informed* (Nov. 20, 2013) http://data-informed.com/ibms-jeff-jonas-baking-data-privacy-predictive-analytics/#sthash.hBM0lg1N.dpuf.

Require Opt-In Consent for Use or Disclosure of Consumer Data

The FCC must require Internet-based service providers to obtain opt-in consent for the use or disclosure of consumer data. As former FCC Commissioner Michael Copps correctly stated, "[a] customer's private information should never be shared by a carrier with any entity for marketing purposes without a customer opting-in to the use of his or her personal information."[11]

An opt-in framework would better protect individuals' rights, and is consistent with most United States privacy laws. For instance, the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, Video Privacy Protection Act, Driver's Privacy Protection Act, and Children's Online Privacy Protection Act all empower the individual by specifying that affirmative consent is needed before information is employed for secondary purposes.[12] In contrast, opt-out regimes create an economic incentive for businesses to make it difficult for consumers to exercise their preference not to disclose personal information to others.

Code of Fair Information Practices for the National Information Infrastructure

EPIC has previously outlined a framework of technology-neutral communication privacy principles, which are set forth in the Code of Fair Information Practices for the National Information Infrastructure.[13] We urge the FCC to incorporate these principles into its forthcoming communications privacy rulemaking:

1. The confidentiality of electronic communications should be protected.
2. Privacy considerations must be recognized explicitly in the provision, use and regulation of telecommunication services.
3. The collection of personal data for telecommunication services should be limited to the extent necessary to provide the service.
4. Service providers should not disclose information without the explicit consent of service users. Service providers should be required to make known their data collection practices to service users.

---

[11] Michael J. Copps, Commissioner, *Fed. Commc'ns Comm'n, Statement on the Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36 (Apr. 2, 2007).

[12] Respectively, at 20 U.S.C. § 1232 g, 47 U.S.C. § 551, 18 U.S.C. § 2510 et. seq., 18 U.S.C. § 2710, 18 U.S.C. § 2721, and 15 U.S.C. § 6501.

[13] Marc Rotenberg, *Code of Fair Information Practices for the National Information Infrastructure (NII)*, in *Ethics of Computing: Codes, Spaces for Discussion and Law* 200 (Jacques Berleur and Klaus Brunnstein eds. 1996). See also ; Marc Rotenberg, "Communications Privacy: Implications for Network Design," Communications of the ACM, Volume 36 Issue 8, Aug. 1993, pp. 61-68.

5. Users should not be required to pay for routine privacy protection. Additional charges for privacy should only be imposed for extraordinary protection.
6. Service providers should be encouraged to explore technical means to protect privacy.
7. Appropriate security policies should be developed to protect network communications.
8. A mechanism should be established to ensure the observance of these principles.[14]

Thank you for your consideration of our views. We look forward to working with you.

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Associate Director

Claire Gartland
EPIC Consumer Protection Counsel

[14] *Id*.