June 13, 2016

The Honorable Greg Walden, Chairman
The Honorable Anna Eshoo, Ranking Member
U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
Washington, DC 20515

RE: Hearing on "FCC Overreach: Examining the Proposed Privacy Rules"

Dear Chairman Walden and Ranking Member Eshoo:

We write to you regarding the upcoming hearing on "FCC Overreach: Examining the Proposed 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]

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in defending consumer privacy interests at the Federal Communications Commission ("FCC" or "Commission") for almost twenty years.[2]

We ask that EPIC's Letter Regarding the FCC Broadband Privacy Rulemaking be entered into the hearing record.

With the current broadband privacy rulemaking, the FCC is acting clearly within the agency's statutory jurisdiction, following the Commission's 2015 Open Internet Order.[3] But the FCC can and should go further to provide meaningful protections for users of communication services in the United States.

---

[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* EPIC, *US West v. FCC – The Privacy of Telephone Records*, https://epic.org/privacy/litigation/uswest/ (1997) (describing the efforts of EPIC and others to defend the FCC's customer proprietary network information ("CPNI") rules). *See also* EPIC *Amicus brief*, *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (defending the FCC's CPNI privacy rules).

[3] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).

From government surveillance, to the use of email content for advertising, to the interception of wireless communications, it is clear there are a broad range of privacy issues within the jurisdiction of the FCC that must be addressed to protect the interests of American consumers.

The existing U.S. privacy framework – based largely on the Federal Trade Commission's ("FTC") "notice and choice" approach – is simply not working. Public opinion polls show that 91% of Americans believe they have lost control of how companies collect and use their personal information.[4] And a recent government study found that nearly half of American Internet users refrain from online activities due to privacy and security concerns.[5]

Maintaining the status quo imposes enormous costs on American consumers and businesses.[6] Customers face unprecedented threats of identity theft, financial fraud, and security breach.[7] Our government must respond with comprehensive, baseline privacy protections that ensure Fair Information Practices – an internationally recognized set of informational privacy practices[8] – are applied across the Internet ecosystem.

The FCC's current rulemaking is a modest first step to protect the privacy of consumers online, who for too long have been at the mercy of corporate self-regulation and weak FTC enforcement. EPIC has repeatedly called on the FCC to use the full extent of its rulemaking authority to provide robust privacy protections for our online communications.[9] For your reference, EPIC has enclosed copies of these documents with this letter.

In EPIC's comments to the FCC on the proposed privacy rules, we urged the Commission to fully apply Fair Information Practices, i.e. baseline privacy standards, to online communications data, rather than limiting its focus to "transparency, choice, and security."[10] We recommended that the FCC endorse data minimization requirements, promote Privacy

---

[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] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[6] *See id*.

[7] *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-januarydecember-2015/160229csn-2015databook.pdf.

[8] *See* EPIC, *Code of Fair Information Practices*, https://www.epic.org/privacy/consumer/code_fair_info.html.

[9] *See, e.g.*, 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, et al., to Chairman Tom Wheeler on ISP Data Practices (Mar. 7, 2016), https://epic.org/privacy/consumer/Broadband-Privacy-Letter-to-FCC.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. *See also*, Letter from EPIC to the U.S. Senate Committee on the Judiciary on Communications Privacy (May 10, 2016), https://epic.org/privacy/consumer/EPIC-SJC-FCC-Privacy.pdf.

[10] *See* EPIC Comments to FCC, *In the Matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, (May 27, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-2016.pdf.

Enhancing Technologies (PETs), and require opt-in consent for all use and disclosure of consumer data beyond what is needed to provide broadband service.[11] And we urged the Commission to regulate the practices of companies other than ISPs that collect and use consumer data generated by communications services.[12] While ISPs are clearly engaged in invasive consumer tracking and profiling practices, they are not the only "gatekeepers" to the Internet who have extensive and detailed views of consumers' online activities. Indeed, many of the largest email, search, and social media companies far exceed the data collection practices of ISPs.[13]

The FCC has authority to regulate companies such as Facebook and Google, which pose significant threats to communications privacy, through ancillary jurisdiction. The Communications Act ("Act") provides the FCC authority to regulate privacy practices of other online service providers where the regulations "encourage deployment of [broadband.]"[14] Courts have held that the Act grants the FCC broad regulatory authority, known as ancillary jurisdiction.[15] To exercise its ancillary jurisdiction, the Commission's general jurisdiction must cover the regulated subject and the regulations must be reasonably ancillary to the Commission's mandated responsibilities.[16] This requires that "[the regulation] will fulfill a specific statutory goal[.]"[17]

Social networking sites, search engines, email services, and other online providers easily fall within the Commission's general jurisdiction over "interstate and foreign communication by wire and radio."[18] Section 706 of the Telecommunications Act explicitly mandates the Commission to encourage deployment of advanced telecommunications capabilities, such as broadband Internet.[19] The D.C. Circuit in *Verizon v. FCC* stated that the FCC's "virtuous circle" argument, where net neutrality increases demand for broadband, fulfilled the ancillary jurisdiction requirements.[20]

Similar to net neutrality, regulating communications privacy will also encourage deployment of broadband capability. The FCC's 2016 Broadband Progress Report acknowledged the Commission has "found that a correlation exists between non-adoption of broadband and security and privacy concerns."[21] The 2015 Open Internet Order acknowledged that "the

---

[11] *See id.*
[12] *See id.*
[13] A 2015 survey of online tracking mechanisms found that Google tracking infrastructure is present on 92 of the 100 most popular websites and 923 of the top 1,000 websites. The researchers aptly observed that "Google's ability to track users on popular websites is unparalleled, and it approaches the level of surveillance that only an Internet Service Provider can achieve." Ibrahim Altaweel et al., *Web Privacy Census*, TECHNOLOGY SCIENCE (Dec. 15, 2015), http://techscience.org/a/2015121502/.
[14] 47 U.S.C. § 1302.
[15] *American Library Ass'n v. FCC*, 406 F.3d 689, 700-03 (D.C. Cir. 2005).
[16] *Id.* at 691-92.
[17] *Verizon v. F.C.C., 740 F.3d 623, 640 (D.C. Cir. 2014).*
[18] 47 U.S.C. § 152(a).
[19] 47 U.S.C. § 1302; *see also Verizon*, 740 F.3d at 639-41.
[20] *See Verizon*, 740 F.3d at 643-44.
[21] *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the*

protection of customers' personal information may spur consumer demand for those services, in turn 'driving demand for broadband connections, and consequently encouraging more broadband investment and deployment' consistent with the goals of the [Telecommunications Act]."[22] And a 2016 National Telecommunications and Information Administration report discovered almost half of American households avoided some "important economic and civic online activity" because of privacy and security concerns.[23] The evidence overwhelmingly indicates that improving online privacy will encourage broadband deployment. Regulating privacy practices of Internet-based service providers thus meets the ancillary jurisdiction requirements articulated by the D.C. Circuit in *American Library Association v. FCC.*

While the Committee's hearing characterizes the FCC's broadband privacy rules as an "overreach," the reality is that the FCC is "under reaching." The privacy concerns of Americans are increasing at a rapid rate. Industry expert Mary Meeker's most recent Internet Trend report said simply, "[a]s data explodes . . . data security trends explode." According to Meeker, 45% of users "are more worried about their online privacy than one year ago" and 74% have limited their online activity in the last year due to privacy concerns."[24] The FCC privacy rule is a modest first step to a widespread concern that is well recognized by the industry. Far from an "overreach," the Commission has not gone far enough.

Some have proposed that the privacy approach of the Federal Trade Commission ("FTC") is sufficient to protect online privacy. Thus, they argue, the FCC should stay on the sidelines. We disagree. EPIC has fought for privacy rights for Internet users at the FTC for more than two decades. We filed landmark complaints about privacy violations by Microsoft, Facebook, and Google.[25] While we respect the efforts of the agency to protect consumers, the reality is that the FTC lacks the statutory authority, the competence, and the political will to protect the online privacy of American consumers.

As a result, consumer privacy violations have proliferated under the FTC's watch. This is illustrated by the FTC's decision to permit Google to consolidate users' personal information across more than 60 Google services, including search, email, browsing, and YouTube, into

---

Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act, GN Docket No. 15-191, 2016 Broadband Progress Report, n. 351 (2016).

[22] *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, ¶ 464, 30 FCC Rcd 5601 (2015) (citations omitted).

[23] Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities. *National Telecommunications and Information Administration*, May 13, 2016. Available at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[24] Mary Meeker, *Internet Trends 2016 – Code Conference*, KPCB (June 1, 2016), http://www.kpcb.com/internet-trends.

[25] *See* Complaint and Request for Injunction, Request for Investigation and for Other Relief, *In the Matter of Microsoft Corporation*, (July 26, 2001), https://www.epic.org/privacy/consumer/MS_complaint.pdf; *see also* Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Facebook, Inc*, (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Google, Inc*, (Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.

single, comprehensive user profiles.[26] Google's plan to consolidate user data without consent was a clear violation of the FTC's 2011 consent order with the company, which bars Google from misrepresenting its privacy practices and sharing user information without affirmative consent.[27] EPIC filed suit seeking to compel the FTC to enforce the terms of its consent order with Google, but the agency succeeded in dismissing the suit and took no action to protect the privacy interests of Google users.[28] Thus, virtually all Internet activity now comes under the purview of one company. This approach is clearly the wrong model for those who seek to protect American consumers from profiling by ISPs.

The FCC has a core responsibility to ensure that communications services offered in the United States are safe for consumers, and EPIC encourages the FCC to continue this important work. However, in the digital age that means protecting communications from all who touch the data.

We respectfully urge the Subcommittee to support the FCC's rulemaking and any further steps the FCC takes to protect communications. These steps should include ensuring Fair Information Practices are applied across the Internet ecosystem and addressing the full range of communication privacy issues facing Americans in the digital age.

Sincerely,

Marc Rotenberg
EPIC President

Khaliah Barnes
EPIC Associate Director

Claire Gartland
EPIC Consumer Protection Counsel

Filippo Raso
EPIC IPIOP Clerk

Enclosures

cc: The Honorable Fred Upton, Chairman, House Energy and Commerce Committee
The Honorable Frank Pallone, Jr., Ranking Member, House Energy and Commerce Committee

[26] *See* EPIC, *EPIC v. FTC (Enforcement of the Google Consent Order)*, https://epic.org/privacy/ftc/google/consent-order.html.
[27] The FTC's 2011 consent order with Google arose from a complaint filed by EPIC in 2010 over the company's introduction of the Google Buzz social network, which automatically enrolled Gmail users and published their contact lists without first notifying users or obtaining their consent. *See* EPIC, *In re Google Buzz*, https://epic.org/privacy/ftc/googlebuzz/.
[28] *See* EPIC, *supra* note 13.