MEMORANDUM

To: Interested Persons
From: Claire Gartland, Khaliah Barnes, and Marc Rotenberg, Electronic Privacy Information Center (EPIC)
Re: FCC Communications Privacy Rulemaking
Date: March 18, 2016

EPIC is circulating this memo in response to Federal Communications Commission Chairman Tom Wheeler's draft broadband privacy rules (the "Proposal"), described in a fact sheet issued March 10, 2016. EPIC earlier submitted a letter to the FCC, expressing similar views.[1]

Consumers deserve basic protections for their online communications. Companies that collect and use personal information have an ongoing responsibility to those whose data they have collected. The starting point for a data protection framework are Fair Information Practices, such as those set out in President Obama's Consumer Privacy Bill of Rights ("CPBR"). While the draft Proposal includes some elements of the CPBR, the protections contained in this framework are interdependent and cannot be applied selectively. The Proposal lacks numerous essential ingredients of the CPBR's comprehensive privacy framework. An "informed choice" policy framework will fail to safeguard consumer privacy. Moreover, the Proposal's framing of the communications privacy challenges facing US consumers is incomplete and fails to address the full range of activities that threaten online privacy.

I. Accurate Framing of Communications Privacy Policy Should Acknowledge Full Range of Threats to Consumer Privacy

The draft Proposal's narrow focus on ISPs misses a significant portion of invasive tracking practices that threaten the privacy of consumers' online communications. EPIC urges the FCC to take this opportunity to address the full range of communications privacy issues facing US consumers. While ISPs are clearly engaged in invasive consumer tracking and profiling practices, they are not the only so-called 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 exceed the scope and data collection activities of the ISPs. A failure to protect the privacy of consumers from these Internet-based services is a failure to provide meaningful communications privacy protections.

Agencies engaged in rulemaking actions have a duty to accurately frame the problem they seek to address. The current description of the problem presents ISPs as the most significant component of online communications that pose the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem, incorrectly

[1] 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.

frames the scope of communications privacy issues facing Americans today, and is counterproductive to consumer privacy.

II. EPIC's Proposed Revisions to Chairman Wheeler's Proposed Privacy Rules

The Commission should issue rules that apply the Consumer Privacy Bill of Rights to communications data. Grounded in the Fair Information Practices, the CPBR grants consumers rights and places obligations on private companies collecting consumer information. The CPBR offers seven technology-neutral practices for consumer privacy:

1. Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
2. Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
3. Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
4. Security: Consumers have a right to secure and responsible handling of personal data.
5. Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
6. Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
7. Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

Application of the practices outlined in the CPBR to ISPs and other Internet-based services is consistent with the "duty to protect the confidentiality of proprietary information of, … customers" required by Section 222(a) of the Telecommunications Act. 47 U.S.C. § 222(a). As applied to ISPs and other Internet-based services, the practices outlined in the CPBR require compliance with the following rules:

1. Consumers Must Have Meaningful Control Over the Collection, Use, and Disclosure of Their Data

Internet-based services must obtain voluntary, specific, and informed opt-in consent from consumers for all collection, use, and disclosure of consumer data beyond what is necessary to accomplish the specific purpose for which that data was disclosed. As a result, companies must obtain opt-in consent to collect, use, and disclose consumer data for behavioral profiling and targeted advertising purposes.

The current Proposal fails to provide for individual control over the collection of consumer data, and focuses solely on the "use and sharing" of information. Consumers must have the ability to prevent companies from collecting data beyond what is necessary to accomplish the

specified purpose. This is consistent with the Fair Information Practices and CPBR mandates on individual control, respect for context, and focused collection.

With respect to ISPs, opt-in consent must be obtained for marketing the service to which the consumer currently subscribes, other communications-related services, and any other services or products. To the extent the Commission retains the current categorization of consent requirements, the rules must narrowly define what constitutes "customer data necessary to provide broadband services" and "communications-related services."

Currently, companies routinely allege to obtain consumer "consent" by having users quickly agree to lengthy, unintelligible terms of service and privacy policies. Research shows that consumers rarely read privacy policies; when they do, these complex legal documents are difficult to understand.

In light of these practices, the following requirements must be met for valid opt-in consent:

- In order for consent to be informed, consumers must be presented with and understand the full extent and consequences of what it is they are consenting to. Merely checking a box indicating agreement with a terms of service and/or privacy policy is insufficient.
- Consent must be specific; blanket consent to vague statements about the collection, use, and disclosure for undefined purposes is insufficient.
- Consent must be voluntary, and cannot be conditioned on the willingness or ability to pay.
- Consumers must have the ability to revoke consent after opting in.

2. Transparency Requires Internet-Based Services to Accurately Disclose Their Data Practices in Clear, Understandable, and Accessible Terms

Internet-based services must provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous information about the covered entity's privacy and security practices. This information must include, at a minimum, the type of data collected about consumers; the purposes for which this data is collected, used, and retained; the entities to whom the company discloses this data, the purposes of such disclosures, and the uses of the disclosed data; if and when such data will be destroyed, deleted, or de-identified; and the measures taken to secure this data.

Where a company seeks to use consumer data in a way that is unexpected or inconsistent with the context of the specific transaction in which the data is disclosed, the company must obtain consumer opt-in consent.

3. Internet-Based Services Must Comply With Data Minimization Requirements

Internet-based services shall collect only data that is directly relevant and necessary to accomplish the specified purpose and only retain that data for as long as is necessary to fulfill the specified purpose. This is consistent with the focused collection provision of the CPBR. It is also an essential component of data security in an age of increasingly frequent data breaches.

Collection of any additional data is permissible only where the consumer has given voluntary, specific, and informed opt-in consent.

In no event should the FCC impose mandatory data retention policies. In recognition of the ongoing risk to consumers that results from mandatory data retention, the FCC must also repeal its regulation requiring retention of telephone toll records for 18 months, 47 CFR § 42.6, as set out in the Petition submitted by EPIC, 28 organizations, and numerous experts.[2]

4. Collection of the Contents of Communications Must Be Prohibited

Deep packet inspection must be prohibited "to protect the confidentiality of proprietary information of, … customers" required by Section 222(a) of the Telecommunications Act. 47 U.S.C. § 222(a). This prohibition is also consistent with the respect for context and focused collection provisions of the CPBR.

5. Internet-Based Services Must Comply With Strict Data Security Standards

Internet-based services must ensure robust, end-to-end encryption for all consumers free of charge. Robust encryption will help protect consumer data from impermissible uses and reduce the risks of identity theft and data breaches.

Internet-based services must take additional data security measures, such as Privacy Enhancing Technologies and techniques for meaningful, independently verified anonymization and deidentification.

6. Internet-Based Services Must Ensure Accuracy, Accessibility, and Accountability for Consumer Data

Internet-based services must allow consumers to access the data collected and used about them, and to correct or remove any collected data.

Companies must be accountable to enforcement authorities and consumers for compliance with communications privacy requirements.

7. 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. We urge the FCC to incorporate these principles into its forthcoming communications privacy rulemaking:

[2] 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.

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.
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.