epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

May 27, 2016

By notice published on April 1, 2016, the Federal Communications Commission ("FCC") proposes rules to apply privacy requirements of the Communications Act to broadband Internet access service providers.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the FCC to revise its proposed rules to fully apply Fair Information Practices and the Consumer Privacy Bill of Rights to communications data, rather than limiting its focus to "transparency, choice, and security."[2] EPIC also recommends the FCC revise its proposed rules to include data minimization requirements, promote Privacy-Enhancing Technologies, and require opt-in consent for the use and disclosure of consumer data. EPIC also urges the Commission to investigate and regulate the practices of companies other than ISPs that

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106 (rel. April 1, 2016) [hereinafter "Broadband Privacy NPRM" or "NPRM"].
[2] NPRM ¶ 5.

collect and use consumer data generated by communications services. It is our view that these services are also subject to the jurisdiction of the FCC.

I. EPIC'S INTEREST

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, freedom of expression, and democratic values.[3] EPIC has a particular interest in protecting consumer privacy, and has played a leading role in defending consumer privacy interests at the FCC for almost twenty years.[4] EPIC's 2005 petition[5] to the FCC calling for enhanced security and authentication standards for access to Customer Proprietary Network Information ("CPNI") led the Commission to strengthen privacy protections for telephone records.[6] EPIC defended these rules in an *amicus curiae* brief before the D.C. Circuit Court in *NCTA v. FCC*, establishing support for opt-in privacy safeguards.[7] This effort followed EPIC's *amicus* brief in 1999 in support of the FCCs earlier CPNI rule.[8] More recently, EPIC has filed an *amicus* brief in support of the Commission, backing the agency's rule implementing the Telecommunications Consumer Protection Act ("TCPA").[9]

[3] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *See* EPIC, *US West v. FCC – the Privacy of Telephone Records*, https://epic.org/privacy/litigation/uswest/ (describing efforts by EPIC and others to defend the FCC's CPNI rule).
[5] EPIC, *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.
[6] 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.
[7] 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.
[8] *U.S. W., Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999).
[9] *See* EPIC, *ACA International v. FCC (2015 TCPA Order Litigation)*, https://epic.org/amicus/acaintl/.

EPIC has also submitted comments to the Commission in numerous proceedings, including notices on privacy and security for mobile devices[10] and broadband deployment.[11] In August of 2015, EPIC filed a petition calling for the repeal of rules mandating retention of telephone toll records, a practice that European courts have determined is a violation of fundamental rights.[12] This petition is still pending before the Commission. And EPIC once again urges the Commission to suspend the unnecessary and risky practice of requiring telecommunications firms to retain customer data.

With respect to the present rulemaking on broadband privacy, EPIC has actively engaged with the FCC and has urged the Commission to use the full extent of its rulemaking authority to protect consumers' online privacy. On January 20, 2016, EPIC sent a letter to FCC Chairman Tom Wheeler and FCC Commissioners calling on the Commission to "address the full range of communications privacy issues facing US consumers" and to apply President Barack Obama's Consumer Privacy Bill of Rights to communications data.[13] On March 7th, EPIC and 11 other consumer privacy organizations sent a letter to the Commission regarding the invasive consumer tracking and profiling practices of Internet service providers ("ISPs") and the insufficiency of the Federal Trade Commission ("FTC") to safeguard consumer privacy.[14] On March 18th, EPIC

[10] EPIC Comments to FCC, *Privacy and Security of Information Stored on Mobile Communications Devices* (July 13, 2012), https://epic.org/privacy/location_privacy/EPIC-FCCMobile-Privacy-Comments.pdf.
[11] 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.
[12] EPIC, *Petition to Repeal 47 C.F.R. § 42.6 ("Retention of Telephone Toll Records")* (Aug. 4, 2015), https://epic.org/privacy/fcc-data-retention-petition.pdf; Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Natural Res. (Apr. 8, 2014), http://curia.europa.eu/juris/documents.jsf?num=C-293/12.
[13] Exhibit 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 [hereinafter January 20 Letter].
[14] Exhibit 2, Letter from EPIC, et al. to FCC Chairman Tom Wheeler on ISP Data Practices (Mar. 7, 2016), https://epic.org/privacy/consumer/Broadband-Privacy-Letter-to-FCC.pdf [hereinafter March 7 Letter].

submitted a memorandum to the FCC urging the Commission to broaden the scope of its proposed rulemaking and to strengthen the substance of its substantive data protections.[15] EPIC has attached herein these three documents and formally submits them into the record of this proceeding.

II. EPIC'S FRAMEWORK FOR COMMUNICATIONS PRIVACY

The unregulated collection of consumer data poses a significant threat to online privacy. A small number of companies and large advertising networks are obtaining extraordinarily detailed profiles of the interests, activities, and personal characteristics of Internet users. Users have little idea how much information is gathered, who has access to it, or how it is used. In the absence of legal rules, companies that are gathering this data will be free to use it for whatever purpose they wish.

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 is Fair Information Practices ("FIPs").[16] The basic premise of the FIPs places responsibilities on entities collecting personal information and grants rights to individuals when their data is collected.

President Barack Obama's Consumer Privacy Bill of Rights ("CPBR") is a significant formulation of the FIPs.[17] The CPBR grants consumers rights and places obligations on private

[15] Exhibit 3, 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 [hereinafter March 18 Memo].
[16] EPIC, *The Code of Fair Information Practices*, https://www.epic.org/privacy/consumer/code_fair_info.html.
[17] 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, CPBR]; *see also White House Sets Out Consumer Privacy Bill of Rights*, EPIC, https://epic.org/privacy/white_house_consumer_privacy_.html.

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.[18]

The FCC's rulemaking is an outgrowth of the 2015 Open Internet Order, which reclassified ISPs as common carriers and thereby removed these companies from FTC enforcement jurisdiction.[19] The proposed FCC action could reduce the tracking and profiling of consumer by ISPs.[20] However, EPIC urges the FCC to strengthen the proposed rules, fully embrace FIPs as articulated in the CPBR, and extend its regulatory authority to other companies offering communications services to consumers.

While the FCC's proposed rules include some elements of the CPBR, they lack numerous essential ingredients of the comprehensive FIPs-based privacy framework. The protections contained in the CPBR are interdependent and cannot be applied selectively. The FCC's

[18] White House, CPBR at 47-48.
[19] *See* Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).
[20] *See* March 7 Letter.

proposed rules are limited to only "choice, transparency, and security."[21] A privacy framework centered on "notice and choice" falls well short of FIPs and the CPBR, and shifts the responsibility for privacy protections from companies to individuals. Ultimately, a "notice and choice" approach will fail to effectively safeguard consumer privacy.[22]

Emphasizing notice or disclosure is an ineffective means of protecting the privacy rights of consumers. Privacy experts and social scientists have identified several important flaws with a notice-centric approach to protecting privacy. Privacy notices are long and frequently incomprehensible. It would take consumers 76 working days to read the privacy policies they encounter in one year.[23] If consumers were to actually read every privacy policy, the opportunity cost to the national economy would be $781 billion.[24] Privacy notices must also confront what Professor Helen Nissenbaum termed the "transparency paradox," where the clarity of a notice is in tension with its comprehensiveness.[25] Additionally, a host of cognitive and behavioral hurdles limit the effectiveness of even ideal notices.

The fundamental flaw with a notice-centric approach to protecting privacy is that notice is not a substantive form of protection but a procedural one. Notice, by itself, does not dictate any limitations on the collection, storage, manipulation, or dissemination of information.

---

[21] NPRM ¶ 5.

[22] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV. 1 (2001).

[23] *See* Alexis Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policiesyou-encounter-in-a-year-would-take-76-work-days/253851/; *see also* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & POL'Y FOR INFO. SOC'Y 543, 544, 564 (2008).

[24] Madrigal, *supra* note 13.

[25] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140(4) DAEDALUS 32, 36 (2011), http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf. Stanford's Ryan Calo explained the paradox in similar terms: "Notice is, in this sense, hydraulic: it is very difficult to convey complex content in a clear and concise format." Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1056 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790144&download=yes.

Because even the best notice cannot provide substantive privacy protections for consumers, most privacy regimes treat notice as only one aspect of a more comprehensive set of protections.

The Consumer Privacy Bill of Rights avoids many of the shortcomings of the "notice and choice" approach.[26] Under this comprehensive framework, companies that collect and use personal data on consumers would necessarily take on privacy responsibilities and consumers who provide personal data to companies would gain new rights. This approach is also technology-neutral and forward-looking. A critical examination of these two approaches – a "Bill of Rights" versus "Notice and Choice" – reveals that the rights-based approach is consistent with other efforts to protect privacy and will be far more effective. Meaningful consumer privacy protections require substantive rules, not procedural guidelines. Thus, we urge the Commission to fully apply the CPBR to communications data.

a. Fully Apply the Consumer Privacy Bill of Rights to Communications Data

Fair Information Practices ("FIPs") are a set of internationally recognized practices to address informational privacy. The Code of Fair Information Practices sets out five obligations for all organizations that collect personal data:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[27]

[26] White House, CPBR.
[27] EPIC, *The Code of Fair Information Practices*, http://epic.org/privacy/consumer/code_fair_info.html.

The FIPs appear in various privacy laws and frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[28] and the Privacy Act of 1974.[29]

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). However, the FCC's proposed rules fail to sufficiently address focused collection, individual control, access and accuracy, and accountability. Instead, the proposal addresses only on "choice, transparency, and security."[30] This limited focus falls short of FIPs and the CPBR and will fail to adequately safeguard consumer privacy. 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

[28] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[29] Privacy Act of 1974, 5 U.S.C. § 552a.
[30] NPRM ¶ 5.

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.[31]

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

[31] *See, e.g.*, Video Privacy Protection Act, 18 U.S.C.§ 2710.

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 C.F.R. § 42.6, as set out in the Petition submitted by EPIC, 28 organizations, and numerous experts.[32]

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

[32] 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.

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 that minimize or eliminate the collection of Personally Identifiable Information ("PII"), as well as and techniques for anonymization and deidentification that are robust, provable, scalable, and independently verified.

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. Consumers are also entitled to know "the logic of the processing,"[33], i.e. the basis of automated decisionmaking for such business practices as profiling, marketing, and advertising. "Algorithmic transparency" is a fundamental right for users of news Internet-based services.[34]

In order to make fully informed decisions about the disclosure of personal information and interactions with various companies, consumers must have access to their complete consumer profile – not just the information they have provided to the company but all of the information the company has gathered on them and uses to make decisions about them. The

[33]EU Data Protection Directive 95/46, arts. 12 and 15 of Oct. 24, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[34] *See* EPIC, *Algorithmic Transparency: End Secret Profiling*, https://epic.org/algorithmic-transparency/.

information maintained about a user should be at least as accessible to the user as it is to business partners, and this information must be provided in an intelligible form.

A right of access is a common element of privacy frameworks. The Fair Credit Report Act ("FCRA") gives consumers the right to access information about them that is held by credit reporting agencies as well as the right to have errors or discrepancies investigated and corrected by the credit reporting agencies.[35] The White House's Consumer Privacy Bill of Rights contains an "Access and Accuracy" principle that provides "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."[36] The Council of Europe Convention 108 gives individuals the right to "rectification or erasure of such data if these have been processed contrary to the provisions of domestic law" and the right to a remedy if a request for confirmation or communication is denied.[37]

Additionally, companies must be accountable to enforcement authorities and consumers for compliance with communications privacy requirements. In addition to meaningful oversight by a federal agency, a private right of action should be created for users who are victims of privacy violations. A private right of action is necessary even where a federal agency is given enforcement authority. Agency action is largely discretionary; thus, there is no guarantee that an individual whose rights have been violated will have the opportunity for relief. A private right of action would properly incentivize privacy-protective practices, enable individual redress for privacy, harms, and enforce Congress's intent to safeguard consumer privacy. A private right of

[35] *See* 15 U.S.C. § 1681g.
[36] 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.
[37] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No.: 108, http://conventions.coe.int/treaty/en/treaties/html/108.htm.

action is not unprecedented – many other federal privacy laws include such provisions.[38] Moreover, the HEW Report recommended that a Code of Fair Information Practices must "give individuals the right to bring suits for information practices to recover actual, liquidated, and punitive damages in individual or class action."[39]

b. Establish Data Minimization Requirements

The Commission must incorporate data minimization requirements based on those described by the CPBR in its final broadband privacy rules. 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."[40] Data minimization protects the confidentiality of consumer data and also serves important data security purposes. Limiting the amount of consumer data that companies collect and retain also limits the harm that results from possible data breaches. The FCC's final rules should explicitly limit collection of data to accomplishing a business purpose that is clearly specified.

In addition to limiting the collection of data, the FCC should 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.[41] In the same vein, EPIC urges to the FCC to ensure that service providers retain consumer data for the shortest duration possible.

---

[38] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u; Telemarketing and Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3), (f)(1); Drivers Privacy Protection Act, 18 U.S.C. § 2724.
[39] U.S. Dep't of Health, Educ. and Welfare, Sec'y's Advisory Comm. on Automated Data Sys., *Records, Computers, and the Rights of Citizens* (1973).
[40] White House, CPBR at 21.
[41] EPIC, *Petition to Repeal 47 C.F.R. § 42.6 ("Retention of Telephone Toll Records")* (Aug. 4, 2015), https://epic.org/privacy/fcc-data-retention-petition.pdf.

c. Promote Privacy Enhancing Technologies (PETs)

The FCC must also promote genuine Privacy Enhancing Technologies that limit or eliminate the collection of personally identifiable information.[42] 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."[43] A "Do Not Track" mechanism is another example of a beneficial privacy enhancing technology.

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

The FCC's final rules must require Internet-based service providers to obtain opt-in consent for the use or disclosure of consumer data for any purpose other than providing the requested service. 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."[44]

An opt-in framework would better protect individuals' rights, and is consistent with most U.S. 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

---

[42] Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision* in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre and Marc Rotenberg eds. 1998).
[43] 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-privacypredictive-analytics/#sthash.hBM0lg1N.dpuf.
[44] 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).

the individual by specifying that affirmative consent is needed before information is employed for secondary purposes.[45]

In contrast, opt-out regimes make it difficult for consumers to exercise their preference not to disclose personal information to others. When it is in the economic interest of a company to prevent a consumer from taking a certain action, companies make it difficult for consumers to control the use of personal data. Opt-out is the standard choice for companies that are trying to stop consumers from taking an action. Moreover, an opt-out approach is inadequate because it is not calculated to reasonably inform consumers about their privacy options. The burden is placed on the consumer to locate, understand, and exercise their right to opt-out, rather than requiring companies to obtain affirmative consent.

An opt-in standard would place the responsibility on the companies that ultimately benefit from the disclosure of private consumer information. Requiring opt-in consent would prevent private information from being shared with third parties unless consumers first agreed to the information sharing. Such an opt-in process would eliminate unintended or unwanted disclosures of private information, and would more closely align with Congressional intent.

e. Adopt Privacy Rules for Full Range of Internet-Based Service Providers With Access to Communications Data

The FCC's narrow focus in this rulemaking on ISPs misses a significant portion of invasive tracking practices that threaten the privacy of consumers' online communications. EPIC has repeatedly urged 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

[45] 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.

Internet who have extensive and detailed views of consumers' online activities. Indeed, many of the largest email, search, and social media companies rival the scope and data collection activities of the ISPs. It is significant also that the FTC permitted Google to consolidate the data of Internet users across multiple Internet services over the strong objections of privacy advocates, technology experts, members of Congress, and the states Attorneys Generals.[46] A failure to protect the privacy of consumers from these Internet-based services is a failure to provide meaningful communications privacy protections.

The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial privacy threats for consumers are not the ISPs.

f. Incorporate the 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 the current proposal and future communications privacy rules:

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.

[46] *See* EPIC, *EPIC v. FTC (Enforcement of the Google Consent Order)*, https://epic.org/privacy/ftc/google/consent-order.html.

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.

III. EPIC'S RESPONSES TO FCC REQUESTS FOR COMMENT

EPIC offers the following responses to specific requests for comment in the Commission's notice of proposed rulemaking. These comments also incorporate the recommendations outlined in Section II and in EPIC's previous correspondence with the Commission related to this rulemaking.

a. Harmonization of Other FCC Privacy Rules

The Commission requests comment on the following:

> *[T]he NPRM asks for public comment on a series of closely-related questions including, for example, whether we should update rules that govern the application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results of this proceeding. Likewise, we seek comment on adopting rules that harmonize the privacy requirements for cable and satellite providers under Sections 631 and 338(i) of the Communications Act with the rules for telecommunications providers.*[47]

The principles described in Section II should be applied to all communications data, including consumer data from telephone, VoIP, cable, and satellite communications. The FCC must also clarify and enhance its enforcement of the privacy requirements for these data to reflect current business practices. Specifically, the FCC should apply the definition of PII proposed in this NPRM[48] to all privacy rules within its enforcement jurisdiction.

[47] NPRM ¶ 24.
[48] NPRM ¶ 60.

b. Definition of Personally Identifiable Information

The Commission requests comment on its proposal to define personally identifiable information (PII) as "any information that is linked or linkable to an individual."[49] EPIC supports a broad definition of PII and commends the Commission for defining this key concept in a way that reflects the reality of modern data practices. This proposed definition is also consistent with existing state and federal law, which routinely define PII to include information that both identifies or could identify an actual individual.[50]

As Professor Jerry Kang explains in his analysis of the collection and use of personally identifiable information by Internet firms, definition of PII is not limited to names and addresses; the term "describes a relationship between the information and a person, namely that the information—whether sensitive or trivial—is somehow identifiable to an individual." [51] Information can be "identifiable" to a person in one of three ways: (1) authorship, (2) description, or (3) instrumental mapping.[52] Information that an individual creates and claims authorship over is identifiable, as is information that "could describe the individual in some manner" including characteristics like age and sex; and persistent identifiers (like Social Security numbers, usernames, IP addresses, and unique device addresses) that can be used to map an individual's interactions with an institution are also identifiable.[53]

---

[49] NPRM ¶ 60.
[50] *See, e.g.*, California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575–22579 (2014) (including information that "permits the physical or online contacting of a specific individual"); E-Government Act of 2002, 44 U.S.C. § 3501 *et seq.* (2014) (including both "direct" and "indirect" identifiers); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2014) (including "persistent identifiers that can be used to recognize a user over time and across different Web sites or online services").
[51] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1207 (1998).
[52] *Id.*
[53] *Id.*

The FCC should apply the proposed definition of PII to all of the statutes and regulations within its jurisdiction. The "linked or linkable" definition represents a more flexible, technology-neutral approach that is consistent with the reality of modern business practices.

c. Definition of Opt-Out and Opt-In Approval

The Commission requests comment on the following:

> *We propose to define the term 'opt-in approval' as a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information that requires that the BIAS provider obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the covered information after the customer is provided appropriate notification of the provider's request consistent with the requirements set forth below in Section 64.7002 of the proposed rules and before any use of, disclosure of, or access to such information.*[54]

The definition of "opt-in approval" should be revised to require that consent must be voluntary, specific, and informed. The text of proposed § 64.7000(h) should be revised as follows:

> (h) *Opt-in Approval*. The term "opt-in approval" means a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information that requires that the BIAS provider obtain affirmative, express, voluntary, specific, written, and informed consent from the customer allowing the requested usage, disclosure, or access to the customer PI, consistent with the requirements set forth in section 64.7002 of this subpart.

These additional requirements are necessary to enhance individual control over personal data by ensuring consumer decisions are meaningful and truly valid. These assurances for valid consent are consistent with the Article 29 Data Protection Working Party's definition of consent.[55] See Section II.a.1 for a more detailed discussion of these requirements.

---

[54] NPRM ¶ 69.

[55] *See* Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* 13 (2011) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

d. Types of Approval Required for Use and Disclosure of Customer PI

EPIC urges the Commission to revise its proposed rules to require opt-in consent for the use and disclosure of customer PI for any purpose other than providing the requested service. Specifically, opt-in consent should be required for the marketing of additional service offerings, upselling services to subscribers, advertising unrelated products and services, and any other uses and disclosures not necessary to provide service.

The Commission's proposal to allow the use of personal information to market additional service offerings without any customer consent conflicts with Section 222(c) of the Communications Act.[56] This provision requires customer approval before the service provider can use the customer's personal information for anything other than "(A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories."[57]

In addition, the Commission's proposed rules fail to include any limitations on the ability of service providers to collect consumer data. The CPBR identifies Focused Collection as a key aspect of FIPs, explaining that "[c]ompanies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle."[58] The FCC should revise its proposed rules to require opt-in approval for the collection of customer PI beyond what is needed to provide the requested service.

e. Requirements for Soliciting Customer Opt-Out and Opt-In Approval

The Commission requests comment on the following:

> *[W]e seek comment on the appropriate procedures and practices for BIAS providers to obtain meaningful customer approval for the use or disclosure of customer PI. To that end, we first propose to require BIAS providers to solicit*

[56] 47 U.S.C. § 222(c).
[57] *Id.*
[58] White House, CPBR at 21.

> *customer approval the first time that a BIAS provider intends to use or disclose the customer's PI in a manner that requires customer approval under our proposed rules. Second, we seek comment on the format of BIAS provider solicitations for customer approval, as well as the methods and formats by which customers may exercise their privacy choices. Specifically, we propose that BIAS providers must give customers a convenient and persistent ability to express their approval or disapproval of the use or disclosure of their information, at no cost to the customer. Third, we propose that a customer's choice must persist until it is altered by the customer, and that it should take effect promptly after the customer's expression of her choice.*[59]

Consent must be voluntary, specific, written, and informed. See Section II.a.1 for more detail on the requirements for valid consumer consent. Consumers must also have the ability to easily revoke consent.[60] As stated in the CPBR, companies should "offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place."[61]

f. Use and Disclosure of Aggregate Customer PI

The Commission requests comment on "reasonable measures to de-identify data …"[62] The FCC should revise its proposed rules to require that techniques for anonymization or deidentification must be meaningful and independently verified.

The FCC must ensure that service providers use anonymization techniques that adequately de-identify data so that data cannot be combined with other information for re-identification. Because not all de-identification techniques adequately anonymize data, it is

[59] NPRM ¶ 139.
[60] In 2012, the Video Privacy Protection Act was amended to require that video tape service providers offer the "opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258 (codified at 18 U.S.C. § 2710(b)(2)(B)(iii)).
[61] White House, CPBR at 11.
[62] NPRM ¶ 158.

important that the process employed is robust, scalable, transparent, and shown to provably prevent the identification of consumer information.[63]

Many companies claim to anonymize or de-identify personal information by aggregating it or assigning pseudonyms to it.[64] Behavioral advertising companies routinely claim that the use of pseudonymous identifiers renders personal information anonymous.[65] Data brokers also rely on the aggregate nature of their marketing data as a defense against criticism of their privacy practices. However, these claims of anonymization are often deceptive. Widely-publicized anonymization failures have shown that even relatively sophisticated techniques have still permitted researchers to identify particular individuals in large data sets.[66]

EPIC favors techniques to de-identify user data,[67] and many scholars are performing valuable research on various de-identification techniques, [68] but greater clarification and standardization is needed. For example, Harvard University professor Cynthia Dwork has espoused "differential privacy" as a "privacy-preserving analysis." [69] Differential privacy "ensures that the removal or addition of a single database item does not (substantially) affect the

---

[63] *See generally* EPIC, *Re-identification*, http://epic.org/privacy/reidentification/.
[64] *See* EPIC, *IMS Health v. Sorrell (Concerning the Use of Prescriber-Identifiable Data for Targeted Marketing)*, https://epic.org/privacy/ims_sorrell/.
[65] *DMA Interest-Based Advertising (IBA) Compliance Alert & Guidelines for Interest-Based Advertising*, Direct Marketing Assoc, http://www.dmaresponsibility.org/privacy/oba.shtml ("Relevant Ads Using Anonymous Data. IBA relies on anonymous, aggregated data to deliver an ad to a computer based on the computer browser's activity, not the activities of a specific individual. Companies use cookies to make this happen.").
[66] *See, e.g.*, Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* http://dataprivacylab.org/projects/identifiability/paper1.pdf; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) ("Data can be either useful or perfectly anonymous but never both.").
[67] *See generally* EPIC, *Re-identification*, https://epic.org/privacy/reidentification/.
[68] *See, e.g.*, Cynthia Dwork, *Differential Privacy: A Survey of Results*, in THEORY AND APPLICATIONS OF MODELS OF COMPUTATION 1, 3 (Manindra Agrawal et al. eds., 2008); *see also* Latanya Sweeney, *k-anonymity: A Model for Protecting Privacy*, INT'L J. ON UNCERTAINTY, FUZZINESS AND KNOWLEDGE-BASED SYSTEMS, 10(5), 2002; 557- 570.
[69] Cynthia Dwork, *Differential Privacy: A Survey of Results*, 1, 2008, http://www.cs.ucdavis.edu/~franklin/ecs289/2010/dwork_2008.pdf.

outcome of any analysis."[70] Although not an "absolute guarantee of privacy," differential privacy "ensures that only a limited amount of additional risk is incurred by participating in the socially beneficial databases."[71]

g. Securing Customer Proprietary Information

The FCC asks whether there are "additional data security obligations that would help to ensure the security, confidentiality, and integrity of customer PI."[72]

America faces an epidemic of data breaches that expose millions of consumers to identity theft and financial fraud daily. Criminals trade stolen Social Security numbers ("SSNs"), credit card numbers, and personal information. As of May 17, 2016, there have been 399 data breaches that exposed 12,041,646 personal records this year alone.[73] According to the most recent report by the Department of Justice, more than seventeen million Americans were the victims of identity theft in 2014.[74] In the face of this national threat, the Commission must require service providers to implement robust security measures to protect the personal information they hold.

EPIC requests the FCC to modify its final rules to require that service providers offer robust, end-to-end encryption for all consumers free of charge. Encryption safeguards the confidentiality of the data from hackers and unauthorized access by employees. Customer information, often collected without the affirmative consent of the consumer, should not be exposed to increased vulnerability simply because encryption does not appeal to a company's cost-benefit analysis.

---

[70] *Id*. at 2.
[71] *Id*. at 2-3.
[72] NPRM ¶ 177.
[73] Identity Theft Res. Ctr., *2016 Data Breach Stats* 13 (May 17, 2016), http://www.idtheftcenter.org/images/breach/DataBreachReports_2016.pdf.
[74] *See* Erika Harrell, Ph.D., Bureau of Justice Statistics, *Victims of Identity Theft, 2014*, at 1 (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

The best approach to protect the security and confidentiality of consumer data is to require that service providers collect only the information needed to provide the service and to retain that information only as long as needed. This can be accomplished by requiring opt-in consent for all collection, use, and disclosure of consumer data beyond what is needed for provision of the service. An opt-in policy would make great strides towards protecting customer privacy and reducing the harm to consumers from a potential data breach. The FCC should also encourage service providers to adopt Privacy-Enhancing Technologies that reduce or eliminate the collection of consumer data.

The Commission also seeks comment on "whether to adopt rules requiring BIAS providers to provide their customers with access to all customer PII in their possession, including all CPNI, and a right to correct that data. Access and correction rights are one of the FIPPs."[75] EPIC urges the FCC to revise its final rules to require that consumers are provided with reasonable access to their personal data, as well as reasonable means to correct inaccurate data and to request deletion of their data. See Section II.b for further discussion.

h. Limiting Collection, Retention, and Disposal of Data

The Commission requests comments on the following:

> *In this section, we seek comment on data minimization, including whether we should impose reasonable data collection and retention limits. We also seek comment on whether we should prescribe specific data destruction policies as part of any data retention limits.*[76]

Data minimization protects the confidentiality of consumer data and reduces consumers' vulnerability to identity theft and other fraudulent activity. Limiting data collection and retention reduce the severity of security breaches by shrinking the quantity of data vulnerable to those who

[75] NPRM ¶ 205.
[76] NPRM ¶ 221.

would misuse it. Such reductions are necessary in light of the data breach and identity theft epidemic currently plaguing American consumers.

As a result, the FCC should require service provides to collect only the data that is necessary and relevant to providing the requested service and to retain that data only as long as necessary to fulfill that purpose. See Section II.b for a more detailed discussion of the need for data minimization requirements.

i. Practices Implicating Privacy that May Be Prohibited Under the Act

The Commission requests comments on "whether business practices that offer customers financial inducements, such as lower monthly rates, for their consent to use and share their confidential information, are permitted under the Communications Act."[77]

EPIC urges the FCC to prohibit financial inducements or other "pay-for-privacy" schemes. Financial pressures reduce the voluntariness of consumer consent, which would no longer truly be voluntary if conditioned on the willingness or ability to pay.[78] Moreover, property-based notions of privacy can be problematic in this context. Louis Brandeis and Samuel Warren recognized the problem with market-based approaches to privacy when they wrote their seminal article on the right to privacy more than a century ago.[79] Intellectual property rights preserve values based on marketplace determinations, whereas privacy protects values unique to each individual. Assigning a monetary value to personal and intimate information is unfeasible,

[77] NPRM ¶ 259.
[78] *See* Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* 13 (2011) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (defining free consent as "taken in the absence of coercion of any kind, be it social, financial, psychological or other").
[79] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

due in part to the fact that "those items that are most personal to us are those where the disparity between what a willing buyer and a willing seller will pay is the largest."[80]

The Commission requests comments on "whether the use of DPI for purposes other than providing broadband services, and reasonable management thereof, should be prohibited or otherwise subject to a heightened approval framework."[81]

EPIC urges the FCC to prohibit the collection of the contents of communications.[82] Deep Packet Inspection ("DPI") provides access to the content of all unencrypted Internet traffic that Internet users send and receive. This highly intrusive surveillance can implicate attorney/client and doctor/patient privilege, trade secrets, other protected communications. Moreover, consumers should not be permitted to consent to DPI because it can collect communications from third parties who have not consented to this invasive surveillance.

Renowned computer scientist Tim Berners-Lee expressed his strong opposition to DPI as follows:

> The access by an ISP of information within an internet packet, other than that information used for routing, is equivalent to wiretapping a phone or opening sealed postal mail. The URLs which people use reveal a huge amount about their lives, loves, hates, and fears. This is extremely sensitive material. People use the web in crisis, when wondering whether they have STDs, or cancer, when wondering whether they are homosexual and whether to talk about it, to discuss political views which may be abhorrent, and so on. […] The power of this information is so great that the commercial incentive for companies or individuals misuse it will be huge, so it is essential to have absolute clarity that it is illegal. The act of reading, like the act of writing, is a pure, fundamental, human act. It must be available without interference or spying.[83]

[80] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1, 92 (2001).
[81] NPRM ¶ 264.
[82] *See* EPIC, *Deep Packet Inspection and Privacy*, https://epic.org/privacy/dpi/.
[83] Tim Berners-Lee, *No Snooping*, W3C (Mar. 11, 2009) https://www.w3.org/DesignIssues/NoSnooping.html.

Americans have a fundamental right to confidentiality of their communications, and DPI must be prohibited to preserve that right.

j. Dispute Resolution

The Commission requests comments on the following:

> *We seek comment on whether our current informal complaint resolution process for alleged violations of the Communications Act is sufficient to address customer concerns or complaints with respect to the collection, use, and disclosure of customer information covered by our proposed rules.*[84]

The FCC must clearly provide a private right of action in its final rules. A private right of action is necessary to properly incentivize privacy-protective practices, enable individual redress for privacy, harms, and enforce Congress's intent to safeguard consumer privacy. See Section II.a.6 for additional discussion of enforcement and accountability considerations.

The FCC also seeks comment on "whether to prohibit BIAS providers from compelling arbitration in their contracts with customers."[85] EPIC urges the FCC to prohibit mandatory arbitration clauses. Only enforceable privacy protections create meaningful safeguards, and a private right of action is indispensable to ensure enforcement.[86] The Commission must prevent corporations from curtailing this right and reducing their accountability to consumers for failing to protect consumer data.[87]

---

[84] NPRM ¶ 273

[85] NPRM ¶ 274.

[86] *See* Jessica Silver-Greenberg and Robert Gebeloff, *Beware the Fine Print Part I: Arbitration Everywhere, Stacking the Deck of Justice*, N.Y. TIMES (Oct. 31, 2015), http://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html; Jessica Silver-Greenberg and Michael Corkery, *Beware the Fine Print Part II: In Arbitration, a 'Privatization of the Justice System,"* N.Y. TIMES (Nov. 1, 2015), http://www.nytimes.com/2015/11/02/business/dealbook/in-arbitration-a-privatization-of-the-justice-system.html.

[87] Congress has also recognized the dangers of mandatory arbitration. 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).

k. Other Proposed Frameworks and Recommendations

The Commission requests comment on EPIC's proposed framework for privacy rules.[88] This proposed framework, which applies Fair Information Practices and the Consumer Privacy Bill of Rights, provides meaningful and comprehensive privacy protections for online communications. While the FCC's proposed rules include some elements of the CPBR, the protections contained in a FIPs-based framework are interdependent and cannot be applied selectively. The proposed rules lack numerous essential ingredients of the CPBR's comprehensive privacy framework. The FCC's focus on "transparency, choice, and security"[89] is more closely aligned with a "notice and choice" framework than FIPs, and will fail to effectively safeguard consumer privacy.

EPIC's proposed data minimization requirements also provide greater confidentiality and security protections to consumer data. The FCC's proposal prescribes no limits on service provider's collection of consumer information, which is incompatible with the CPBR principles of Focused Collection and Respect for Context.

l. Legal Analysis: Section 706 of the Telecommunications Act of 1996

The commission requests comment on the following:

> *We also believe that the proposed transparency, choice, and security requirements further align with the virtuous cycle of Section 706, since they have the potential to increase customer confidence in BIAS providers' practices, thereby boosting confidence in and therefore use of broadband services, which encourages the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans. We seek comment on this analysis.*[90]

[88] NPRM ¶¶ 287-88.
[89] NPRM ¶ 5.
[90] NPRM ¶ 309.

EPIC finds this analysis to be reasonable, and believes it applies to the data practices of all Internet-based service providers.

The FCC has a duty to "encourage the deployment on a reasonable and timely basis of advanced telecommunications" and "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition" under Section 706 of the Telecommunications Act of 1996.[91]

The FCC "has recognized that consumers fearful of the loss of privacy may be less likely to use broadband connectivity, thus decreasing the demand for broadband investment and deployment."[92] The 2016 Broadband Progress Report acknowledged the Commission has "found that a correlation exists between non-adoption of broadband and security and privacy concerns."[93] Indeed, this NPRM acknowledges that "the Commission has found previously, [that] 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 1996 Act."[94]

A recent study by the National Telecommunications and Information Administration ("NTIA") confirms the FCC's conclusion that privacy concerns impact consumer Internet

[91] 47 U.S.C. § 1302(a), (b).
[92] Broadband Privacy NPRM ¶ 26 (citing *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 Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, GN Docket No. 15-191, 2016 Broadband Progress Report, FCC 16-6, at 53-54, para. 126 (Jan. 29, 2016) (*2016 Broadband Progress Report*).).
[93] *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 Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, GN Docket No. 15-191, 2016 Broadband Progress Report, n. 351 (2016) [hereinafter 2016 Broadband Progress Report].
[94] 2015 Open Internet Order at para. 464 (citations omitted).

usage.[95] Forty-five percent of U.S. households reported that privacy and security concerns "stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet."[96] The study concluded that, "[i]n addition to being a problem of great concern to many Americans, privacy and security issues may reduce economic activity and hamper the free exchange of ideas online."[97]

IV. CONCLUSION

For the foregoing reasons, EPIC urges the FCC to (1) enforce all Fair Information Practices to communications data; (2) mandate data minimization requirements; (3) promote Privacy-Enhancing Technologies; and (4) require opt-in consent for the use and disclosure of consumer data.

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and
Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Counsel

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

Exhibit 1

Letter from EPIC to FCC Chairman Tom Wheeler on Communications Privacy

January 20, 2016

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*.

Exhibit 2

Letter from EPIC et al., to FCC Chairman Tom Wheeler on ISP Data Practices

March 7, 2016

March 7, 2016
Tom Wheeler
Chairman
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

Re: Broadband Privacy Rulemaking

Dear Chairman Wheeler:

On March 1, 2016, five large trade associations for broadband Internet service providers ("ISPs") proposed a framework for the Federal Communication Commission's ("FCC") forthcoming rulemaking on broadband privacy.[1] While it is encouraging that ISPs now appear willing to engage on this issue and to recognize the importance of FCC data security and data breach regulations, the proposed framework fails to provide consumers with the robust protections needed in light of ongoing ISP information collection practices. We therefore submit this letter reviewing the collection practices of ISPs across multiple platforms (including their video offerings), and urging the FCC to adopt rules that will provide meaningful protections for broadband consumers.

ISPs currently play a leading role in the complex ecosystem of online behavioral advertising and related forms of data-driven, targeted marketing. These companies are showing an increased interest in monetizing the data they collect about their customers, and they are leveraging their position as gatekeepers to the Internet to harness this data in powerful and invasive ways.

Verizon, for example, has in place powerful data-driven tracking and targeting infrastructure for multiple platforms and devices, including mobile phones. Verizon's acquisition of both AOL and Millennial Media in 2015, as well as its advertising partnership with Microsoft, provide the company with extraordinary capabilities for data gathering, analysis, and monetization of subscriber information.[2]

---

[1] Letter of American Cable Association, Competitive Carrier Association, CTIA, NCTA and USTelecom to Tom Wheeler, Chairman, Federal Communications Commission (Mar. 1, 2016).

[2] Center for Digital Democracy, *Big Data That Watches You Across Platforms* (forthcoming Mar. 2016) [hereinafter "CDD Report"]; Rich McCormick, *Verizon Will Share Your Browsing Habits With AOL's Massive Ad Network*, THE VERGE (Oct. 6, 2015), http://www.theverge.com/2015/10/6/9468025/verizon-will-share-your-browsing-habits-with-aols-massive-ad-network; *AOL to Deepen its Programmatic Leadership with Agreement to Acquire Millennial Media*, MILLENNIAL MEDIA (Sept. 3, 2015) http://www.millennialmedia.com/press/aol-to-deepen-its-programmatic-leadership-with-agreement-to-acquire-millennial-media.

Last year, Comcast announced it would share viewer data collected by its cable set-top boxes with its NBCUniversal media division.[3] As a result, Comcast is now actively involved in the race to build advanced data collection technologies into broadband networks and multi-screen video systems. Through its "Spotlight" advertising service, Comcast provides "multi-screen" targeting, including on mobile devices.[4] In addition to its own intensive research and development efforts, Comcast has also acquired a number of leading advanced advertising and data-targeting companies.[5] Comcast is able to harvest "terabytes of unstructured data" from the set-top boxes it controls, which it then enriches with demographic information to provide data "more meaningful to advertisers," including those targeted via "Comcast's IP-based systems."[6]

Cox Communications offers data-driven, cross-device targeting on television, Internet, and mobile devices. Its targeting capabilities "[l]everage household demographics, like income, ethnicity and home ownership."[7] And through "data partnerships" and related online targeting techniques, Cox gathers additional information about consumers to create highly detailed behavioral profiles.[8]

These consumer tracking and targeted advertising practices are exacerbated by the position of ISPs as gatekeepers to the Internet, which can provide them with a highly detailed and comprehensive view of their subscribers' online communications, personal habits, and daily lives. Moreover, ISPs have access to additional information by virtue of their business relationship with subscribers, such as home addresses, financial information, and credit ratings.

As of April 2015, sixty-five percent of Internet traffic in North America was unencrypted,[9] thereby allowing ISPs expansive access to the content of subscribers' online communications. However, even as websites increasingly adopt encryption to protect privacy, this measure does not eliminate ISP data collection capabilities. Most forms of encryption

---

[3] Shalini Ramachandran & Suzanne Vranica, *Comcast Seeks to Harness Trove of TV Data*, WALL ST. J. (Oct. 20, 2015), http://www.wsj.com/articles/comcast-seeks-to-harness-trove-of-tv-data-1445333401.

[4] *Ad Solutions*, COMCAST SPOTLIGHT, http://www.comcastspotlight.com/ad-solutions/overview.

[5] CDD Report, *supra*; Suzanne Vranica, *Comcast Has Agreed to Acquire Ad Tech Firm Visible World*, WALL ST. J. (June 4, 2015), http://blogs.wsj.com/cmo/2015/06/04/comcast-has-agreed-to-acquire-ad-tech-firm-visible-world; Ryan Lawler, *Comcast is Acquiring Video Ad Company FreeWheel for $320 Million*, TECHCRUNCH (Mar. 1, 2014), http://techcrunch.com/2014/03/01/comcast-freewheel/.

[6] *Comcast Uses MapR for New Advertising Platform That Provides Real-Time Targeted Ads*, MAPR, https://www.mapr.com/resources/comcast-uses-mapr-new-advertising-platform-provides-real-time-targeted-ads.

[7] *Cox Digital Ad Network Solutions*, COX MEDIA, http://www.coxmedia.com/products-and-services/online/cox-digital-ad-network-solutions.aspx.

[8] *Digital VideoX*, COX MEDIA, http://www.coxmedia.com/products-and-services/online/digital-videox.aspx.

[9] *See* Sandvine, *Global Internet Phenomena Spotlight: Encrypted Internet Traffic* 3 (May 8, 2015) https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.

obscure the content of communications, but the packet headers remain visible.[10] Thus, ISPs would still have access to this metadata, which includes information regarding the time, size, origin, and destination of the communication.[11] HTTPS also does not prevent ISPs from seeing the websites to which a user navigates. Such information can reveal intimate details of the user's lifestyle. Moreover, communications via devices connected to the Internet of Things are largely unencrypted, allowing ISPs access to the information these devices are reporting on their users.[12]

Regardless of encryption, ISPs still receive data related to the frequency, timing, location, and volume of a user's Internet access. This information can reveal intimate details about the subscriber, such as when a user has recently become employed or given birth to a child.

While use of a "virtual private network" ("VPN") also provides additional privacy protections, Americans who utilize free broadband access cannot rely on VPNs to protect their privacy. This is particularly true with respect to low-income Americans and children who use access points maintained by E-Rate recipients, since E-Rate recipients are required to filter for adult content.[13] Moreover, many Internet users do not even know what VPNs are, much less how to use them. Consumers should not be forced to pay for extra precautions to protect their privacy.[14] Privacy should not be reserved for the privileged, and no American should have to choose between Internet access and their privacy.

The invasive and ubiquitous tracking practices of ISPs underscore the imperative for the FCC to exercise the full extent of its rulemaking authority to protect consumer privacy. As it stands, the Federal Trade Commission is simply not equipped to provide meaningful protections for consumer privacy for numerous reasons.

---

[10] *See* Ctr. for Democracy & Tech., *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (Jan. 20, 2016), https://cdt.org/insight/applying-communications-act-consumer-privacy-protections-to-broadband-providers/.

[11] *Id*.

[12] *See* Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016), https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-ofthings/ (noting several Internet of Things devices transmitting video, ZIP codes, and other sensitive data without encryption); Lorenzo Franceschi-Bicchierai, *Nest Thermostat Leaked Zip Codes Over the Internet*, VICE: MOTHERBOARD (Jan. 20, 2016), http://motherboard. vice.com/read/nest-thermostat-leaked-home-locations-over-the-internet ("Some smart devices have such little computing power that they couldn't perform the necessary encryption processes even if their creators wanted them to . . . .").

[13] *See* 47 U.S.C. § 254(h)(5)(B).

[14] *See* Marc Rotenberg, *Privacy Guidelines for the National Research and Education Network*, NCLIS (1992) ("Users should not be required to pay for routine privacy protection. Additional costs for privacy should only be imposed for extraordinary protection.") *reprinted in* ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY 762 (2016); *see also* Marc Rotenberg, *Communications Privacy: Implications for Network Design,* 36 Communications of the ACM 61-68 (Aug. 1993).

The FTC's emphasis on the "notice and choice" approach to privacy protections 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 meaningful 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.[15] Moreover, the Commission rarely incorporates public comments into its proposed settlements, which is contrary to public policy and the interest of American consumers. 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 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. The FCC has the opportunity to fill this void. In light of the increasingly pervasive tracking practices of ISPs, it is imperative that the FCC take this opportunity to exercise the full extent of its rulemaking authority to protect consumer privacy.

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 in this field.

Sincerely,

American Civil Liberties Union
Center for Digital Democracy
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Electronic Privacy Information Center
Free Press
New America's Open Technology Institute
Privacy Rights Clearinghouse
Public Knowledge

[15] *See* Compl., *EPIC v. FTC*, 844 F. Supp. 2d 98 (D.C. Cir. 2012) (No. 12-206).

Exhibit 3

Memo from EPIC to Interested Persons on FCC Communications Privacy Rulemaking

March 18, 2016

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.