epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL COMMUNICATIONS COMMISSION

Restoring Internet Freedom

Docket No. 2017-11455
FCC 17-60

July 17, 2017

By notice published on June 2, 2017 the Federal Communications Commission ("FCC") requested comment on a proposed rule to reclassify broadband Internet access service as an information service and remove it from the FCC's Title II jurisdiction, classify mobile broadband as a private mobile service, and whether to keep, modify, or eliminate the bright-line rules set out in the Title II Order.[1] The Commission also requested comment on whether the FCC or the Federal Trade Commission ("FTC") should have jurisdiction over the privacy practices of Internet service providers ("ISPs") online privacy.[2] The Electronic Privacy Information Center ("EPIC") submits these comments to address the question of Internet privacy posed by the Commission.

[1] *Request for Comment on "Restoring Internet Freedom,"* 82 Fed. Reg. 25,568 (Jun. 2, 2017) (hereafter "Restoring Internet Freedom").
[2] Restoring Internet Freedom at ¶ 50.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights related issues, and to protect privacy, the First Amendment, and constitutional values.[3] EPIC previously urged the FCC to adopt rules that provided for strong privacy protections that applied to ISPs and websites alike.[4] Despite EPIC's clear recommendations, last October the Commission chose to adopt a modest privacy rule that only applied to ISPs.[5] However, even those privacy protections were recently repealed by Congress with the Congressional Review Act.[6]

EPIC submits these comments to (1) emphasize that no matter how the Commission chooses to classify broadband Internet service the Commission should protect online privacy; (2) Highlight past FTC online privacy incidents; (3) urge the FCC to consider concurrent jurisdiction with the FTC on Internet privacy; and (4) propose privacy rules based on Fair Information Practices that the FCC should immediately adopt as EPIC proposed earlier.

I. Telecommunications vs. Information Services

The primary purpose of the Commission's proposed rule and request for comments is to examine how broadband Internet should be classified.[7] EPIC has no opinion on this matter.

---

[3] *About EPIC,* EPIC, http://epic.org/epic/about.html.
[4] Comments of EPIC to the Federal Communications Commission, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* May 27, 2016, https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-2016.pdf; Reply Comments of EPIC to the Federal Communications Commission, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Jul. 6, 2016, https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf; 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; 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; 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.
[5] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Report and Order,* Federal Communications Commission, Oct. 27, 2016.
[6] Kelly Reilly, *President Trump Signs Bill Overturning Internet Privacy Protections,* Time, Apr. 3, 2017, http://time.com/4724128/donald-trump-internet-history-isp-privacy-browser-history/.
[7] *See generally* Restoring Internet Freedom.

However the FCC chooses to classify broadband Internet it should develop privacy rules and regulations. Whether broadband Internet is defined as a "telecommunications service" or an "information service" makes no difference.

If the FCC keeps the current broadband Internet classification as a telecommunications service then it should regulate online privacy. This is clear from the text of Section 222 of the Communications Act.[8] Section 222 states that the responsibility to issue online privacy regulations should be done by the FCC and the mandate to issue such regulations cannot be passed on to other federal agencies.[9]

If the FCC chooses to reclassify broadband Internet as an information service it still has the ability to, and should, protect consumer privacy. The FCC can do this under their ancillary jurisdiction under Section 706 of the Communications Act. Protecting online privacy fits into the test laid out by the D.C. Circuit in *American Library Association v. FCC* and was recently affirmed in *Verizon v. FCC*.[10] The Commission may use its ancillary jurisdiction if two conditions are met: "(1) the Commission's general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to Commission's effective performance of its statutorily mandated responsibilities." ISPs and websites fall into these categories.[11]

II. FTC's Past Role in Online Privacy

The Commission is proposing that the FTC be primarily responsible for protecting consumer's online privacy because the FTC has "historically…protected the privacy of

[8] 47 U.S.C. §222.
[9] *Id.*
[10] *American Library Ass'n v. FCC*, 406 F.3d 689, 700-03 (D.C. Cir. 2005); *Verizon v. FCC*, 740 F.3d 623, 632 (D.C. Cir. 2014).
[11] *American Library Ass'n,* 406 F. 3d at 691-92 (D.C. Cir. 2005).

broadband consumers."[12] While the FTC does have experience in this area, their willingness and ability to take strong meaningful steps to protect online privacy has been muted and, unlike the FCC, the FTC is not statutorily mandated to protect online privacy. Furthermore, the FTC lacks the regulatory authority to protect consumers before any harm occurs and, if they do decide to take action, consumers have already suffered from not having adequate privacy protections.

While we respect the efforts of the FTC to protect consumers, the reality is that the FTC lacks the statutory authority, the competence, and the political will to protect the online privacy of American consumers.

As a result, consumer privacy violations have proliferated under the FTC's watch. In 2012 the FTC allowed Google to consolidate users' personal information across more than 60 Google services, including search, email, browsing, and YouTube, into single, comprehensive user profiles.[13] Google's plan to consolidate user data without consent was a clear violation of the FTC's 2011 consent order with the company, which bars Google from misrepresenting its privacy practices and sharing user information without affirmative consent.[14] EPIC filed suit seeking to compel the FTC to enforce the terms of its consent order with Google, but the agency succeeded in dismissing the suit and took no action to protect the privacy interests of Google users.[15] Thus, virtually all Internet activity now comes under the purview of one company. This permissive approach is clearly the wrong model for those who seek to protect the privacy of American consumers.

---

[12] Restoring Internet Freedom at ¶ 49.
[13] *See* EPIC, *EPIC v. FTC (Enforcement of the Google Consent Order)*, https://epic.org/privacy/ftc/google/consent- order.html.
[14] The FTC's 2011 consent order with Google arose from a complaint filed by EPIC in 2010 over the company's introduction of the Google Buzz social network, which automatically enrolled Gmail users and published their contact lists without first notifying users or obtaining their consent. *See* EPIC, *In re Google Buzz*, https://epic.org/privacy/ftc/googlebuzz/.
[15] *See* EPIC, *supra* note 14.

The FTC's failure to enforce its own consent orders allows invasive corporate practices to continue. For example, Facebook's GraphSearch allowed users to locate an individual profile that matched hyper-specific searches such as "Married People who like Prostitutes."[16] Such activities violate the FTC's 2011 consent order with Facebook and should have been prohibited.[17] Supercookies and canvas fingerprinting prevent consumers from deleting online trackers and expose them to tracking across entire ad networks.[18] These consumer tracking technologies are highly invasive, yet the FTC cannot prevent them as long as the companies engaged in these practices disclose this fact to the public.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[19] The Commission rarely incorporates public comments into its proposed settlements, which is contrary to public policy and the interest of American consumers. Moreover, American consumers whose privacy has been violated by unfair or deceptive trade practices do not have a private right of action to obtain redress. Only enforceable privacy protections create meaningful safeguards, and the lack of FTC enforcement has left consumers with little recourse.

EPIC also raised objections to the FTC in 2014 concerning Facebook's proposed acquisition of WhatsApp, a popular text messaging application that had been praised for its

---

[16] Tom Scott, *Actual Facebook Graph Searches*, Tumblr (Jan. 23, 2013), http://actualfacebookgraphsearches.tumblr.com/.

[17] *Facebook, Inc*., FTC File No. 092 3184 (2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf. *See also* EPIC, *FTC Facebook Settlement*, https://epic.org/privacy/ftc/facebook/.

[18] Jacob Kastrenakes, *FCC Fines Verizon $1.35 Million Over 'Supercookie' Tracking*, The Verge, Mar. 7, 2016, http://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fcc. *See also* Julia Angwin, *Meet the Online Tracking Device That Is Virtually Impossible to Block*, ProPublica, Jul. 21, 2014, https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block.

[19] *See, e.g.*, Complaint for Injunctive Relief, *EPIC v. FTC* (filed Feb. 8, 2012), http://epic.org/privacy/ftc/google/EPIC-Complaint-Final.pdf.

privacy safeguards.[20] The FTC allowed the merger to go forward but said it would require the companies to honor their privacy policies. However, in August 2016 WhatsApp announced it would revise its privacy policy and disclose personal data, most notably the phone numbers of WhatsApp users, to "Facebook and the Facebook family of companies."[21] EPIC again filed a complaint with the FTC on August 31, 2016.[22] While the FTC has yet to take any official action, the European Commission recently fined Facebook $122 million for misleading them during their investigation of the merger.[23]

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. Not surprisingly, the privacy concerns of Americans are increasing at a rapid rate. Industry expert Mary Meeker noted in 2016 that 45 percent of users "are more worried about their online privacy than one year ago" and 74 percent have limited their online activity in the last year due to privacy concerns."[24]

III. FCC & FTC Concurrent Jurisdiction

---

[20] EPIC & Center for Digital Democracy, *In the Matter of WhatsApp Inc.: Complaint, Request or Investigation, Injunction, and Other Relief*, Aug. 29, 2016, https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf [hereafter "WhatsApp Complaint]; See generally EPIC In re WhatsApp, https://epic.org/privacy/internet/ftc/whatsapp/.

[21] *I Have Questions About the Updated Terms of Service and Privacy,* WhatsApp, https://www.whatsapp.com/faq/en/general/28030012.

[22] WhatsApp Complaint.

[23] *Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover*, European Commission, May 18, 2017, http://europa.eu/rapid/press-release_IP-17-1369_en.htm.

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

The FCC states that by allowing the FTC to take the lead on online privacy they are "respect[ing] the jurisdictional line drawn by Congress."[25] However, Congress has already drawn jurisdictional lines in this area and has chosen the FCC to take steps to protect online privacy.[26] If the FCC feels that more than just their expertise is needed they should consider having concurrent jurisdiction over online privacy with the FTC. Such an approach could provide a solution to the ongoing problem of protecting consumer privacy online by allowing the FCC to issue proactive, privacy protecting regulations and allowing both agencies to address privacy violations when they occur.

There is no question that consumers value their privacy online. However, as has been detailed above the FTC is not the best agency to protect consumer privacy.[27] However, the FTC does have experience in dealing with this area and in some instances their expertise may be valuable. For instance, the FTC may be suitable to hear cases where privacy rights are at risk or where a harm has occurred and the FCC has not yet issued regulations that deal with that specific problem. Such a system would allow the FCC to respect the FTC's "historic" role in online privacy while not abdicating their duty to protect privacy.

However, we reiterate that the FCC has a duty to protect privacy in an area that clearly falls under their jurisdiction. The FCC is the agency that has the most experience and knowledge of the intricacies of the Internet and can issue forward-looking regulations. The FCC is the agency with the ability to issue proactive regulations to protect consumers from harm before it occurs. The FTC lacks these abilities, which are necessary to establishing strong Internet privacy safeguards.

[25] Restoring Internet Freedom at ¶ 49.
[26] 47 U.S.C. §222.
[27] See *supra* Part II.

The FCC should issue privacy regulations for both broadband providers and websites, such as Google and Facebook, that collect vast amounts of consumer data, are unquestionably used by millions of individuals every day to communicate, and that would cease to exist without the Internet. Furthermore, the FCC already has a system in place to hear such violations of regulations as they occur and an open public comment period. Where violations occur that fall outside of FCC regulations the FTC can serve to adjudicate those concerns. However, when such a case arises that should signal to the FCC that new protections are needed.

IV. Framework for Privacy Rules Based on Fair Information Practices

The current 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").[28] The basic premise of the FIPs places responsibilities on entities collecting personal information and grants rights to individuals when their data is collected.

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

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

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; and (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.[29] FIPs appear in various privacy laws and frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[30] and the Privacy Act of 1974.[31]

Application of these is consistent with the "duty to protect the confidentiality of proprietary information of, ... customers" required by Section 222(a) of the Telecommunications Act.[32] However, with the repeal of the privacy rules the FCC is failing to carry out its duty under Section 222. There is currently no agency proactively working to protect consumers online either from ISPs or websites that collect substantial amounts of personal data. The FCC must take immediately steps to require that ISPs and other Internet-based services comply 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

[29] *Id.*
[30] 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.
[31] Privacy Act of 1974, 5 U.S.C. § 552a.
[32] 47 U.S.C. §222(a).

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. Consumers must have the ability to prevent companies from collecting data beyond what is necessary to accomplish the specified purpose. This is consistent with FIPs.

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.[33]

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

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

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 an essential component of data security in an age of increasingly frequent data breaches.

Collection of any additional data should be 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[34], as set out in the Petition submitted by EPIC, 28 organizations, and numerous experts.[35]

---

[34] 47 C.F.R. §42.6

[35] *EPIC Petition to Repeal 47 C.F.R. §42.6, Federal Communications Commission ("Retention of Telephone Toll Records")*, Aug. 4, 2015, https://epic.org/privacy/fcc-data-retention-petition.pdf; *End the FCC Data Retention Mandate!,* EPIC, https://epic.org/privacy/fcc-data-retention/#legal; Docket 17-130, *Petition for Rulemaking to Repeal 47 C.F.R. 42.6 (Retention of Telephone Records),* https://www.fcc.gov/ecfs/search/filings?proceedings_name=17-130&sort=date_disseminated,DESC.

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.[36]

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 de-identification 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,"[37] 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.[38]

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

[36] 47 U.S.C.§222(a).

[37] 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.

[38] *See* EPIC, *Algorithmic Transparency: End Secret Profiling*, https://epic.org/algorithmic-transparency/.

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 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.[39] 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.[40]

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 action is not unprecedented – many other federal privacy laws include such provisions.[41]

---

[39] *See* 15 U.S.C. §1681g.
[40] 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.
[41] *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.

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."[42]

Conclusion

For the foregoing reasons, EPIC urges the Commission not to abdicate its responsibility to protect online privacy and to promptly issue new, comprehensive online privacy rules.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow

[42] 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).