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
	)	

REPLY COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER

July 6, 2016

By notice published April 1, 2016, the Federal Communications Commission ("FCC") seeks reply comments in response to the Broadband Privacy Notice of Proposed Rulemaking.[1] The Electronic Privacy Information Center ("EPIC") submits these reply comments to (1) respond to comments referencing EPIC's advocacy on this rulemaking; (2) urge the Commission to reject calls to adopt the FTC's "notice and choice" approach to privacy; (3) clarify the need and statutory authority for the FCC to adopt data minimization requirements; (4) address the constitutionality and necessity of opt-in consent rules; (5) counter industry arguments that privacy is bad for business; and (6) reject calls for a alternative multi-stakeholder process or self-regulatory approach to broadband privacy.

[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"].

I. OPPONENTS TO THE FCC'S RULEMAKING MISREPRESENT EPIC'S ADVOCACY FOR STRONGER PRIVACY RULES

EPIC has been actively engaged with the FCC throughout this rulemaking. As part of this process, EPIC has identified shortcomings in the Commission's proposal and offered recommendations on how the proposed rules could be strengthened. It is our belief that the FCC can and should go further to provide meaningful protections for users of communications services in the United States.

The National Cable & Telecommunications Association ("NCTA"),[2] CenturyLink, Inc. ("CenturyLink"), [3] Comcast Corporation ("Comcast"), [4] and Verizon [5] have taken EPIC's statements out of context to support their opposition to the FCC's proposal. To be clear, EPIC's view is that the FCC's proposed privacy rules are preferable to no action by the FCC. Commenters who cite EPIC in opposition to privacy rules misconstrue our position. We have urged the FCC to do *more* within its statutory authority, not less. If those commentators do indeed agree with the EPIC positions they cite, then they should support stronger, more comprehensive rules for the reasons outlined below.

The Federal Trade Commission's ("FTC") privacy framework – based largely on "notice and choice"– is simply not working. Public opinion polls show that 91 percent of Americans believe they have lost control of how companies collect and use their personal information.[6] And

[2] Comments of the National Cable & Telecommunications Association, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 46, 50, WC Docket NO. 16-106 (May 27, 2016) [hereinafter NCTA Comments].
[3] Comments of CenturyLink, Inc., *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* n.5, WC Docket NO. 16-106 (May 27, 2016) [hereinafter CenturyLink Comments].
[4] Comments of Comcast Corporation, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 30, WC Docket NO. 16-106 (May 27, 2016) [hereinafter Comcast Comments].
[5] Comments of Verizon, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* n.10, WC Docket NO. 16-106 (May 27, 2016) [hereinafter Verizon Comments].
[6] Lee Rainie, *The State of Privacy in America: What We Learned*, PEW RESEARCH CENTER (Jan. 20, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

a recent government study found that nearly half of American Internet users refrain from online activities due to privacy and security concerns.[7]

Maintaining the status quo imposes enormous costs on American consumers and businesses.[8] Consumers face unprecedented threats of identity theft, financial fraud, and security breach.[9] The FCC should respond with comprehensive, baseline privacy protections that ensure Fair Information Practices ("FIPs")—an internationally recognized set of informational privacy practices[10]—are applied across the Internet ecosystem. Lobbyists who call for regulatory parity in support of maintaining the status quo – i.e., no consumer meaningful privacy rules at all – do not make these arguments out of genuine concern for consumers.

The FCC's current rulemaking is a modest first step to protect the privacy of consumers online, who for too long have been at the mercy of corporate self-regulation and weak FTC enforcement. EPIC supports the Commission doing as much as it believes is possible to move forward in providing these much-needed protections.[11]

---

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

[8] *See id*.

[9] *See, e.g.*, FED. TRADE COMM'N, *Consumer Sentinel Network Data Book* (Feb. 2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-januarydecember-2015/160229csn-2015databook.pdf.

[10] *See* ELEC. PRIVACY INFO. CTR., *Code of Fair Information Practices*, https://www.epic.org/privacy/consumer/code_fair_info.html (last accessed July 7, 2016).

[11] *See, e.g.*, Memo from EPIC to Interested Persons on FCC Communications Privacy Rulemaking (Mar. 18, 2016), https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf; Letter from EPIC, et al., to Chairman Tom Wheeler on ISP Data Practices (Mar. 7, 2016), https://epic.org/privacy/consumer/Broadband-Privacy-Letter-to-FCC.pdf [hereinafter "Coalition Letter to FCC Chairman"]; Letter from EPIC to FCC Chairman Tom Wheeler on Communications Privacy (Jan. 20, 2016), https://epic.org/privacy/consumer/EPIC-to-FCC-on-Communications-Privacy.pdf. *See also*, Letter from EPIC to the U.S. Senate Committee on the Judiciary on Communications Privacy (May 10, 2016), https://epic.org/privacy/consumer/EPIC-SJC-FCC-Privacy.pdf [hereinafter "EPIC Letter to SJC"].

II. THE FTC'S "NOTICE AND CHOICE" APPROACH TO PRIVACY FAILS CONSUMERS

Some have suggested that the FTC approach to privacy enforcement is sufficient to protect American consumers. Although EPIC has worked with the FTC for over 20 years to develop the Commission's authority to protect consumer privacy and is responsible for several of its leading privacy settlements,[12] it is not our view that the FTC's approach is effective in protecting consumer privacy.

A. Consumer Privacy Violations Have Proliferated Under the FTC's Regime

Comcast claims that the "FTC's privacy regime is widely regarded as highly effective at protecting privacy[.]"[13] The NCTA states "the successful FTC's model [] has successfully protected consumers for years[.]"[14] Verizon declares, "[t]he FTC's notice-and-choice regime has proven successful[.]"[15] EPIC disagrees.[16] Contrary to the characterization provided by ISPs, the FTC's "notice and choice" approach has failed to provide meaningful privacy protections for consumers.

EPIC has fought for privacy rights for Internet users at the FTC for more than two decades. We filed landmark complaints about privacy violations by Microsoft, Facebook, and

[12] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney (Dec. 14, 1995), http://epic.org/privacy/internet/ftc/ftc_letter.html (urging the FTC to investigate the misuse of personal information by the direct marketing industry); *DoubleClick, Inc.*, FTC File No. 071-0170 (2000), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf (Complaint and Request for Injunction, Request for Investigation and for Other Relief); *Microsoft Corporation*, FTC File No. 012 3240 (2002), http://epic.org/privacy/consumer/MS_complaint.pdf (Complaint and Request for Injunction, Request for Investigation and for Other Relief); *Choicepoint, Inc.*, FTC File No. 052-3069 (2004) http://epic.org/privacy/choicepoint/fcraltr12.16.04.html (Request for Investigation and for Other Relief).
[13] Comcast Comments at 20.
[14] NCTA Comments at 7.
[15] Verizon Comments at 23.
[16] *See, generally*, Coalition Letter to FCC Chairman; Comments of the Electronic Privacy Information Center, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket NO. 16-106 (May 27, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf; EPIC Letter to SJC.

Google.[17] While we respect the efforts of the Commission to protect consumers, the reality is that the FTC lacks the statutory authority, the competence, and the political will to protect the online privacy of American consumers.

As a result, consumer privacy violations have proliferated under the FTC's watch. This is illustrated by the FTC's decision to permit Google to consolidate users' personal information across more than 60 Google services, including search, email, browsing, and YouTube, into single, comprehensive user profiles.[18] 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.[19] 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.[20] 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 American consumers from privacy invasions by ISPs.

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

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

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

[19] 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/.

[20] *See* EPIC, *supra* note 18.

that matched hyper-specific searches such as "Married People who like Prostitutes."[21] Such activities violate the FTC's 2011 consent order with Facebook and should have been prohibited.[22] Supercookies and canvas fingerprinting prevent consumers from deleting online trackers and expose them to tracking across entire ad networks.[23] 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.[24] The Commission has never required compliance with the Consumer Privacy Bill of Rights ("CPBR"),[25] a basic set of privacy requirements, under its Consent Orders even when companies are found to violate Section 5 of the FTC Act.[26] And the Commission rarely incorporates public comments into its proposed settlements, which is contrary to public policy and the interest of American consumers.

---

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

[22] *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/.

[23] Jacob Kastrenakes, *FCC Fines Verizon $1.35 Million Over 'Supercookie' Tracking*, THEVERGE (March 7, 2016 12:43 pm), 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 (July 21, 2014 9 am), https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block.

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

[25] 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. *See also* EPIC, *White House Sets Out Consumer Privacy Bill of Rights,* https://epic.org/privacy/white_house_consumer_privacy_.html.

[26] EPIC has recommended compliance with the CPBR in numerous settlement proceeding where the FTC has asked for public comment. *See, e.g*., EPIC Comments, FTC Project No P114506 (Jul. 11, 2012), https://epic.org/privacy/ftc/FTC-In-Short-Cmts-7-11-12-FINAL.pdf; EPIC Comments, FTC Docket No. 102 3058 (Jun. 8, 2012), https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; EPIC Comments, FTC Project No P114506 (May 11, 2012), https://epic.org/privacy/ftc/EPIC-FTCAd-Disclosures-FINAL.pdf; EPIC Comments, FTC Docket No. 092 3184 (Dec. 17, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf; EPIC Comments, FTC Docket No. 102 3136 (May 2, 2011), https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

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.

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's most recent Internet Trend report said simply, "[a]s data explodes . . . data security trends explode." According to Meeker, 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."[27]

B. The FCC Should Reject a "Notice and Choice" Approach to Privacy

Verizon urges the Commission to "adopt rules under Section 222 that are consistent with the FTC's consent framework[.]"[28] The NCTA and Comcast echo this recommendation.[29] The FTC's "notice and choice" framework fails to protect consumer privacy, and EPIC urges the FCC to reject these calls. A "notice and choice" framework is based on faulty assumptions, fails

[27] Mary Meeker, *Internet Trends 2016 – Code Conference*, KPCB (June 1, 2016), http://www.kpcb.com/internet-trends.
[28] Verizon Comments at 13.
[29] NCTA Comments at 96; Comcast Comments at 2.

to inform consumers of corporate privacy practices, and is inapposite to the values embodied in the FIPs. "Notice and choice" is directly at odds with baseline privacy standards.[30]

1. "Notice and Choice" is Based on Flawed Assumptions

"Notice and choice" fails to protect consumers because it incorrectly assumes that consumers are informed about online data practices and make rational decisions according to this information. The reality is that privacy policies are often inaccurate, incomprehensible for the majority of consumers, and infrequently read. They fail to provide meaningful descriptions of business practices and are incomprehensible to the majority of consumers. Even if notices were perfectly clear and comprehensible, there are behavioral and cognitive biases that prevent consumers from acting rationally. And the reality of the Internet economy is that there is little competition for Internet search, social network services, or email. Most market sectors are characterized by monopoly or duopolies, which severely limits the ability of consumers to select among competing providers.

Privacy policies are incredibly time consuming to read, and it is unrealistic to expect consumers to do so. It would also take 76 work days to read all of the first-party privacy policies the average Internet user encounters.[31] Within a 261 workday-year, this would unacceptably damage productivity and output. Even if consumers read every privacy policy, they are unlikely to understand what practices they are authorizing. Privacy policies are notoriously difficult to understand. A longitudinal study of privacy policies found they are written above a high school reading level, are becoming more difficult to read, and are becoming longer, with an average of

[30] Marc Rotenberg, *Promoting Innovation, Protecting Privacy*, OECD Observer (June 2016), http://www.oecdobserver.org/news/fullstory.php/aid/5593/Promoting_innovation,_protecting_privacy.html.
[31] Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 J. L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008).

1,951 words each.[32] But even those consumers who read and ostensibly understand privacy policies are nonetheless left uninformed about how their data will be used. Privacy policies do little to explain how consumers' data are actually used and disclosed, instead focusing on broad categories such as advertising or "sharing" with unidentified third parties.

Once confronted with the real implications of data collection, consumers become more privacy-conscious. Professors Alessandro Acquisti and Jens Grossklags found that consumers are less likely to use a service when primed with the consequences of information disclosure. Despite 43 percent of consumers stating they would share their information for "free" services, this dropped to 20 percent once directed to think about how their data can be used.[33] This finding accords with research suggesting privacy concerns increase with familiarity of privacy practices and experience with online business models.[34] Unfortunately, "[c]onsumers cannot have perfect knowledge of all business practices, nor would consumers find it efficient to acquire perfect knowledge."[35]

2. "Notice and Choice" Disregards the "Transparency Paradox"

The "notice and choice" framework assumes notices can truly inform consumers while retaining comprehensibility. This assumption has been proven wrong. Helen Nissenbaum, professor of Media, Culture, and Communication at New York University, refers to this tension as the "transparency paradox":

---

[32] *See* George R. Milne et al., *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 242-43 (2006). *See also* Carlos Jensen & Colin Potts, *Privacy Policies Examined: Fair Warning or Fair Game?* ftp://ftp.cc.gatech.edu/pub/gvu/tr/2003/03-04.pdf.

[33] Joseph Turow, Michael Hennessy, & Nora Drape, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up To Explotation*, ANNENBERG SCHOOL OF COMMUNICATIONS, UNIVERSITY OF PENNSYLVANIA 13 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf. *See also* Alessandro Acquisti & Jens Grossklags, *Uncertainty, Ambiguity and Privacy,* WORKSHOP ON ECONOMICS AND INFORMATION SECURITY (2005).

[34] Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information* 140-42 (1993).

[35] Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363, 370-73 (Alessandro Acquisti et al. eds., 2008).

> Achieving transparency means conveying information-handling practices in ways that are relevant and meaningful to the choices individuals must make. If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used. An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance.[36]

Companies that have attempted to make their privacy practices clear and understandable have often failed to provide the level of detail necessary for a complete understanding of their practices.[37] Conversely, an extremely thorough privacy policy would be incomprehensible to most users.

3. "Notice and Choice" Does Not Offer Predictability or Uniformity to Consumers

Verizon claims that "[c]onsumers will benefit most from a privacy regime that applies [] uniformly to their data regardless of who has it. A consistent regime will avoid creating the consumer confusion, . . . that would result if consumers are subjected to multiple and varying privacy regimes as they conduct themselves online."[38] These concerns ring hollow. Consumers are already confused when it comes to online data practices, and the FTC's "notice and choice" framework only exacerbates the problem.

The absence of meaningful privacy rules creates consumer confusion. Consumers misunderstand the meaning of "privacy policy" and mistakenly believe there are substantive

[36] 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).

[37] For a summary regarding the transparency paradox, see EPIC Comments to the FTC, *Advertising and Privacy Disclosures in a Digital World* 5-9 (May 11, 2012), https://epic.org/privacy/ftc/EPIC-FTC-Ad-Disclosures-FINAL.pdf.

[38] Verizon Comments at 1.

legal protections for their personal data. While industry alleges that two regulatory regimes will somehow confuse consumers, the true cause of consumer confusion is trying to decipher how companies actually use and disclose their data. Moreover, privacy policies vary significantly under the FTC's notice and choice framework. There are essentially no substantive requirements for privacy policies, and the form of these disclaimers varies wildly. These long, confusing documents often fail to identify third-parties or ad networks.[39] Connecting with an ad network exposes users to the networks' privacy policies, none of which are available on the first-party website.[40] The first-party does not set the policies for the third parties with whom they contract. Privacy policies also define key terms such as PII differently.[41] They remain silent on commonplace business practices, vary on how consumers are notified about changes,[42] and offer unclear opt-out mechanisms.[43]

III. DATA MINIMIZATION PRACTICES ARE INDISPENSABLE TO PROTECTING THE CONFIDENTIALITY OF CONSUMER DATA

CTIA – The Wireless Association ("CTIA") claims the FCC "has no statutory authority to regulate ISP data collection, retention, and disposal."[44] EPIC disagrees. Section 222(a) requires telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to, …customers…".[45] The Commission has previously recognized a "general

[39] *See generally* Lorrie F. Cranor, Candice Hoke, Pedro G. Leon, & Alyssa Au, *Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies*, 11 J. L. & POL'Y FOR INFO. SOC'Y 325 (2015).
[40] Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble With Notice and Consent*, http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf.
[41] *See generally* Cranor, *Are They Worth Reading*.
[42] *Id.*
[43] *Id.*
[44] Comments of CTIA, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 173, WC Docket NO. 16-106 (May 27, 2016) [hereinafter "CTIA Comments"].
[45] 47 U.S.C. § 222(a).

mandate to protect confidentiality in 222(a)."[46] Section 222 does not offer a definition of confidentiality. However, the Federal Information Security Management Act provides a useful formulation that defines confidentiality as "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information."[47] Data minimization practices are key to protecting the confidentiality of consumer data.

The best way to prevent loss or misuse of sensitive personal information is to avoid gathering or storing it in the first place. Data that is not collected or retained cannot be subject to unauthorized access or disclosure. Minimizing stored user data reduces incentives for hackers to attack data storage systems by reducing the amount of data available to steal. This practice also reduces the costs of data breaches. Data minimization is actually more effective at protecting the confidentiality of consumer data than notice and choice: "most harms are not mitigated through notice or control alone, but require security and data minimization."[48] Research by FTC Chief Technologist Lorrie Cranor correctly summarized the benefits of data minimization: "If there is less data to transmit and protect, there is less chance of unauthorized access."[49]

IV. THE FCC'S PROPOSED OPT-IN RULES ARE CONSTITUTIONAL AND NECESSARY TO PROTECT CONSUMER PRIVACY

The FCC's proposal to require opt-in consent for using or disclosing customer information for secondary purposes[50] is consistent with the First Amendment. Moreover, opt-in consent is necessary to protect the privacy of consumers' personal communications data.

---

[46] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 81 FR 23360-01 (proposed Apr. 1, 2016) [hereinafter "FCC Broadband Privacy NPRM"].
[47] 44 U.S.C.A. § 3552(b)(3)(B).
[48] Rebecca Balebako, Cristian Bravo-Lillo, & Lorrie Faith Cranor, *Is Notice Enough: Mitigating the Risks of Smartphone Data Sharing*, 11 J. L. & POL'Y FOR INFO. SOC'Y 279, 314 (2015).
[49] *Id.*
[50] For ease of reference, EPIC's reply comments will refer to "secondary purposes" as shorthand for uses other than to market communications-related services, disclosures to affiliates that do not provide communications-related services, and disclosures to non-affiliate third parties. FCC Broadband Privacy NPRM ¶ 107.

The D.C. Circuit Court of Appeals has already affirmed the FCC's rulemaking authority with respect to privacy in its 2009 decision in *National Cable & Telecommunications Ass'n v. FCC*.[51] This case involved opt-in consent rules the FCC issued in response to EPIC's 2005 petition urging the Commission to strengthen privacy and security protections for telephone data.[52] EPIC filed an amicus brief arguing that a comprehensive opt-in policy is the only truly effective means to protect consumer privacy.[53] The D.C. Circuit Court's decision spoke directly to the constitutionality of opt-in consent requirements when it upheld analogous opt-in rules for telephone service providers against First Amendment challenges.[54]

In affirming the FCC's privacy rulemaking, the D.C. Circuit explained "common sense supports the Commission's determination that the risk of unauthorized disclosure of customer information increases with the number of entities possessing it. The Commission therefore reasonably concluded that an opt-in consent requirement directly and materially advanced the interests in protecting customer privacy and in ensuring customer control over the information."[55] The court's decision focused on the reasonableness of the Commission's decision to select opt-in over opt-out rules: "the Commission carefully considered the differences between these two regulatory approaches, and the evidence supports the Commission's decision to prefer opt-in consent."[56]

The D.C. Circuit's decision in *NCTA* focused significantly on whether the Commission's regulatory decisions were reasonable and supported by evidence. The FCC's current proposed

[51] *Nat'l Cable & Telecommunications Ass'n v. F.C.C.*, 555 F.3d 996 (D.C. Cir. 2009)
[52] *See* EPIC, *NCTA v. FCC (Concerning Privacy of Customer Proprietary Network Information*), https://epic.org/privacy/nctafcc/.
[53] EPIC, *Petition for Review of the FCC's 2007 Order* (May 6, 2008), https://epic.org/privacy/nctafcc/epic-ncta-050608.pdf.
[54] *Nat'l Cable & Telecommunications*, 555 F.3d at 998.
[55] *Id*. at 1002.
[56] *Id*.

opt-in consent rules meet this standard. Moreover, the proposed rules satisfy the commercial speech requirements set out by the U.S. Supreme Court in *Central Hudson Gas & Electric Corp v. Public Service Commission of New York*.[57] American jurisprudence recognizes a fundamental right to privacy in personal communications, and it is well established that the government interest in protecting privacy is substantial.[58] The FCC's proposed opt-in consent requirements for the use and disclosure of consumer information for secondary purposes directly advance the right to privacy. Limitations on the use and disclosure of personal information are essential ingredients of the right to privacy.[59] The Supreme Court has recognized that control over one's information is paramount to privacy: "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[60]

The FCC's proposed rules do not prohibit the use of customer information. The rules would simply require ISPs to obtain their customer's informed, express consent prior to using that data for purposes unrelated to the context in which it was obtained. This limitation is

[57] *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 564 (1980).
[58] *See, e.g.*, *In re Primus*, 436 U.S. 412, 432 (1978) (preventing "invasion of privacy" is important state interest); *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 461-62 (1978) (recognizing "legitimate and important state interest" in "protect[ing] the privacy of individuals");
Edenfield v. Fane, 507 U.S. 761, 769 (1993) ("[T]he protection of potential clients' privacy is a substantial state interest."); *Trans Union Corp. v. FTC,* 245 F.3d 809, 818 (D.C.Cir.2001) ("protecting the privacy of consumer credit information" is a substantial governmental interest); *Trans Union Corp. v. FTC (Trans Union I)*, 245 F.3d 809 (D.C. Cir. 2001) (upholding Fair Credit Reporting Act against First Amendment challenge, noting "we have no doubt that this interest -- protecting the privacy of consumer credit information -- is substantial"); *Lanphere & Urbaniak v. Colorado*, 21 F.3d 1508 (10th Cir. 1994) (recognizing that an invasion of privacy is most pernicious when "it is by those whose purpose is to use the information for pecuniary gain").
[59] *See, e.g.,* 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) ("An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record."); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last updated 2013) ("Purpose Specification" and "Use Limitation" principles prohibit the use of personal data for purposes unrelated to the initial data collection without the consent of the data subject); WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* 1 (Feb. 23, 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("Individual Control" principle that states consumers have "a right to exercise control over what personal data companies collect from them and how they use it").
[60] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press,* 489 U.S. 749, 763 (1989).

consistent with FIPs and numerous articulations of data protection practices.[61] Moreover, such a requirement is explicitly contemplated in Section 222, which mandates that "a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information" with customer approval or in other limited circumstances.[62]

A. A Comprehensive Opt-In Policy is the Only Effective Means to Obtain Meaningful Consumer Consent

The FCC's proposed opt-in approach is necessary to ensure informed, express consent with respect to the privacy of consumers' personal information. As former FCC Commissioner Michael Copps 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."[63] An opt-out policy would provide neither adequate protection for consumer data nor a sufficient mechanism for consumers to make voluntary and informed choices.

Opt-out is the standard choice for companies that do not want their customers to take a certain action. Digital advertisers have long known that consumers regularly fail to exercise their opt-out rights.[64] When Netscape first introduced the option for consumers to opt-out of tracking cookies in 1997, a leading ad industry publication explained the advantage of opt-out rules to online advertisers: "because the vast majority of Web users never bother to change their cookie

---

[61] *See, e.g.*, White House, CPBR.
[62] 47 U.S.C. § 222(c)(1).
[63] 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).
[64] *See generally*, Joseph A. Tomain, *Online Privacy & the First Amendment: An Opt-in Approach to Data Processing*, 83 U. CIN. L. REV. 1, 24-25 (2014).

preferences, the effect on companies that use cookies as targeting tools will be minimal."[65] Comcast explicitly acknowledges this fact in its comments to this rulemaking: "In the marketing context, a rough rule of thumb is that opt-out consent mechanisms may yield approximately 82% or much higher of individuals preserving their consent, whereas an opt- in consent model may yield only approximately 18% or much lower of individuals consenting."[66]

An opt-out approach presumes consent unless the consumer takes additional steps to affirmatively register her objections. In other words, the default assumption is that the consumer consents to the proposed transaction. The Supreme Court has recognized that default rules should "comport with the probable preferences" of the individual and that "[c]ourts 'do not presume acquiescence in the loss of fundamental rights.'"[67] The following statement by CTIA represents a concerning disregard for consumer preferences: "That some consumers might *prefer* not to have advertising tailored to their interests is a red herring; consumers certainly have come to *expect* these practices, and an opt-out opportunity is more than adequate for those who truly find such advertising vexatious."[68]

Notably, the European Union's recently updated data protection law requires opt-in consent prior to the processing of personal data. The General Data Protection Regulation specifically states, "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, . . . Silence, pre-ticked boxes or inactivity should not

---

[65] *Id.* (quoting Rick Bruner, *Advertisers Win One in Debate Over 'Cookies,'* ADVERTISINGAGE (May 12, 1997), http://adage.com/article/news/advertisers-win-debate-cookies/405/).
[66] Comcast Comments at 48 (citing Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out,'* MARKETING WEEK (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/).
[67] *Knox v. Serv. Employees Int'l Union, Local 1000*, 132 S. Ct. 2277, 2290 (2012) (quoting *College Savings Bank v. Florida Prepaid Postsecondary Ed. Expense Bd.,* 527 U.S. 666, 682 (1999)).
[68] CTIA Comments at 89.

therefore constitute consent."[69] In other words, companies cannot assume that a consumer agrees to give up their fundamental right to privacy.

Public opinion polls show that the majority of consumers would prefer greater control over their personal information. A recent University of Pennsylvania survey found that 85 percent of Americans "want to have control over what marketers can learn about" them online, yet 65 percent believe they have little control over this.[70] The Pew Research center recently found that 74 percent of Americans believe control over personal information is "very important," yet only nine percent believe they have such control.[71] Thus, because default rules should reflect consumers' probable preferences, default privacy rules should presume consumers do not consent to abandoning control over their personal information unless they affirmatively opt-in.

V. CONSUMER PRIVACY PROTECTIONS BENEFIT THE ECONOMY AND FOSTER INNOVATION

Arguments that heightened consumer protections will stifle innovation and harm American business reflect a flawed understanding of how privacy functions in the modern information economy. That depiction of the dynamic between robust privacy protections and investment incentives is both myopic and misguided.[72] According to Professor Julie Cohen,

> This simplistic view of the relationship between privacy and innovation is wrong… External obstacles, whether material or regulatory, affect the feedback loops [between privacy and innovation], but also represent opportunities; innovation emerges from the interplay between freedom and constraint. Innovative practice is threatened most directly when circumstances impose intellectual regimentation, prescribing orthodoxies and restricting the freedom to tinker. It thrives most fully when circumstances yield serendipitous

[69] Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and the Free Movement of Such Data, O.J. (L 119) ¶ 32.
[70] Turow, *Tradeoff Fallacy*, *supra* n.33 at 14.
[71] Pew Research, *supra* n.6.
[72] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1919 (2013)

> encounters with new resources and ideas, and afford the intellectual and material breathing room to experiment with them.[73]

The common refrain that European-style privacy protections are contrary to innovation is simply wrong. According to a recent report by the World Economic Forum, three of the top five countries that benefit most from technology innovation are members of the European Union: Finland, Sweden, and Norway.[74] The United States ranked fifth in this report. These European countries are subject to robust EU data protection laws, yet foster greater technology innovation than that of the United States. Privacy and innovation are not mutually exclusive. As the FCC has aptly observed, "sensible regulation and robust investment are not mutually exclusive."[75]

Strong privacy protections are also a necessary and pragmatic part of risk mitigation in the age of the ubiquitous cybersecurity breach. Failure to protect user privacy frequently stems from failure to adequately protect user data, which can result in enormous liability for companies.[76] The more data a company stores, the more valuable a target its database is for hackers; and the more stored data, the greater the company's losses in the event of a breach.[77] The risk of data breach is far from speculative: the ubiquity, frequency, and scale of cyberattacks on both public and private entities has become as undeniable as it is alarming. In the public sector, the Office of Personnel Management breaches in 2015 put 21.5 million individuals at risk

---

[73] *Id*.
[74] WORLD ECONOMIC FORUM, *Global Information Technology Report 2016*, http://reports.weforum.org/global-information-technology-report-2016/report-highlights/.
[75] *Id.* at 414.
[76] *2016 Cost of Data Breach Study: United States*, PONEMON INST., 1 (June 2016) [hereinafter "Cost of Data Breach"].
[77] Bruce Schneier, *Data Is A Toxic Asset*, SCHNEIER ON SECURITY, (March 4, 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html ("saving [data] is dangerous because failing to secure it is damaging. It will reduce a company's profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company's computers and networks.").

of identity theft.[78] In the private sector, up to 70 million Target customers were affected by a breach the company suffered in 2013.[79] A study from the Ponemon Institute found that the past year saw record high numbers for cost per breach, total organizational cost, and the volume of breaches.[80] Crucially, the study also noted that the cost per data breach has not fluctuated significantly, indicating that it is a "permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies."[81]Thus, protecting privacy through robust cybersecurity precautions is not merely good policy, it is a pragmatic business strategy that prevents future loss of revenue. Cybersecurity breaches, and the privacy violations that go with them, are bad for business. The FCC's proposed rules will help prevent those breaches, and will benefit, not burden, the industry bottom line.

Increased consumer privacy protections will benefit American business interests, both at home and abroad. The competitiveness of American technology companies in the global market also requires strong U.S. legal protections for communications privacy.[82] Communications officials in Europe are reviewing the "ePrivacy Directive" as users of Internet-based services in Europe face challenges similar to those faced by American consumers.[83]

---

[78] *Cybersecurity Resource Center,* OPM.GOV, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.
[79] *Data Breach FAQ,* TARGET, https://corporate.target.com/about/shopping-experience/payment-card-issue-faq.
[80] Cost of Data Breach, *supra* n.76 at 1.
[81] *Id.*
[82] *See* Aarti Shahani, *A Year After Snowden, U.S. Tech Losing Trust Overseas*, NPR (June 5, 2014), http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas; Claire Caine Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, NY TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.
[83] *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, European Commission (June 10, 2015), https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data. Other relevant international privacy frameworks include: Art. 12, Universal Declaration of Human Rights, United Nations, 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, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; Art. 7, Charter of Fundamental Rights of the European Union, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm; *Madrid Privacy Declaration:*

In addition to helping smooth the regulatory landscape, strong privacy protections will attract privacy-conscious European consumers. Privacy is a fundamental human right and it is a norm that shapes consumer habits.[84] According to the European Commission, 62 percent of Europeans report that they do not trust ISPs with their personal information,[85] and 89 percent think that it is important for them to have the same level of protection for their information, regardless of where the company or public authority collecting it is based.[86] European firms have recognized this gap in the market, and are eager to exploit it by appealing to their own stronger privacy practices.[87] American business cannot afford to isolate itself in a globalized information economy, and enacting stronger privacy protections will help increase appeal to a global market.

VI. THE FCC SHOULD REJECT CALLS FOR MULTI-STAKEHOLDER PROCESSES AND INDUSTRY SELF-REGULATION, WHICH ARE INSUFFICIENT TO PROTECT CONSUMER PRIVACY

AT&T Services, Inc., ("AT&T") proposes that the FCC "should rely on privacy guidelines developed by industry bodies and multistakeholder processes."[88] Comcast suggests that "a multistakeholder process could be workable here, *but only if done before and in lieu of the Commission adopting any rules, not as a sidekick or supplemental form of regulation*."[89] The

---

Global Privacy Standards for a Global World, The Public Voice (Nov. 3, 2009), http://thepublicvoice.org/madrid-declaration/.

[84] *See* Art. 12, Universal Declaration of Human Rights, United Nations, available at http://www.un.org/en/universal-declarationhuman-rights/index.html; Art. 17, International Covenant on Civil and Political Rights, The Office of the United Nations High Commissioner for Human Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; Art. 7, Charter of Fundamental Rights of the European Union, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.html.

[85] *Data Protection Eurobarometer Factsheet*, EUROPEAN COMMISSION, 1 (June 2015), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.

[86] *Id.* at 4.

[87] 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-20151007story.html; Mark Scott, *European Firm Turns Privacy Into Sales Pitch*, NEW YORK TIMES (June 11, 2014), http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch/.

[88] Comments of AT&T Services, Inc., *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 2, WC Docket NO. 16-106 (May 27, 2016) [hereinafter AT&T Comments].

[89] Comcast Comments at 24 (emphasis in original).

FCC should reject this approach because voluntary multi-stakeholder processes consistently fail in the absence of enforceable regulations. Industry self-regulatory programs simply cannot provide realistic privacy protections when they are not supported by enforceable legal standards.

Industry self-regulation and multi-stakeholder processes have repeatedly failed to protect consumer privacy. EPIC has previously raised concerns about the effectiveness of voluntary self-regulatory regimes.[90] Because codes of conduct produced by a multi-stakeholder process are not binding unless they are voluntarily adopted, companies are free to ignore them. Without legislation, multi-stakeholder processes and industry self-regulation are merely aspirational. These processes also tend to have insufficient enforcement, and limited market penetration.

Compounding the lack of legally enforceable standards, the governing organizations of multi-stakeholder and self-regulatory schemes typically do not have sufficient resources to enforce the regulation.[91] Because the governing organizations rely on the financial support from the industry, most multi-stakeholder/self-regulatory organizations are underfunded.[92] Without financial resources, these organizations cannot effectively monitor and ensure compliance. Additionally, the lack of independence between governing organizations and the industries they police further impede the enforcement of multi-stakeholder processes and industry self-regulation.[93] A multi-stakeholder or self-regulatory approach to broadband privacy will face the same enforcement problem. In contrast, robust regulatory enforcement by the FCC is much more likely to command close industry attention.

---

[90] *See, e.g.*, EPIC Comments to NTIA, *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct* (Apr. 2, 2012), https://epic.org/privacy/consumer/EPIC-NTIA-Comments-FINAL.pdf; Marc Rotenberg, Testimony before the U.S. House of Representatives Committee on International Relations, *The European Union Data Directive and Privacy* (May 7,1998) https://epic.org/privacy/intl/rotenberg-eu-testimony-598.html.
[91] Robert Gellman and Pam Dixon, *WPF Report: Many Failures – A Brief History of Privacy Self-Regulation* 10 (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf.
[92] *Id.*
[93] *Id.* at 29.

The absence of meaningful and independent supervision and participation from the public also contributes to insufficient enforcement of multi-stakeholder and self-regulatory processes. Governing organizations are likely to be dominated by the industry,[94] and most self-regulatory rules are formulated in non-public meetings.[95] This fundamental flaw of multi-stakeholder processes is exemplified by the breakdown of efforts to develop a "Do Not Track" mechanism.[96] Instead of adopting a legislative solution to allow consumers to limit online tracking, the FTC "adopted a strategy that favors big companies and Washington lobbyists over Internet users and online privacy: vague goals, endless meetings, more warnings for users and no real impact on business practices."[97]

The voluntary nature of multi-stakeholder processes and self-regulation also results in low participation rates within the industry.[98] For instance, the Network Advertising Initiative—a self-regulatory program created to promote consumer protections in the behavioral advertising industry—experienced less than 20 to 25 percent of industry member participation.[99] The lack of government and public oversight also contributes to low participation rates. By definition, a self-regulatory scheme is policed only by the self-regulating organization. These organizations

[94] Omer Tene & J. Trevor Hughes, *The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study*, 66 Me. L. Rev. 437, 455 (2014).
[95] Robert Gellman and Pam Dixon, *WPF Report: Many Failures – A Brief History of Privacy Self-Regulation* 6 (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf.
[96] *See, e.g.*, Fred. B. Campbell, *The Slow Death of 'Do Not Track,'* N.Y. TIMES (Dec. 26, 2014), http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html?module=Search&mabReward=relbias&.
[97] Marc Rotenberg, *Online Privacy: Who Writes the Rules?*, N.Y. TIMES (Dec. 31, 2014), http://www.nytimes.com/2015/01/01/opinion/online-privacy-who-writes-the-rules.html?_r=0.
[98] *See, e.g.*, Marc Rotenberg, Testimony before the U.S. House of Representatives Committee on International Relations, *The European Union Data Directive and Privacy* (May 7,1998), https://epic.org/privacy/intl/rotenberg-eu-testimony-598.html.
[99] Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* 29, 2007, http://www.worldprivacyforum.org/wp-content/uploads/2007/11/WPF_NAI_report_Nov2_2007fs.pdf.

typically have lax rules for companies to join and exit the self-regulation.[100] For example, the NAI allows companies to join, drop out, and rejoin the regulation "at will over the years, without any apparent consequence."[101] Consequently, companies that no longer wished to comply with the regulation would simply drop out of the program.

The procedures established in the public rulemaking process, pursuant to the Administrative Procedure Act ("APA"),[102] offer more effective mechanisms to develop and implement industry regulations. The APA is a more durable and well-established process than multi-stakeholder approaches for government agencies to receive public comments on proposed regulatory action. The APA notice and comment rulemaking process fosters meaningful, transparent, and inclusive public participation in the development of agency regulations. Public rulemaking permits all interested persons, including those without access to Washington-based meetings, to express their views. It will also impose time limits and requirements on the agency that will help ensure public comments are fully considered and that public participation is meaningful.

After agencies have considered public comments and adopted final regulations, final agency action is subject to judicial review.[103] This helps ensure that whatever action is taken by the agency reflects an outcome that is consistent with purpose of the rulemaking and the public comments received. Most importantly, compliance with formal regulations is legally enforceable and holds industry accountable. The FCC should continue with its formal rulemaking process to promulgate mandatory, enforceable privacy rules.

---

[100] Robert Gellman & Pam Dixon, *WPF Report: Many Failures – A Brief History of Privacy Self-Regulation* 6 (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf.
[101] Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* 28, 2007, http://www.worldprivacyforum.org/wp-content/uploads/2007/11/WPF_NAI_report_Nov2_2007fs.pdf.
[102] 5 U.S.C. § 500 et seq.
[103] 5 U.S.C. § 706.

VII. CONCLUSION

For the foregoing reasons, EPIC urges the FCC to (1) reject calls to adopt the FTC's "notice and choice" approach to consumer privacy; (2) adopt data minimization requirements to ensure the confidentiality of consumer information; (3) refrain from weakening opt-in consent requirements; and (4) reject requests to engage in alternative multi-stakeholder or industry self-regulation processes.

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

Claire Gartland
EPIC Consumer Protection Counsel

Lindsey Barrett
EPIC IPIOP Clerk

Filippo Raso
EPIC IPIOP Clerk

Janet Zhang
EPIC IPIOP Clerk