epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

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

In the Matter of	)	
	)	
Expanding Consumers' Video Navigation Choices	)	MB Docket No. 16-42
	)	
Commercial Availability of Navigation Devices	)	CS Docket No. 97-80

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

April 22, 2016

By notice published on March 16, 2016, the Federal Communications Commission ("FCC") proposes rules to require cable operators to provide content and programming to retail navigation devices, on the condition that manufacturers of these devices self-certify compliance with cable subscriber privacy rules.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the FCC to: (1) apply the Cable Act's subscriber privacy provision directly to retail navigation device manufacturers, and (2) clarify and strengthen enforcement of these privacy rules.

[1] *Expanding Consumers' Video Navigation Choices, Commercial Availability of Navigation Devices*, Notice of Proposed Rulemaking and Memorandum Opinion and Order, MB Docket No. 16-42, CS Docket No. 97-80, FCC 16-18 (rel. Feb. 18, 2016) [hereinafter "Set-Top Box NPRM"].

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.[2] 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.[3] EPIC's 2005 petition[4] 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.[5] 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.[6]

EPIC has also submitted comments to the Commission in numerous proceedings, including notices on privacy and security for mobile devices[7] and broadband deployment.[8] Most recently, EPIC filed a petition in August of 2015 calling for the repeal of rules mandating

---

[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] *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).
[4] 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.
[5] 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.
[6] 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.
[7] EPIC Comments to FCC, *Privacy and Security of Information Stored on Mobile Communications Devices* (July 13, 2012), https://epic.org/privacy/location_privacy/EPIC-FCC-Mobile-Privacy-Comments.pdf.
[8] 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.

retention of telephone toll records, a practice that European courts have determined is a violation of fundamental rights.[9] This petition is still pending before the Commission.

EPIC offers these recommendations to protect the interests of consumers and to ensure meaningful privacy safeguards for consumer cable programming choices.

I. The FCC Must Require All Companies With Access to Cable Subscriber Data to Comply With Cable Subscriber Privacy Rules

Concerns about the privacy risks posed by interactive cable have been well understood for many years. In a 1985 publication titled "Protecting Privacy in Two-Way Electronic Services," EPIC Advisory Board member David H. Flaherty predicted the significant implications this new communications medium would present for consumer privacy:

> Because interactive cable services can collect information about individuals and their behavior within the confines of their own homes and often without their knowledge – e.g., the data available to cable company computers as a result of channel-monitoring capacity – they represent a heretofore unprecedented potential for violation of personal privacy and challenge the traditional concept that "a man's house is his castle."[10]

Flaherty issued this warning in the year after Congress passed federal cable privacy legislation that remains in force today. Despite these strong privacy rules, the same challenges Flaherty identified over three decades ago continue to plague consumers.

The Cable Communications Policy Act of 1984 ("Cable Act") provides strong protections for cable subscriber privacy. The subscriber privacy provision of the Cable Act provides a comprehensive statutory framework for the protection of cable subscribers' "personally identifiable information," ensuring that cable operators collect only the user data

---

[9] 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.

[10] David H. Flaherty, PROTECTING PRIVACY IN TWO-WAY ELECTRONIC SERVICES 8 (Knowledge Industry Publications 1985).

needed to operate the service, keep the data secure while it is in use, and delete the data once it has served its purpose.[11] The subscriber privacy provision also gives cable consumers the right to access their data.[12] The private right of action set out in this provision is an important means of enforcing the terms of the law and upholding subscribers' privacy rights. The Cable Subscriber Privacy Rules are an effective model for privacy rules in the commercial sector, particularly concerning the collection of data about cable programming.[13]

Congress placed a high priority on consumer privacy when it enacted the Cable Act, which recognized the invasive capabilities of cable services.[14] Consumers have a legitimate and significant expectation of privacy with respect to sensitive personal information such as programming selections and service subscriptions. Today, cable companies pose an even greater risk to consumer privacy because of their ability to directly monitor subscribers' programming choices, online activities, and mobile device usage.

A. The FCC Must Directly Enforce Compliance with Cable Subscriber Privacy Rules for Retail Navigation Device Providers

By enacting the Cable Act, Congress sought to protect the privacy of consumer viewing data. Retail navigation devices can – and do – collect consumer viewing data and history, and they should not be permitted to circumvent established public policy to protect this private data. For example, TiVo offers targeted advertising services that "match the TV and online advertising

[11] 47 U.S.C. § 551 [hereinafter "Cable Subscriber Privacy Rules"].
[12] *Id*.
[13] *See, e.g.*, Marc Rotenberg, Testimony before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, *Privacy in the Commercial World* (Mar. 1, 2001), https://epic.org/privacy/testimony_0301.html; EPIC Comments to FCC, *In the Matter of Digital Broadcast Copy Protection* (Dec. 6, 2002), https://epic.org/privacy/drm/broadcastflagcomments.html; Letter from EPIC to FCC Chairman Michael K. Powell on VOIP Privacy (Dec. 15, 2003), https://epic.org/privacy/voip/fccltr12.15.03.html.
[14] H.R. REP. NO. 98-934, at 29-30 (1984).

that households actually receive with the products that the same households actually buy."[15] And Roku's privacy policy informs its users that it "regularly and automatically collects information" about users' Roku Devices and usage data, which includes

> [S]earch history (including letters [users] key in for searches, and utterances provided if [users] choose to use voice search (if available on [the] Roku Device)), search results, content and advertisements [users] select and view and content settings and preferences, channels [users] add and view, including time and duration in the channels, and other usage statistics.[16]

Roku uses unique identifiers called "Roku Identifiers for Advertisers (RIDAs)" to track viewing activity and "try to understand [users] interests."[17] According to the company, Roku "supplement[s] that information with information collected from Roku Sites, Roku Mobile Apps or third party data sources to further personalize the advertising [consumers] see on [their] Roku Devices. [Roku] use[s] third party service providers, such as Google, to help deliver, personalize and target this advertising."[18] Third parties, including advertisers, also automatically collect information about Roku users, including "personally identifiable information about your online activities over time and across different websites, devices, online channels and applications when you use our services."[19]

In the Set-Top Box NPRM, the FCC states it is "encouraged by the fact that retail navigation devices, such as TiVos, have been deployed in the market for over a decade without allegations of a loss of consumer privacy . . . ."[20] This is inconsistent with the reality of

---

[15] *Products and Services*, TIVO RESEARCH, http://www.tivoresearch.com/ (last visited Apr. 21, 2016).
[16] *Roku Privacy Policy*, ROKU, https://docs.roku.com/doc/userprivacypolicy/en-us (last visited Apr. 21, 2016).
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] Set-Top Box NPRM at 36.

commercial data practices that capitalize on data-driven tracking and targeting across all screens and platforms.

The FCC makes an additional inconsistent claim in the NPRM that "today's smart TVs prove that we can preserve all the privacy, security, and copyright protections of the set-top box without that actual box."[21] In reality, smart TVs have been the subject of a host of lawsuits and legal complaints due to the tracking technologies deployed by these devices. In 2015, EPIC filed a complaint with the Federal Trade Commission ("FTC") concerning consumer privacy violations by Samsung's "always on" SmartTV that secretly recorded consumers' private communications. Vizio's Smart TV has also been the subject of multiple class action lawsuits for its invasive tracking practices, which were enabled by default and disclosed viewing activity connected with IP addresses for targeted advertising delivered to any device connected to that IP address.[22]

It appears that the FCC underestimates the powerful data-driven business models currently entrenched across the video delivery marketplace, which must be remedied through strong FCC enforcement of the Cable Subscriber Privacy Rules.

The FCC must not issue any final rule until the Cable Subscriber Privacy Rules are directly applied to all manufacturers and developers with access to cable subscriber data. The FCC can enact this critical consumer protection measure through use of its ancillary jurisdiction. Privacy regulations for all navigation devices are related to radio and wire communication services under Title I and would be reasonably ancillary to the FCC's effective execution of its

[21] *Id*. at 58.
[22] Pulkit Chandna, *Vizio Slapped With Two Class-Action Lawsuits Over Alleged Smart-TV Spying*, TECHHIVE (Nov. 17, 2015), http://www.techhive.com/article/3005718/smart-tv/vizio-slapped-with-two-class-action-lawsuits-over-alleged-smart-tv-spying.html.

duty under 47 U.S.C. § 551 to protect the privacy of cable subscribers.[23] Moreover, clear and enforceable privacy rules are necessary to provide meaningful consumer safeguards against invasive targeting and profiling practices and to uphold the Congressional intent of the Cable Act.

The FCC's proposal to require retail navigation device manufacturers to self-certify compliance with privacy rules fails to meaningfully protect consumers.[24] The proposal fails to provide for effective oversight and enforcement, and instead appears to deputize cable companies to enforce privacy rules on retail device manufacturers. Significantly, the proposal lacks clarity on whether the FCC could bring an enforcement action against device manufacturers for false certifications or violations of the Cable Subscriber Privacy Rules. Suggestions that the FTC would enforce privacy self-certifications provide little reassurance to consumers, as this agency rarely enforces the terms of its settlement agreements with privacy violators.[25]

Moreover, the proposal fails to affirmatively provide a private right of action or another meaningful recourse for consumers whose privacy rights are violated by retail navigation devices. Consumers have no clear direction on who to turn to – cable operators or retail device manufacturers – if their personal information is misused. Companies will have little incentive to comply with privacy rules without the deterrent of meaningful and robust enforcement. Private

[23] *See EchoStar Satellite L.L.C. v. F.C.C.*, 704 F.3d 992, 998 (D.C. Cir. 2013).
[24] Set-Top Box NPRM at 36.
[25] *See* Compl., *EPIC v. FTC*, 844 F. Supp. 2d 98 (D.C. Cir. 2012) (No. 12-206).

lawsuits are a key enforcement mechanism,[26] and the FCC must clarify the existence of this statutory right of action.

II. The FCC Must Clarify and Enhance Enforcement of Cable Subscriber Privacy Rules to Reflect Current Business Practices

Cable companies currently engage in extensive and invasive consumer tracking, profiling, and targeting across computers, mobile devices, and – increasingly – televisions. A report entered into the record for this proceeding by the Center for Digital Democracy provides an excellent overview of cable companies' current data practices.[27] The FCC must address these concerning practices with robust and meaningful enforcement of the Cable Subscriber Privacy Rules that reflects the reality of modern data practices.

Companies engaged in behavioral advertising no longer use an individual's name and address to track her activities and viewing habits; rather, they use persistent identifiers and other technologies to develop detailed profiles about consumers with a wealth of revealing information.[28] Cable companies are thus able to circumvent the Cable Subscriber Privacy Rules simply by asserting that they do not store or disclose "personally identifiable information," which they generally define as limited to names and addresses.[29] Cable companies also

---

[26] *Cannon v. Univ. of Chicago*, 441 U.S. 677, 705-06 (1979) ("The award of individual relief to a private litigant who has prosecuted her own suit is not only sensible but is also fully consistent with—and in some cases even necessary to—the orderly enforcement of the statute.").

[27] Center for Digital Democracy, *Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers* (Mar. 23, 2016) https://www.democraticmedia.org/article/big-data-watching-growing-digital-data-surveillance-consumers-isps-and-other-leading-video; *Filing by Center for Digital Democracy*, Federal Communications Commission, http://apps.fcc.gov/ecfs/comment/view?id=60001536229.

[28] Paul M. Schwartz & Daniel J. Solove, *The Pii Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1818 (2011).

[29] *See, e.g., Comcast Privacy Policy*, XFINITY (Aug 1, 2015), http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html ("However, we do not store or share your activity data in association with your name or address, except as necessary to render or bill for our services.").

circumvent privacy laws by tracking "household" viewing data, rather than the viewing data of an individual.[30] Specific households are targeted regardless of whether specific names are used, but the practical impact on consumer privacy is the same. Although companies may not use individual names to track and disclose viewing habit, this is simply semantics. These companies collect, use, and disclose every available detail about consumers *except* their names.

As Professor Jerry Kang explains in his analysis of the collection and use of personally identifiable information ("PII") by Internet firms, 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."[31] Information can be "identifiable" to a person in one of three ways: (1) authorship, (2) description, or (3) instrumental mapping.[32] 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 information.[33]

Cable companies also circumvent Cable Subscriber Privacy Rules with claims they use only anonymous or de-identified consumer data.[34] But even information that may seem anonymous when it is disclosed could be potentially linked to a known individual in the future.

---

[30] Jessica E. Vascellaro, *TV's Next Wave: Tuning In to You*, WALL ST. J. (Mar. 7, 2011), http://www.wsj.com/articles/SB10001424052748704288304576171251689944350?mg=id-wsj.
[31] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1207 (1998).
[32] *Id*.
[33] *Id*.
[34] *Comcast Privacy Policy*, XFINITY (Aug 1, 2015), http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html ("[W]e collect [user] *activity data* without names and addresses or other personally identifiable information and we consider it *de-identified* data.").

That is one the reasons why PII has been routinely defined in federal and state privacy laws to include information that both identifies or could identify an actual individual.[35] Moreover, cable companies and their marketing partners rely on usernames, IP addresses, and other digital data to identify and track users across the web, and to deliver targeted ads.[36] These firms are not only capable of identifying and tracking users using this data, it is their entire business model.

Companies that claim to deal only in "anonymous" data, "do not mean that they have no way to distinguish a specific person," or that "they have no way to recognize [the user] as the same person with whom they have interacted previously."[37] Instead, these companies simply mean that they "rely on unique persistent identifiers that differ from those in common and everyday use (i.e. a name and other so-called [PII])."[38] The widespread use of the Social Security number ("SSN") illustrates the limitations of a name-focused conception of PII. On its own, an SSN is nothing more than a nine-digit number. Large institutions, however, frequently use SSNs for identification because they are "necessarily more unique than given names, the more common of which (e.g. John Smith) could easily recur multiple times in the same database."[39] This is precisely the case with unique persistent identifiers that are routinely swept up by online

[35] *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").
[36] *See* Jessica Rich, Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, *Beyond Cookies: Privacy Lessons for Internet Advertising* (Jan. 21, 2015), https://www.ftc.gov/system/files/documents/public_statements/620061/150121beyondcookies.pdf.
[37] Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent, in Privacy, Big Data, and the Public Good* 53 (Julia Lane et al. eds. 2014).
[38] *Id*.
[39] *Id*. at 54.

companies. Thus, any realistic discussion of PII must consider the collection, storage, or disclosing of unique persistent identifiers beyond names.

It is well established that IP addresses and other unique, persistent identifiers constitute personal information that "can be used to recognize a user over time and across different websites or online services."[40] IP addresses can be used to identify users and link consumers to television viewing data. They are akin to Internet versions of consumers' home telephone numbers. The FCC must clarify its enforcement of the Cable Subscriber Privacy Rules to include IP addresses and other unique, persistent identifiers as PII subject to privacy protections.

III. Conclusion

For the foregoing reasons, EPIC urges the FCC to apply the Cable Subscriber Privacy Rules directly to retail navigation device manufacturers and other providers with access to cable subscriber data, and to clarify and strengthen enforcement of these important privacy rules to reflect the reality of modern data practices.

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associated Director and
Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Counsel

[40] Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.