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
	)	

OPPOSITION TO PETITIONS FOR RECONSIDERATION

The Center for Digital Democracy (CDD) and Campaign for a Commercial Free Childhood ("CCFC"), by their attorneys, the Institute for Public Representation ("IPR"), along with Common Sense Kids Action, Consumer Action, and the Electronic Privacy Information Center ("EPIC"), (collectively "Children's Advocates") oppose the petitions for reconsideration of the broadband privacy rules adopted in the above-referenced proceeding.

The broadband privacy rules are intended to give consumers the tools they need to make informed decisions about how their information is used by their ISP. To this end, the rules require ISPs to obtain opt-in approval for use and sharing of sensitive customer personal information.[1]

Children's Advocates oppose the request of some petitioners to rescind the rules in their entirety.[2] Because the FTC's Section 5 jurisdiction does not extend to common carriers,[3] the

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, (rel. Nov. 2, 2016) [hereinafter *Order*].

[2] *E.g.*, American Cable Association Petition for Reconsideration, WC Docket No. 16-106, at 3 (filed Jan. 3, 2017); NCTA Petition for Reconsideration, WC Docket No. 16-106, at 1 (filed Jan. 3, 2017).

[3] Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2016).

effect of rescinding the rules in their entirety could mean that parents would have no control over their ISP's use of their children's information.

Children's Advocates also oppose petitions to modify the broadband privacy rules by changing the classification of certain sensitive information to nonsensitive, or replacing opt-in consent with opt-out.[4] As discussed below, these proposed modifications would significantly weaken privacy protections for children.

A. Treating Children's Information as Sensitive and Requiring Notice and Opt-In Consent is Necessary to Protect Children and Consistent with the FTC's Practices.

The broadband privacy rules define sensitive customer proprietary information to include "financial information; health information; Social Security numbers; precise geo-location information; *information pertaining to children*; content of communications; call detail information; and a customer's web browsing history, application usage history, and their functional equivalents."[5] None of the eleven petitioners seeking reconsideration of the broadband privacy rules challenges the Commission's determination that children's information is sensitive and deserving of protection.

Some petitioners urge the FCC to modify the rules to ensure consistency with the FTC's approach to privacy.[6] In the case of children's privacy, however, the FCC's rules are already consistent with the FTC's approach. In determining which categories are sensitive, the FCC

[4] *E.g.*, United States Telecom Association Petition for Reconsideration, WC Docket No. 16-106, at 1-2 (filed Jan. 3, 2017); CTIA Petition for Reconsideration, WC Docket No. 16-106, at 6-7 (filed Jan. 3, 2017).

[5] *Order* at ¶177 (emphasis added).

[6] *See, e.g.*, NCTA Petition for Reconsideration, WC Docket No. 16-106, at 16 (filed Jan. 3, 2017); Consumer Technology Association Petition for Reconsideration, WC Docket No. 16-106, at 5 (filed Jan. 3, 2017); Oracle Petition for Reconsideration, WC Docket No. 16-106, at 2 (filed Dec. 21, 2016).

explicitly looked to the FTC for guidance, noting that the FTC regards children's information along with health information, financial information, and social security numbers to be sensitive categories.[7]

The FCC also looked to the Children' Online Privacy Protection Act (COPPA), which is enforced by the FTC.[8] A major purpose of COPPA was to limit advertising targeted to children by prohibiting the collection, use, and dissemination of personal information from children without informed, advance parental consent.[9] In introducing the legislation, Senators Richard Bryan and John McCain explained that the legislation was necessary to prevent marketers from targeting and exploiting children:

> Unfortunately, the same marvelous advances in computer and telecommunication technology that allow our children to reach out to new resources of knowledge and cultural experiences are also leaving them unwittingly vulnerable to exploitation and harm by deceptive marketers . . .
>
> Web sites were using games, contests and offers of free merchandise to entice children to give them exceedingly personal and private information about themselves and their families. Some even used cartoon characters who asked children for personal information . . .
>
> The Internet gives marketers the capability of interacting with your children and developing a relationship without your knowledge.[10]

In 2013, the FTC revised the COPPA rules to ensure that marketers could not use newer forms of online tracking to profile or target advertising to children. It amended the definition of

---

[7] *Order* at ¶178. *See also* FEDERAL TRADE COMMISSION STAFF REPORT, *Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009) at ii, 10; FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012) at 15-16; FEDERAL TRADE COMMISSION STAFF REPORT, *Cross-Device Tracking* (Jan. 2017) at 1 [hereinafter *Cross-Device Tracking*].

[8] *Order* at n.487.

[9] 144 CONG. REC. S8482-83 (July 17, 1998).

[10] *Id.*

"personal information" to include "persistent identifiers that can be used to recognize a user over time and across different websites or online services, such as a cookie, IP address, serial number, or unique device identifier."[11] Thus, under the revised rules

> Without parental consent, operators may not gather persistent identifiers for the purpose of behaviorally targeting advertising to a specific child. They also may not use persistent identifiers to amass a profile on an individual child user based on the collection of such identifiers over time and across different Web sites in order to make decisions or draw insights about that child, whether that information is used at the time of collection or later.[12]

In sum, the FCC's requirement that children's information should be treated as sensitive information is consistent with the FTC's approach. Indeed, a recent FTC report on Cross-Device Tracking recommended that companies refrain from cross-device tracking on sensitive topics including children's information without consumers' affirmative express consent.[13] The FCC's rules are also similar to the parental notice and consent requirements imposed by the FTC's COPPA rules. Like the COPPA rules, the FCC's broadband privacy rules require notice that is "clear and conspicuous, comprehensible, and not misleading."[14] Similarly, the FCC's rules require opt-in consent.[15] Thus, the broadband privacy rules are consistent with the FTC approach and are necessary, although not sufficient, to protect children's privacy.

---

[11] *Cross-Device Tracking*, at n.76.

[12] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3981 (2013) (to be codified at 16 C.F.R. pt. 312). *See also* Jon Leibowitz, Former Chairman, FTC, Statement on Updated COPPA Rule, (Dec. 19, 2012), https://www.ftc.gov/public-statements/2012/12/statement-ftc-chairman-jon-leibowitz-updated-coppa-rule-prepared-delivery ("We also extend the Rule to cover persistent identifiers like IP addresses and mobile device IDs, which could be used to build massive profiles of children by behavioral marketers.").

[13] *Cross-Device Tracking*, at 15.

[14] Compare *Order* at ¶ 122-23, with 16 C.F.R. §312.4.

[15] Compare *Order* at ¶ 167, with 16 C.F.R. § 312.5. In fact, the COPPA rule goes further in requiring that online operators generally obtain verifiable parental consent before any personal information from children is collected, used, or disclosed.

B. Web Browsing and Application Usage Histories Must be Treated as Sensitive Information

The broadband privacy rules also treat other categories of information -- including web browsing and application usage -- as sensitive. The *Order* explains that "BIAS providers' gatekeeper position allows them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents."[16] Web browsing and application usage histories contain extremely intimate information that may be used to gain insight into a customer's beliefs, preferences, and potential future activities.[17] Thus, Children's Advocates oppose petitions that seek to reclassify this information as non-sensitive.[18]

As CDD showed in its report, *Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers*, ISPs have the ability to track customers across platforms.[19] ISPs know when a consumer is online, what a consumer is doing, and whether the internet is being accessed from a mobile phone, computer, or television.[20] AT&T's ad division, AdWorks, for example, claims to enable marketers to "reach your audience everywhere they watch on every screen."[21] Comcast harvests "terrabytes" of data from its set-

---

[16] *Order* at ¶ 30.

[17] *Order* at ¶ 181, 183.

[18] *E.g.*, NCTA Petition for Reconsideration, WC Docket No. 16-106, at 20 (filed Jan. 3, 2017); Wireless Internet Service Providers Association Petition for Reconsideration, WC Docket No. 16-106, at 20 (filed Jan. 3, 2017).

[19] CENTER FOR DIGITAL DEMOCRACY, *Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers* (Mar. 2016) at 3, https://www.democraticmedia.org/sites/default/files/field/public-files/2016/ispbigdatamarch2016.pdf [hereinafter *Big Data is Watching*]. This study was submitted to Docket 16-106 on May 23, 2016. *See also Cross-Device Tracking*, at 1 (discussing how advertisers "can analyze an individual consumer's activities based not only on her habits on one browser or device, but on her entire 'device graph' – the map of devices that are linked to her, her household, or her other devices. Often, companies combine the information from a consumer's device graph with offline behavior, such as purchases at brick-and-mortar stores.").

[20] *Big Data is Watching*, at 3.

[21] *Id.* at 4 (citations omitted).

top boxes, combines it with data from its IP-based systems and other sources, and uses "big data" techniques to buy and sell individuals to marketers.[22] Companies, such as Verizon, are optimizing data mining to gather real-time insights. Verizon plans to unveil two platforms that combine clickstream (pages a website visitor goes to), location, and demographic (age, gender, income, etc.) data in two to three seconds.[23] Because data analytics and modeling allow for inferences of the most personal traits, characteristics, likes and dislikes of any person or group of persons, use of this information without consent is harmful for all consumers, and particularly for children.[24]

Marketers are intensely interested in targeting children and adolescents.[25] The Coalition for Innovative Media Measurement, for example, has initiated a project to "make possible a thorough and comprehensive view of cross-platform, digital and mobile measurement of content and ads among children and teens aged 2 to 17."[26]

As the Commission has long understood, children lack the cognitive capacity to identify advertising, understand its purpose and defend against it.[27] Today's generation of children will be the first to have a digital footprint for their entire lives. The quantity and detail of this

---

[22] *Id.* at 5. Comcast has also invested in Videology, a television and video advertising specialist that integrates consumer and personal information from mobile devices, tablets, computers, and connected televisions. *Id.* at 38; VIDEOLOGY, https://videologygroup.com/about-us/ (last visited Mar. 1, 2017).

[23] KDD2016 Video, *Large Scale Machine Learning at Verizon: Theory and Applications*, YOUTUBE (Sept. 5, 2016), https://www.youtube.com/watch?v=KKNoyWmbK1k.

[24] *Big Data is Watching*, at 7.

[25] Lindsay Rowntree, *How Kids' Digital Media is Turning into a Multi-Billion-Dollar Opportunity*, EXCHANGEWIRE, Apr. 20, 2016, https://www.exchangewire.com/blog/2016/04/20/how-kids-digital-media-became-the-hottest-market-in-the-world/.

[26] *Big Data is Watching*, at n.41.

[27] Children's Television Report and Policy Statement, 50 FCC 2d 1, 5 (1974). *See generally* Angela J. Campbell, *Rethinking Children's Advertising Policies for the Digital Age*, 29 LOY. CONSUMER L. REV. 1 (2016).

information makes children especially vulnerable to targeted marketing.[28] If ISPs were permitted to use children's web browsing and app usage data without parental permission to market directly to children, or to sell this information to others for marketing, advertisers would have a much greater ability to take unfair advantage of children.

C. The FCC Should Retain Opt-In Requirements for Use of All Categories of Sensitive Information

Children's Advocates also oppose changing the requirement that ISPs obtain opt-in consent before collecting sensitive web browsing and application usage histories. The web browsing and online activity of children and teens are "inextricably intertwined" with adult activities of this kind. [29] As a result, ISPs either would not distinguish data collected from children from that of adults, which would result in little to no protection for children's personal information, or they would need to examine the data in more detail to determine its source. The alternative of requiring ISPs to determine the source of the information would be both costly and likely to further invade the privacy of both children and adults.[30]

USTA argues for opt-out consent because most consumers will withhold consent.[31] Yet if anything, this argument cuts in favor of setting opt-in as the default. Because most consumers tend to stay with the default option,[32] opt-in consent will provide greater protection for children.

---

[28] *See, e.g.*, Samantha Graff et al., *Government Can Regulate Food Advertising To Children Because Cognitive Research Shows That It Is Inherently Misleading*, 31 HEALTH AFFAIRS 392 (2012).

[29] Reply Comments of Center for Digital Democracy and Common Sense Kids Action Regarding Children and Teens, WC Docket No. 16-106, at 3 (filed July 6, 2016).

[30] *Ex Parte* Letter filed by New America's Open Technology Institute, Center for Digital Democracy, Common Sense, et al., WC Docket No. 16-106, at 2 (filed Sept. 12, 2016).

[31] United States Telecom Association Petition for Reconsideration, WC Docket No. 16-106, at 7 (filed Jan. 3, 2017).

[32] *Order* at n.558.

Opt-in consent also helps to protect teens, who are particularly vulnerable to targeted marketing but for different reasons than children.[33]

Further, it is unreasonable to put the burden of opting out on parents. Parents typically are not equipped to assess the risks of disclosing information. They are unlikely to know what information is collected simply by virtue of subscribing to an ISP, nor do they know how it will be combined with information from other sources, or how that information will be used in the future.[34] It is the obligation of ISPs to make a convincing case to parents that opting into the ISP's data practices is in their children's best interests.

Finally, some petitioners contend that opt-in will confuse consumers and conflict with consumer preferences.[35] Yet, parents have come to expect opt-in consent with respect to the collection and use of children's information. Because parents are accustomed to providing advance, verifiable consent for child-directed websites or online services, they may incorrectly assume that their children's information will be protected if they do nothing. Moreover, the fact that opt-out consent is used in other telecommunications areas, such as the Do Not Call Registry,[36] does not mean that opt-out would be effective in the ISP context to protect children. A prerecorded call from a telemarketer is simply not comparable to targeted marketing messages based on data profiles of the broad information collected by ISPs.

---

[33] Reply Comments of Center for Digital Democracy and Common Sense Kids Action Regarding Children and Teens, WC Docket No. 16-106, at 2-4 (filed July 6, 2016).

[34] Privacy policies, which are rarely read, typically do not provide sufficient information. The information these policies do provide is so full of jargon that most consumers would not understand it. In fact, the FTC found that a majority of top websites do not include clear disclosures about if and how cross-device tracking is occurring. *Cross Device Tracking*, at 8.

[35] *See, e.g.*, Competitive Carriers Association Petition for Reconsideration, WC Docket No. 16-106, at 11 (filed Jan. 3, 2017); American Cable Association Petition for Reconsideration, WC Docket No. 16-106, at 20-21 (filed Jan. 3, 2017).

[36] CTIA Petition for Reconsideration, WC Docket No. 16-106, at 10 (filed Jan. 3, 2017).

CONCLUSION

For all the above reasons, the Commission should deny the petitions for reconsideration seeking to overturn or modify the broadband privacy rules.

Respectfully submitted,

/s/ Angela J. Campbell

Angela J. Campbell
Chris Laughlin
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, N.W.
Washington, D.C. 20001
Counsel for CDD and CCFC

Ariel Fox Johnson
Senior Policy Counsel
Common Sense Kids Action

Jim Graves
Law and Technology Fellow
Electronic Privacy Information Center

Linda Sherry
Director of National Priorities
Consumer Action

March 6, 2017

CERTIFICATE OF SERVICE

I, Cassandra Vangellow, hereby certify on this 6th day of March, 2017, a copy of the foregoing Opposition to Petitions for Reconsideration was served by first-class mail, postage prepaid, upon the following:

Jonathan Banks
B. Lynn Follansbee
607 14th Street, NW, Suite 400
Washington, D.C. 20005

Steven K. Berry
Rebecca Murphy Thompson
Elizabeth Barket
Competitive Carriers Association
805 15th Street NW, Suite 401
Washington, DC 20005

Thomas Cohen
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, DC 20007

Stephen E. Coran
S. Jenell Trigg
Paul A. Cicelski
Lerman Senter PLLC
2001 L Street, NW, Suite 400
Washington, DC 20036

Kenneth Glueck
Oracle Corporation
1015 15th St. NW, Suite 200
Washington, DC 20005

Christopher J. Harvie
Ari Z. Moskowitz
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.
701 Pennsylvania Avenue, N.W., Suite 900
Washington, D.C. 20004

Stuart P. Ingis
Michael Signorelli
Robert Hartwell
Venable LLP
575 7th Street, NW
Washington, D.C. 20004

Julie M. Kearney
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

Genevieve Morelli
Michael J. Jacobs
ITTA
1101 Vermont Ave., NW, Suite 501
Washington, D.C. 20005

Thomas C. Power
Maria Kirby
Scott K. Bergmann
CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036

Brita D. Strandberg
Adrienne E. Fowler
Elizabeth B. Uzelac
Harris, Wiltshire & Grannis Llp
1919 M Street, N.W., 8th Floor
Washington, DC 20036

/s/ Cassandra Vangellow
Cassandra Vangellow