Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

REPLY COMMENTS OF CENTER FOR DIGITAL DEMOCRACY AND COMMON SENSE KIDS ACTION REGARDING CHILDREN AND TEENS

The Center for Digital Democracy and Common Sense Kids Action, on behalf of millions of children, teens, and their families, are pleased to submit these reply comments in response to the Notice of Proposed Rulemaking In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services by the Federal Communications Commission (the "Commission" or "FCC"). We support the Commission's efforts to enhance the privacy of all Americans on broadband networks. And we believe it is particularly important to protect vulnerable children and teens on these networks.

In today's big data environment, where even innocuous data or third party information can be used to identify personal characteristics given the totality of information collected, children and teens are particularly vulnerable. They are more apt to share information, more susceptible to privacy harms, and heavy users of broadband whose information is intermingled on the network, such that providers may not know they are dealing with children and teens absent further privacy intrusions and data inspection. Therefore, strong overall rules protecting personal information on broadband networks are necessary. In general, personal information collected by broadband providers should only be used to provide broadband services unless there is opt-in consent. Furthermore, if providers are intentionally targeting children or teens, greater transparency and parental control are needed.

- **Everyone Agrees Children Are Vulnerable And Merit Opt-In Protection.** Even in the United States, where there are few protections giving individuals control over their information, children's information has long been considered sensitive and meriting opt-in protection. This is because children are vulnerable. They are more apt to share online and often unaware of how their behavior can be monitored, stored, and used by online companies, including the Internet Service Providers (ISPs) that supply broadband to their homes and schools. Children are unlikely to adopt complex security mechanisms like encryption. Their information—including their user data,

usage data, and inference data of the type that enables a provider to make accurate assumptions about children within a household—can be used to develop dossiers that track and profile them from birth, with potentially devastating long-term consequences for kids who are just developing their voices and need the freedom to make mistakes and learn and grow. Their information can also be used to target personalized ads, to which young people are particularly susceptible.[1] Indeed, even in this rulemaking, entities of all stripes have acknowledged the particular vulnerability of children. Even those who otherwise largely oppose the FCC's proposed framework acknowledge and accept the benefits of protecting young people, and the risks of collecting their information without opt-in consent are widely acknowledged and accepted.[2]

- **Teens Are Vulnerable Too.** There is a growing understanding that teens are particularly vulnerable as well.[3] Teens are also apt to share information. They tend to act impulsively, without fully thinking through consequences,[4] and live in a culture that promotes sharing 24/7, with no signs of abatement.[5] Moreover, they too are learning and developing their voices, and they deserve the freedom to explore without it costing them their college admissions, future careers, or ability to find housing.[6]

---

[1] Children under eight, for example, do not understand the intent is to sell them something, and very few older children can distinguish paid search ads from organic results. *See, e.g.,* Workgroup on Children's Online Privacy Protection, Report to the Maryland General Assembly on Children's Online Privacy, 16 (Dec. 30, 2013); Ofcom, Children and Parents: Media Use and Attitudes Report 2015 (Nov. 20, 2015), http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parentsnov-15/ (only 16% of children 8-11 could distinguish between ads and search results).

[2] *See, e.g.,* Comments In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services WC Docket 16-106 ("Broadband Privacy Proceeding") filed by Federal Trade Commissioner Maureen Ohlhausen, Hughes Network Systems, ICLE, Internet Commerce Coalition, NCTA, SIAA, T-Mobile, USTA, Verizon, Larry Tribe, Association of National Advertisers, Century Link, Comcast, Consumer Electronics Association, and CTIA. Other experts, like the Federal Trade Commission Staff, have also reiterated the importance of opt-in consent for children's information.

[3] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, 47, 60 (Mar. 2012) (stating that when sensitive data such as "children's information is involved … the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased," and that, "companies that target teens should consider additional protections."). *See also* Do Not Track Kids Act of 2015, H.R. 2734, 114th Cong. (2015); Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, 55 (May 2014) (noting that principles underlying the Children's Online Privacy Protection Act may apply equally in offline contexts, and that teens often fail to appreciate long-term consequences of posting data online); Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 25-26 (May 2014) (noting young people "need appropriate freedoms to explore and experiment safely and without the specter of being haunted by mistakes in the future").

[4] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, 70 (Mar. 2012).

[5] Teens average over an hour a day of social media use. Common Sense Media, Common Sense Census: Media Use by Tweens and Teens, Executive Summary, 31 (Nov. 3, 2015), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens. At least 90% of teens have used social media. See Common Sense Media, Social Media, Social Life: How Teens View Their Digital Lives, 9 (June 26, 2012), https://www.commonsensemedia.org/file/socialmediasociallifefinal-061812pdf-0/download.

[6] More and more admissions officers, employers, and even landlords are mining social media. *See* Kaitlin Mulhere, Lots More College Admissions Officers Are Checking Your Instagram and Facebook, Time, Jan. 13, 2016, *http://time.com/money/4179392/college-applications-social-media/* (40% of admissions officers looked at social media, 4x more than in 2008, and a third discovered something that hurt the applicant's

- **Current Rules Leave Vulnerable Children And Teens At Risk.** Some commentators assert that the Children's Online Privacy Protection Act (COPPA) will adequately protect children.[7] While COPPA provides many protections, it does not govern the entire internet ecosystem and provides limited protection to families and youth in the broadband network context. COPPA only applies to children under 13, and only applies to online operators who are deemed child-directed or who have actual knowledge that they collect personal information from children.[8] Children and teens will receive much needed safeguards that help supplement long-standing policy safeguards addressing fair consumer and data collection practices to youth if the FCC proceeds with its plans. In today's big data environment, the FCC's rules will provide parents with necessary additional safeguards that help ensure the goal of COPPA is maintained.

- **Young People's Information Is Inextricably Intertwined In The Network.** Children and teens are avid media users, with more access to devices and the internet than ever before. They are required to use the internet for school, and are on it almost constantly at home and on the go, as parents can attest. They are ready adopters of new technology. And, they are particularly heavy users of mobile devices, which can collect sensitive data like geolocation anytime and anywhere.[9] Tweens and teens spend, respectively, over four and over six hours a day with screens, half of which are mobile.[10] All of this highly detailed information about vulnerable children and teens is getting sent over the same network as other information, inextricably intertwined. Indeed, as persuasively explained by telecommunications experts like Public Knowledge, providers would be hard pressed to determine which information is that of a child or teen unless they dug even deeper and manually inspected all the

---

chances); Careerbuilder, Number of Employers Passing on Applicants Due to Social Media Posts Continues to Rise, June 26, 2014, *http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014* (43% of employers use social media to research employees, and 51% of employers in 2014 had found information on social media that caused them not to hire the individual, up from 2012); Caitlin Dewey, Creepy startup will help landlords, employers and online dates strip-mine intimate data from your Facebook page, Washington Post, June 9, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/06/09/creepy-startup-will-help-landlords-employers-and-online-dates-strip-mine-intimate-data-from-your-facebook-page/ (Tenant Assured, for landlords, already live).

[7] *See* Comments of Internet Commerce Coalition and Sprint in Broadband Privacy Proceeding.

[8] *See* Comments of Center for Digital Democracy and Common Sense Kids Action in Broadband Privacy Proceeding.

[9] Twice as many young children used mobile devices in 2013 than just two years prior, and 38% of toddlers under age two have used a mobile device. *See* Common Sense Media, Zero to Eight: Children's Media Use in America, 11 (Oct. 28, 2013), https://www.commonsensemedia.org/file/zerotoeightfinal2011pdf 0/download. 91% percent of teenagers use their mobile devices to go online. *See* Pew Research Center, Mobile Access Shifts Social Media Use and Other Online Activities (Apr. 9, 2015), http://www.pewinternet.org/2015/04/09/mobile-access-shifts-socialmedia-use-and-other-online-activities/.

[10] Common Sense Media, Common Sense Census: Media Use by Tweens and Teens, 16, 20 (Nov. 3, 2015), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens.

information flowing through their network.[11] The intertwined nature of the data, and the sorting of data into sensitive and non-sensitive categories related to vulnerable and less-vulnerable populations, would require further analysis and further violations of privacy. Such activities would run exactly counter to the FCC's intention of providing individuals with greater control over their personal information. Therefore, the overall rule for all information should be opt-in. And, given the particular vulnerability of children and teens, when providers specifically target them, greater transparency and parental control should be required.

We believe that privacy protections for children and teens need to be strengthened across the board, including in Congress, at the Federal Trade Commission, and at the FCC, where the envisioned broadband privacy rules are necessary to capture the entire ecosystem. Children, teens, families, and all users of broadband deserve the right to control what happens to their personal information on the network, and the FCC should move forward with its proposed privacy framework. The risks of not doing so are particularly acute for young people, who are just getting their start in the world. We look forward to working with the Commission on this important issue.

Respectfully submitted,

/s/ Ariel Fox Johnson
Ariel Fox Johnson
Senior Policy Counsel, Privacy and Consumer Affairs
Common Sense Kids Action
2200 Pennsylvania Ave NW, 4E
Washington, DC 20037

July 6, 2016

[11] *See* Comments of Public Knowledge in Broadband Privacy Proceeding, noting that providing heightened protection to sensitive information on broadband networks "is not feasible, as it would necessarily require ISPs to first determine whether sensitive information is present in any given communication — a task necessarily requiring manual inspection of each packet — before applying the appropriate amount of protection. DPI is not only impractical, but contrary to both the letter and spirit of privacy regulation. …In addition, there is no way that DPI could be implemented with any meaningful consent regime. … We agree with the FTC's recognition that certain types of data are, prima facie, more sensitive than others. The only way to ensure those extra-sensitive communications are given adequate protection against collection and dissemination by ISPs is to assume that all communications could potentially contain such highly sensitive information." (24-25.)