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**
	)	
	)	

COMMENTS OF COMMON SENSE KIDS ACTION

James P. Steyer
Founder and CEO
Common Sense Media

Ariel Fox Johnson
Senior Policy Counsel,
Privacy and Consumer Affairs
Common Sense Kids Action

650 Townsend Street, Suite 435
San Francisco, CA 94103

May 27, 2016

TABLE OF CONTENTS

I. Introduction

Common Sense Kids Action, the advocacy arm of Common Sense Media (collectively, "Common Sense"), is pleased to submit these 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"). Common Sense is a national, independent, nonpartisan voice for America's children, working to ensure that every child has the opportunity to thrive in the 21st century. Common Sense has researched media and technology use by children and teens from a variety of perspectives. Our most recent reports include: *Children, Teens, Media, and Body Image* (2015), *The Common Sense Census: Media Use by Tweens and Teens* (2015), and *Technology Addiction: Concern, Controversy, and Finding Balance* (2016). We appreciate the Commission's longstanding commitment to protecting communications privacy.

We support the privacy rights of all Americans. But these comments, and our efforts, focus on the privacy rights of children and teens. Young people are constantly online. With the explosive growth of digital devices and smart phones, education technology in the classroom, and social and mobile media, today's youth are living out their days almost entirely online at home, at school, and in between. This generation of children is the first to have a digital footprint for their entire lives.

New connectivity offers a wonderful potential for our kids to learn, communicate, and create—as well as the potential for online actors to amass personally identifiable information about young people that can be tracked, mined, and exploited. Kids and students are particularly vulnerable in two ways. First, kids and students are often unaware of the ways in which their online behavior can be monitored, stored, and used by online companies, including the Internet Service Providers (ISPs) that supply broadband to their homes, schools, and libraries. Second, with the advent of technology in schools, young people have no choice but to engage online and, as a result, unwittingly share information about themselves over the internet. Sensitive information can find its way to unintended audiences with unexpected consequences for children and families. Marketers can create dossiers beginning at birth of a young person's interests, finely tuning sales pitches to impressionable audiences who may not even understand they are seeing ads. Profitable profiles can be developed, labeling and potentially limiting opportunities for education and jobs as kids are tracked and channeled.

Young people need the freedom to make mistakes, try new things, and find their voices, unencumbered by the looming threat of a permanent digital record. Failure to appropriately address privacy protections for young people could temper their online exploration and lead them to self-censor their thoughts or withhold information. It could squelch expression or limit opportunities for development.

The entire online ecosystem requires stronger privacy protections than are in place today. It is important for all online actors to be transparent and responsible with young

people's information. This is why Common Sense has fought for updates to the Children's Online Privacy Protection Act (COPPA), robust rules for educational technology products, through laws such as California's Student Online Personal Information Protection Act (SOPIPA), rules governing data brokers and app operators, and more. Because different actors play different roles, privacy concerns—and the best way to address them—can vary. This is reflected in our sectoral system of privacy regulations. Here, the Commission has a statutory mandate to protect privacy on telecommunications services.[1] Broadband is the foremost telecommunications service of our time, with broadband networks carrying vitally important communications and sensitive information on a constant basis.

It is necessary that the FCC act to protect communications on broadband networks. In 1980, FCC Chairman Charles D. Ferris presciently foresaw a time

> "when my children's homes are wired, a computer will have a record of what they buy and how much they spend. It will know whether they pay bills quickly, slowly or not at all and it will know where all their money comes from. It will know whether they watched the debates, or the football game or a controversial movie. In other words, it will know more about them than anyone should."[2]

He then proposed that, "We can and should move at the outset of this information era to address the potential privacy problem so that it in fact does not become an actual one." While we are well past the outset of the information era, we are also well past the time when privacy problems are "potential," not having put in place strong enough consumer protections at the beginning.[3] Now is the time to act.

The Commission's proposed framework provides a strong foundation on which to protect broadband users' privacy—including children and teens and school and library users. Common Sense supports one strong overall rule and special protections in the unique school and library context:

- Because children and teens' information is sensitive, and because children and teens are more apt to share information, more vulnerable 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 intrusions—strong overall rules are necessary. **In general, personal information collected by broadband providers should only be used to provide broadband services unless there is opt-in consent.**

[1] Telecommunications Act, 47 U.S.C § 222 (c)(1); *see also* 47 U.S.C. § 222(a) (carriers must protect confidentiality of other proprietary customer information in addition to CPNI); 47 U.S.C. § 201(b) (carrier practices must be just and reasonable).
[2] *Official Warns on Privacy*, NY TIMES, Oct. 14, 1980.
[3] *See* Ohm, *infra* n.10, at 1148 ("far too many people continue to suffer harm from data in databases without protection or possibility for redress," including stalking, blackmail, discrimination and harassment by companies, and censorship).

- If, however, the FCC determines that certain categories of information will receive heightened protection, **children and teens' information should receive the utmost protection.**

- In schools and libraries, there are unique circumstances governing access, consent, and the customer relationship. These circumstances merit—and the nature of access through one point allows for—specific safeguards that ensure information is not used for any purpose other than providing necessary services without an individual's consent, and **providers should not be allowed to use personal information collected from schools and libraries for any purpose other than providing broadband services.**

II. Children And Teens Share A Lot of Information Online, Which Has Long Been Recognized As Sensitive And Deserving of Protection

Children and teens are avid media users. Children today have more access to devices and the internet than ever before. They are the first to have a digital trail spanning the length of their entire lives, if not longer.[4] They are avid adopters of new technology. And children and teens are particularly heavy users of mobile devices,[5] which can collect sensitive data like geolocation anytime and anywhere. By the age of four, over half of children have their own mobile devices.[6] More than half of tweens have their own tablets.[7] And tweens and teens spend, respectively, over four and over six hours a day with screens, half of which are mobile.[8] Indeed, almost all teens use mobile devices to go online daily. A quarter of teens report using the internet constantly.[9] And, in school, the proliferation of educational technology and digitization of school records and activities—from nurse visits to student keystrokes—means digital dossiers that are lengthier and more persistent than any paper file.

---

[4] At least a quarter of children have an online presence before being born. *See, e.g.,* Business Wire Press Release, Digital Birth: Welcome to the Online World – AVG Study Finds a Quarter of Children Have Online Births Before Their Actual Birth Dates (Oct. 6, 2010), (http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth- Online-World).

[5] 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 in the last two years. *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-social-media-use-and-other-online-activities/.

[6] 96.6% of children between the ages of 6 months and 4 years old have used mobile devices. Among children who were 4, half had their own television and three-quarters their own mobile devices. *See* Hilda Kabali et al., *Exposure and Use of Mobile Media Devices by Young Children,* Vol. 136, No. 6 (Dec. 2015), http://pediatrics.aappublications.org/content/early/2015/10/28/peds.2015-2151.

[7] Common Sense Media, Common Sense Census: Media Use by Tweens and Teens, 22-23 (Nov. 3, 2015), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens.

[8] *Id.* at 16, 20.

[9] 92% of teenagers go online daily. 56% of teenagers report using the internet many times a day, and 24% admit to using the internet "almost constantly." *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-social-media-use-and-other-online-activities/.

Children's information has long been recognized as sensitive,[10] and, there is growing understanding that teens' information is sensitive as well.[11] For these reasons, special rules typically apply when dealing with children and teens at the federal and state levels—they are among the few Americans whose online privacy has specific safeguards. In the states, laws like California's Eraser Button Law and Delaware's Online Privacy and Protection Act give children and teens rights with respect to their online postings, or regulate certain advertising on child and teen-directed sites.[12]

a. COPPA Provides Limited Protection In These Circumstances

The primary federal law protecting children online is the Children's Online Privacy Protection Act (COPPA).[13] COPPA was passed by Congress in 1998. The Federal Trade Commission (FTC) oversees COPPA and last updated the COPPA regulations in 2013. COPPA was designed to give parents control over what personal information child-directed websites and apps, and websites and apps with actual knowledge of child users, collect from children under 13. COPPA is most well-known for its requirement of verifiable parental consent before sites collect or disclose personal information from children. COPPA also contains disclosure and notice requirements, as well as security guidelines.[14]

Nonetheless, COPPA—like most U.S. privacy rules—does not govern the entire ecosystem and provides limited protections to families and youth in the broadband network context. First, COPPA does not apply at all to anyone 13 and older.[15] So, even a 13-year-old is treated exactly like an adult under COPPA. Second, to the extent that broadband providers are acting as common carriers subject to Title II of the telecommunications act—and therefore to the privacy rules proposed by the FCC here—they are arguably exempt

---

[10] As articulated by Paul Ohm in *Sensitive Information,* "sensitive information" is widely discussed but under-theorized. Ohm finds four factors that lead to an information's sensitivity: it can lead to significant forms of harm; it exposes the data subject to a high probability of harm; it is often transmitted in a confidential setting (such as between a teacher and a student); it involves harms that apply to the majority of data subjects (such as all children and anyone with children). Paul Ohm, *Sensitive Information,* 88 S. Cal. L. Rev. 1125, 1158 (2014-2015).

[11] 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"); Federal Trade Commission, Mobile Privacy Disclosures: Building Trust Through Transparency, 23 (Feb. 2013) (noting children's data is sensitive and apps should provide notice and obtain affirmative express consent when collecting or sharing such information).

[12] Cal. Bus. & Prof. § 22580; 80 Del. Laws, c. 148, § 1 (2015).

[13] Children's Online Privacy Protection Act, 15 U.S.C. § 6501.

[14] *See* 16 C.F.R. § 312.

[15] As noted above, there have been repeated efforts to increase protections for teens. *See, e.g.,* Do Not Track Kids Act of 2015, H.R. 2734, 114th Cong. (2015) and previous legislative efforts in 2011 and 2013.

from COPPA enforcement as the FTC does not have general authority to regulate common carriers.[16] (However, the FTC and FCC's Enforcement Bureaus have indicated that the FTC may address non-common carrier activities engaged in by common carriers.[17] This is being contested in court.[18]) Moreover, regardless of common carrier jurisdiction, COPPA applies to a further limited subset of entities: commercial websites and online services, including mobile apps, that: (1) are directed to children under 13 and collect, use, or disclose personal information, or (2) are for general audiences but have actual knowledge that they collect, use, or disclose personal information from children under 13.[19]

Internet providers may not fall into either category, by function or by design. In the past, ISPs have argued that they should not be subject to COPPA's rules, drawing distinctions between themselves and edge providers who provide content and online services.[20] Though ISPs have now reversed themselves in terms of wanting to be treated differently from edge providers,[21] this does demonstrate a historical understanding and acceptance of the need for different regulations for different types of entities. And COPPA, as noted, has traditionally been focused on online sites and services. Moreover, COPPA is focused on child-directed sites and services—which ISPs would almost certainly not be considered—or general audience sites and services that have actual knowledge they are collecting information from children under 13. This actual knowledge standard is one the ISPs have fought to maintain under FTC jurisdiction, opposing efforts to make the standard one that would include situations in which ISPs know or have reason to know they are collecting information from children under 13.[22] The FTC, despite considering a situation where operators would be liable if they had "reason to know" they were collecting information from a child, maintained an actual knowledge requirement.[23]

With an actual knowledge standard, the ISPs can maintain that they don't know when they are dealing with children's information, and can't know this unless they collect

---

[16] 15 U.S.C. § 45(a)(2). The proposed Do Not Track Kids Act of 2015 would make clear that the FTC can enforce COPPA against telecommunications providers also subject to FCC jurisdiction. H.R. 2734, 114th Cong. § 7(d)(1) (2015).
[17] Federal Communications Commission and Federal Trade Commission, Consumer Protection Memorandum of Understanding (Nov. 16, 2015).
[18] *AT&T Mobility, LLC v. Federal Trade Commission*, No. 15-16585 (9th Cir).
[19] 16 C.F.R. § 312.3. In its initial implementing regulations, the FTC clarified that it had not intended to cover ISPs and other mere conduits that did not actively collect information from children. 64 Fed. Reg. 59891 (Nov. 3, 1999).
[20] "COPPA's obligation falls (and should remain) on the function of providing of Internet content and online services… and not on the function of providing the platforms used to access the Internet. COPPA should not be expanded to cover the provision of Internet access functions because it is the provision of websites and online content that Congress intended the rules to address." Comments of CTIA-The Wireless Association to Federal Trade Commission in COPPA Rule Review P104503, 2 (June 30, 2010).
[21] *See, e.g.,* American Cable Association et al., Letter to Chairman Wheeler (Feb. 11, 2016), https://www.ncta.com/sites/prod/files/Privacy_Letter_021116.pdf/ (letter from internet provider associations to FCC asking for same rules for providers as in FTC space).
[22] Comments of Comments of CTIA-The Wireless Association to Federal Trade Commission in COPPA Rule Review P104503, 10-12 (June 30, 2010); Supplemental Comments of the National Cable & Telecommunications Association and the Motion Picture Association of America, Inc. in COPPA Rule Review P104503, 8-11 (Sep. 24, 2012).
[23] 78 Fed. Reg. 3978 (2013).

further information. While these proclamations are at odds with their advertising materials, which indicate they can and do detect the presence of children in households, it is true that without inquiry and analysis of data collected ISPs generally do not know they are dealing with children. This provides support for a robust rule overall, versus a separate rule for young people, in the network context.

All in all, the protections COPPA offers here are limited. Strong protections from the Commission are needed to protect children and teens on broadband networks.

III. Children And Teens Are Different Than Adult Users, Uniquely Apt To Share Information And Uniquely Vulnerable To Marketing

Children and teens are different actors than adults. This is true both in terms of their online activities and their ability to make informed choices and understand content and messages online. These differences provide further rationale for treating their information with greater care.

Young people are inclined to share more information. Children may not appreciate the sensitivity of what they are sharing. And teens live in a culture that promotes sharing,[24] with no signs of abatement.[25] Teens also tend to act impulsively without fully thinking through the consequences.[26] Furthermore, young people often do not understand what data they are sharing and with whom it will be shared afterwards.[27] Additionally, they are unlikely to adopt complex security procedures to protect themselves, like private encryption. ISPs are poised to collect much of the information shared. As the FCC notes, "ISPs are the most important and extensive conduits of consumer information and thus have access to very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears."[28]

Children and teens are also more susceptible to ads. They are less likely to understand an advertisement for what it is—an offer of sale from the point of view of a

---

[24] 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/socialmediasociallife-final-061812pdf-0/download.

[25] 15% of teens spend more than three hours a day on social networks. Common Sense Media, Common Sense Census: Media Use by Tweens and Teens, Executive Summary, 17 (Nov. 3, 2015), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens. 71% of teens use more than one social media site as of 2015. Amanda Lenhart, Pew Research Center, Teens, Social Media & Technology Overview 2015 (Apr. 9, 2015), http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/prev.

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

[27] Pew Research Center & Berkman Center for Internet & Society, Teens, Social Media, and Privacy, 2 (May 21, 2013), http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

[28] Notice of Proposed Rulemaking In the Matter of Protecting the Privacy of Customers of Broadband and Telecommunications Services, 2016 WL 1312850 at 2 (Apr. 1, 2016) (*2016 Broadband Privacy NPRM*).

marketer. This confusion is exacerbated by native advertising—quite prevalent on social media—where ads look like the rest of the content on a website, and advergames, where ads are woven into games. Young children in particular have trouble understanding the persuasive intent of ads. Children under eight, for example, do not understand the intent is to sell them something.[29] Older children very often confuse Google search ads with organic search results.[30] Teens may be unknowingly conscripted into being product ambassadors, encouraged to submit their own photos and share products and content with friends, all monitored and monetized.[31] All of this sharing takes place across the network, with broadband providers in a position to amass information from multiple devices, sites, and services.

Further, the onslaught of online ads can have serious consequences for a child's well-being. When advertisements for specific products are regularly viewed by a child online, their decisions and actions are heavily influenced. For example, sales in e-cigarettes amongst middle school and high school students increased drastically when U.S. tobacco companies began exploiting their online ads to children. Children who saw the online ads were significantly more likely to use the products.[32] Young adults, especially young women, are also incredibly susceptible to advertisements related to body image. By viewing these ads, women are more likely to objectify themselves.[33]

Given these vulnerabilities, ISPs must approach data collection—what type of notice is given and consent received—and data practices—such as use of personal information for advertising—with respect to children and teens cautiously and carefully. As noted, young people, who are wired to share more, understand the commercial nature of an ad less, and respond particularly strongly to targeted ads, deserve strong protections. This is of increasing importance as ISPs, who control the networks, expand into the advertising

---

[29] Workgroup on Children's Online Privacy Protection, Report to the Maryland General Assembly on Children's Online Privacy, 16 (Dec. 30, 2013) (stating in footnotes that "the FTC has noted that advergames are often marketed to children, for example describing one case where 'children were directed to hold a cereal box up to a webcam in order to interact with an advergame'" and that an investigation by the U.K. Office of Fair Trading that found that some online games included "potentially unfair and aggressive commercial practices" and that "children' s inexperience, vulnerability and credulity" were being exploited).

[30] 16% of children ages 8-11 could distinguish between a sponsored ad and an organic search result on Google. 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-parents-nov-15/.

[31] PBS Frontline, Generation Like (Feb. 18, 2014), http://www.pbs.org/wgbh/frontline/film/generation-like/; workgroup on Children's Online Privacy Protection, Report to the Maryland General Assembly on Children's Online Privacy, 17 (Dec. 30, 2013).

[32] Middle school students were three times more likely and high schoolers two times more likely to use e-cigarettes than their peers when they routinely saw the advertisements for the product online. Three million middle and high school students were current users of e-cigarettes, up from about 2.5 million in 2014. Lisa Rapaport, Reuters Health Report, Teens Most Drawn to E Cigarettes by Online Ads (Apr. 2016), http://www.reuters.com/article/us-health-ecigarettes-internet-advertisi-idUSKCN0XM08T.

[33]Idealizations of the female body are very prevalent in advertisements. In a content review of women's fashion magazines, 95% of models were characterized as lean. Furthermore, research has found that young women are more likely to objectify themselves in a public profile after being exposed to an objectifying perfume advertisement. *See* Common Sense Media, Children, Teens, Media, and Body Image (January 21, 2015), https://www.commonsensemedia.org/research/children-teens-media-and-body-image.

space, "partner[ing] with powerful data brokers" and forming "'digital dossiers' on millions of Americans."[34] Unfortunately, according to ISP marketing materials, such dossiers include information on children and teens.[35] Strong broadband privacy rules are needed.

IV. Broadband Providers Should Be Cautious And Transparent In Any Collection And Use Of Children And Teens' Personal Information

Given the sensitivity of children and teens' information, and given the prevalent use of the internet by young people and the fact that this information is in general mixed in with all the other personal information being communicated over the networks, we support strong broadband privacy rules for everyone. We believe there should be one unified policy for the vast majority of users. If, however, the FCC determines that certain classes of information or subscribers merit special consideration or special protections, young people deserve the utmost privacy protections, as their information is sensitive.

a. Because Children And Teens Are Heavy Internet Users Whose Information Is Present Throughout the Network, Strong Rules Should Apply Across The Board

We support the robust definitions of CPNI and PI offered by the FCC. It is particularly important to protect information that broadband providers acquire, simply by virtue of providing service, that is "linked or linkable to an individual"—in this case a child or teen. Education information is important to include in this definition, as has been recognized recently in numerous enacted state laws and proposed federal laws.[36] Some laws, like COPPA,[37] and the FCC's proposal, also appropriately protect persistent identifiers as personal information. This is significant. And racial and ethnic data, which have been used in marketing campaigns to young people and which can be used for far more nefarious purposes, should also be considered PI. Furthermore, because this information is rightly considered personal, breaches involving it should be regulated, as the FCC has proposed.

For all subscribers, it is important that broadband providers follow a general standard of only using personal information to provide necessary services, unless there is additional consent. We support the FCC's proposed framework, which requires opt-in consent for the vast majority of non-service-related uses of personal information.

---

[34] *See* Center for Digital Democracy, Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers, Executive Summary, 1 (Mar. 2016), https://www.democraticmedia.org/sites/default/files/field/public-files/2016/bigdataispexecsum032316final.pdf.

[35] *See, e.g.*, Center for Digital Democracy, Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers, 42,52, fn. 94 (Mar. 2016), https://www.democraticmedia.org/sites/default/files/field/public-files/2016/ispbigdatamarch2016.pdf.

[36] *See, e.g.*, Student Online Personal Information Protection Act (SOPIPA), Cal. Bus. & Prof. Code § 22584; Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015); SAFE Kids Act, S. 1788, 114th Cong. (2015).

[37] 16 C.F.R. § 312.2.

For young people, making the baseline opt-in is even more important, given the sensitivity of their information and unique nature of their online experience. Moreover, making the baseline opt-in is consistent with current regulations of other actors in this space, including everyone subject to COPPA. COPPA requires verifiable parental consent before the collection or disclosure of children's personal information. Indeed, even those who may oppose the FCC's proposed framework in general have acknowledged that for sensitive information—like children's—an opt-in standard is appropriate and desirable. Consumer preferences are generally considered uniform on this point, that the collection and use of children's information without consent creates risks of harm that outweigh any benefits.[38] Even ISPs agree that sensitive information may merit opt-in protection.[39]

Opt-in requires meaningful notice and consent. Given the reality that multiple users may use a single broadband service, and that many of those users may be children who are unable to understand notice and consent, we would support a "parent" or "customer dashboard" in which a main subscriber can set different privacy preferences for different devices or log-ins.[40] Parents should be the ones providing consent for their children under 13. This, again, is consistent with COPPA. It is conceivable that an adult has no problem with opting in for their own smartphone traffic to be used for targeted advertising, but has no interest in their 10 year old's phone, or the family's smart TV, being treated similarly.

For teenagers, to the extent they are in a position to provide consent, any notice must be appropriate to the teen's age and level of understanding.[41] Since a provider may

---

[38] *See, e.g.*, *Examining the Proposed FCC Privacy Rules Before the Subcomm. On Privacy, Tech., and the Law of the S. Comm. on the Judiciary,* 114th Cong. (2016) (statement of Maureen Ohlhausen, Comm'r, Fed. Trade Comm'n) ("In some areas, consumer preferences are nearly uniform. For example, consumers generally want to be asked for permission to use their sensitive, personally identifiable information, such as medical information, real time location data, and information about children. Without consent, uses of such personal information are likely to cause a substantial, unavoidable consumer harm that isn't outweighed by benefits to competition or consumers."); Jon Leibowitz, Notice of Ex Parte Letter to Federal Communications Commission On Proposed Rules to Protect Broadband Consumer Privacy (May 10, 2016) (discussing whether "opt-in requirement should apply only to sensitive customer").

[39] *See, e.g.*, Verizon, Notice of Ex Parte Letter to Federal Communications Commission on Proposed Rules to Protect Broadband Consumer Privacy (Apr. 18, 2016) (suggesting opt-in could occur in most sensitive use cases); Verizon, Notice of Ex Parte Letter on Proposed Rules to Protect Broadband Consumer Privacy (May 9, 2016) (noting current options allow for opt-in based on sensitivity of data).

[40] Schools, libraries, and other institutions that fall within the ambit of the 2015 Open Internet Order and therefore this rulemaking merit special consideration, and we do not propose a dashboard with individual settings for every single student, for example. Please see our comments in Section V.

[41] This framework is consistent with what Common Sense proposed for data brokers in the FTC's Big Data inquiry. We proposed there and elsewhere that consumer-facing companies, whether online or off, should provide special protections for children and teens: (1) Companies should obtain affirmative express consent from parents (for children under 13) or teens before collecting minors' personal information or geolocation; (2) companies should obtain affirmative express consent from parents (for children under 13) or teens before targeting them with behavioral advertising; (3) consumer-facing entities that share child or teen data with third parties such as data brokers should provide notice to their customers, and should obtain affirmative, express opt-in consent from either a parent (for children under 13) or a teen before they collect or share information from or about a child or teen. Comments of Common Sense Media to Federal Trade Commission in Big Data: A Tool for Inclusion or Exclusion P145406 (Aug. 15, 2014), https://www.ftc.gov/system/files/documents/public_comments/2014/08/00016-92371.pdf.

not know when it is giving notice to and getting consent from a teen, all notices should be clear and direct and not require a college degree to decipher. Notices about what happens with personal information should be clear, so any consent can be fully informed. We support short, standardized disclosures, that make it easy for consumers to understand across different platforms and devices. Given, as the Commission notes, notice and consent of minors may be more likely to happen on mobile devices, broadband providers should be encouraged to provide especially clear, short notices that will show up on small screens. Transparency is important for the general population, and is of utmost importance when dealing with youth.

b. If The FCC Decides To Provide Heightened Protection For Sensitive Information, Children And Teens' Information Qualifies

To the extent the FCC determines that sensitive information should receive special protections, children and teen's information should be included in this category.

If children and teens' information is receiving special treatment, additional protections could apply: For example, broadband providers could be prohibited from all marketing, including of communications-related services, to kids. Broadband providers could limit their collection and retention of young people's information, collecting only what is necessary to provide connectivity services and retaining it only as long as it needed for such services. Days or months of retention, rather than years, could be the norm.

As noted above, transparency on the part of broadband providers is also particularly important when considering young people. Heightened notice obligations are appropriate when dealing with sensitive information like that of kids. In addition, companies could provide additional clarity about any of their efforts to target ads or other marketing to minors, and any data analysis they perform with young people's information.

V. School And Library Users Of Broadband Deserve Network Privacy Protections

Children—and many adults, including those of lower incomes—spend significant portions of their time online at schools and libraries.[42] Millions of students, teachers, families, and community residents of all ages and backgrounds utilize commercial broadband networks from schools and libraries every day. Libraries and schools also supplement home broadband access in an increasingly mobile and technology-enriched digital age.

[42] More than a third of parents living below poverty, and almost half of their children, access the internet at a library. Victoria Rideout & Vikki S. Katz, Opportunity for all? Technology and learning in lower-income families, 15 (Winter 2016). Among students in grades 3-5, 31% report using the internet in school to access class information through online portals. By the time students reach high school, 75% report using the Internet at school in this manner. Project Tomorrow, SpeakUp Digital Learning 24/7: Understanding Technology –Enhanced Learning in the Lives of Today's Students, 3 (Apr. 2015).

These users deserve to have access that will not put their personal information at risk—just like those in residential settings. Moreover, these users are in some ways even more vulnerable than others, and not just because many of them are children. Two aspects of the school and library user broadband experience make strong privacy rules particularly important. First, those who use broadband at schools or libraries have no choice in the selection of the ISP. Second, school and public library broadband users are unable to adopt additional personal security procedures within a complex public access environment.

And, particularly in schools, the information these users expose is their educational data. Educational data is another category of data that has been recognized as sensitive.[43] Educational records can lead to inferences—algorithmic or human—about abilities and intelligence, and channel individuals' futures for better or for worse, far more directly than, say, TV viewing habits. Inaccurate records could cause significant problems for individuals later in life.[44] Children's educational data, then, merits protection on a number of metrics.

The FCC's current proposal leaves school and library broadband users and their information open to privacy abuses. First, it does not explicitly extend protections to school and library customers, though they have been mentioned explicitly in the past, leaving their status open to interpretation. Second, by defining "customer" as a paying or nonpaying "subscriber" or "applicant",[45] the proposed rule appears to limit privacy protections to only subscribers (past, present, and future), as well as other individuals on a group or family plan. This definition of customer is a more narrow definition than that of "end user" adopted in the 2015 Open Internet Order, which is "[a]ny individual or entity that uses a broadband Internet access service."[46] So, while the proposal appears—albeit implicitly—to apply to schools and libraries as "customers," it is far less clear what protections apply to users. The FCC should follow through on its recognition that broadband is a Title II common carrier service and make it clear that it is protecting school and library broadband customers and their users in this rulemaking.

a. The FCC Explicitly Included School And Library Users In Its Open Internet Order, And There Is No Reason To Deny Them A Key Protection Flowing From Title II

There is clear authority for explicitly including schools and libraries in this rulemaking. In the Open Internet Order, schools and libraries are specifically mentioned as broadband recipients covered. In the 2015 Open Internet Order, the FCC drew from its 2010 Order and defined broadband internet access services (BIAS) as, "A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are

[43] *See, e.g.*, Ohm, *Sensitive Information*, *supra* n.10, at 1157-58 (noting that children's information has traditionally been regarded as sensitive); Family Educational and Privacy Rights Act, 20 U.S.C. § 1232(g); Student Online Personal Information Protection Act (SOPIPA), Cal. Bus. & Prof. Code § 22584.
[44] *See* Ohm, *supra* n.10, at 1157, 1164, 1170.
[45] *2016 Broadband Privacy NPRM*, 2016 WL 1312850 at 31.
[46] *See, e.g.*, 47 C.F.R. 8.2(c); *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5884 (2015) (*2015 Open Internet Order*).

incidental to and enable the operation of the communications service, but excluding dial-up Internet access service." The 2015 Order notes that, "We continue to define 'mass market' as 'a service marketed and sold on a standardized basis to residential customers, small businesses, and other end-user customers such as schools and libraries.' To be clear, 'mass market' includes broadband Internet access services purchased with support of the E-rate."[47] And, the 2010 Order had already made clear that E-rate can be individually negotiated and still constitute a mass-market service. [48] Thus, schools and libraries are recipients of BIAS.

The FCC had good reason for covering schools and libraries in the Open Internet Order, and similarly has good reason for including them in the protections here. One purpose of the Open Internet Order, and subsequent guidelines like this rulemaking, is to encourage broadband use and deployment. Boosting confidence and trust regarding the security of sensitive personal information among broadband users will encourage the deployment of broadband nationwide. As noted, children and teens are heavy tech users who are particularly vulnerable online. The increased use of technology in schools is leading to greater proliferation of traceable student data used for purposes other than education. While bolstering transparency, choice, and security for all broadband users should remain a high priority, the unique attributes of kids, students, and library users demonstrate the particular importance of creating clear, bright-line rules governing the privacy and security practices of ISPs in schools and libraries.

Section 706 of the Telecommunications Act of 1996 authorizes the Commission to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular elementary and secondary schools and classrooms)." [49] To achieve this goal, the Commission may implement, "in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment."[50] The Commission also initiates "a notice of inquiry concerning the availability of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms)."[51] Upon inquiry, if the Commission determines that advanced telecommunications capability is not being deployed to all Americans in a reasonable and timely manner, the Commission shall "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market."[52] In *Verizon v. FCC*, the D.C. Circuit upheld the Commission's analysis that

[47] *See 2015 Open Internet* Order, 30 FCC Rcd at 5682-85, para. 187, 189. *See also id.* at 5745-46, para. 336.
[48] *See Preserving the Open Internet Broadband Industry Practices*, 25 FCC Rcd 17905, 17932, para. 45 (*2010 Open Internet Order*).
[49] 47 U.S.C. § 1302(a).
[50] *Id.*
[51] 47 U.S.C. § 1302(b).
[52] *Id.*

Section 706 provides an independent source of affirmative statutory authority to regulate BIAS providers.[53]

Section 706 of the Telecommunications Act specifically and uniquely calls attention to schools and libraries, indicating the particular need for the Commission to concern itself with the advancement and regulation of broadband in schools and libraries. Section 706 and the D.C. Circuit's ruling in *Verizon v. FCC* provide the Commission with the authority to remove barriers to infrastructure investment and promote competition by regulating BIAS providers in order to achieve the Commission's goals of promoting transparency and security for customers, including schools and libraries, in order to ensure that broadband deployment to schools and libraries throughout the nation continues to progress.[54] Because the Commission has specific statutory authority to incorporate schools and libraries into its considerations regarding whether or not telecommunications, specifically broadband, is being deployed in a reasonable and timely fashion and because the Commission as well as Congress have demonstrated intent to include schools and libraries in this consideration, schools and libraries should not be left out of the Commission's broadband privacy regulations. The Commission should explicitly acknowledge that they are covered.

b. The Realities Of School And Library Users' Broadband Access Demonstrate The Need For Privacy Rules

In addition, there are important factual reasons to cover schools and libraries in this rulemaking. First, while purchasers of home broadband have limited choices in selecting a provider, the children and adults relying on school and library access have no choice whatsoever. (Indeed, nearly all children cannot even decide whether they want to go online at school at all—it is required as part of their education.[55])

Furthermore, school and library patrons are limited in their technical options. Even if young children were to understand the need for or nature of a VPN—a highly unlikely proposition—the actual mechanics of their access would largely prevent them from making use of such technology at school. Unlike home broadband consumers, the most technically-savvy of whom may be able to take privacy-protective steps and shield their activities, school and library patrons have little control over how their personal information is collected, stored, and shared as they access broadband services.

Also, given the nature of public broadband access, schools and libraries are not in a position to independently comprehensively protect these children and adults from data

---

[53] *Verizon v. FCC*, 740 F.3d 623, 635-42 (2014).

[54] *See, e.g.,* Annual Performance Report, 2015 WL 10059227 (Jan. 1 2015) (stating that FCC goal is to maximize availability of broadband to community anchor institutions); Broadband Progress Report, 2015 WL 9942032 (Jan. 28 2015) (stating that 41 percent of schools have not yet met the FCC's goals for broadband, showing that broadband is not being deployed to all Americans in a reasonable and timely fashion).

[55] There is a groundswell of national support to better protect students' privacy. However, recently enacted and proposed laws focus on educational technology providers and educational institutions. Whether a broadband provider is adequately protecting schoolchildren's privacy is largely dependent on the vagaries of pre-existing procurement laws.

collection by commercial broadband providers (not to mention any subsequent data use or sharing). Schools and libraries are limited in what additional technical measures they can take to protect individuals' privacy. These institutions, while certainly knowledgeable about the risks, face mechanical and practical limitations in a complex public access environment. It is often infeasible, if not impossible, to install useful and easy to use encryption on all equipment. This is particularly true for E-Rate recipients who may be subject to filtering requirements to comply with the Children's Internet Protection Act.[56]

c. Indeed, These Users May Be More Vulnerable And Deserve Specific Protections

Privacy should not be a privilege reserved for those with time, money, and technical expertise. School children and library patrons are equally deserving of protection. Further, in many ways, these individuals are more vulnerable to privacy harms. As detailed above, children are developing a footprint that will last their lifetimes. The educational information they expose in schools is sensitive in its own right. And adult library populations are often those who may be more likely to suffer harms related to digital redlining and algorithmic discrimination.

Given the unique harms these users may face, and given the realities and configuration of their access, the rules should very clearly apply to them. Moreover, certain specific rules can and should apply in the school and library context.

Consistent with the FCC's apparent proposal, that schools and libraries are the customers, and to make things easier from a technical perspective, we would propose that each school or library customer have one set of universal rules for all users, as we understand it may be difficult for providers to adopt different rules for each user or device and as the vast majority of school users—i.e., children—should not be selecting privacy options on their own.

Moreover, schools and libraries will benefit from additional privacy protections for their users, and, given the access set up, can have specific rules. Broadband providers, knowing they are overwhelmingly dealing with children in these contexts, should only use the information they receive to provide the necessary services. They should not use personal information collected from school and library networks to provide targeted advertisements about anything, including communications-related services. And schools and libraries should not have the option to "opt in" on behalf of their users. There should be no sharing or non-service related use of information collected from school and library users. Such a rule is feasible to impose in this context because broadband providers offer specific service to schools and libraries. This information can be separated from the other information on the network and treated with the care it deserves.

Relatedly, to the extent the FCC approves pay for privacy options or similar schemes, such options should not be allowed in the school and library context. The FCC has previously recognized the unique situation of schools and libraries in its 2015 Open

[56] Children's Internet Protection Act, Pub. L. No. 106-554, 114 Stat. 2764 (codified in 47 U.S.C. 254).

Internet Order, noting that paid priority agreements can be a particular threat to non-commercial end users, including schools and libraries, "who would be less able to pay for priority service."[57] The same is true with pay for privacy protections. These institutions are often cash-strapped, and it would be inappropriate for them to be put in a situation where they feel they must bargain away students' privacy in exchange for cheaper service.[58] Given that E-Rate recipients must use price as the primary factor when considering bids, weighted more heavily than any other factor,[59] a cheap price in exchange for giving up privacy protections is an unfair inducement.

Rather, schools and libraries should be trusted educational zones where children can engage online without fear that broadband providers are tracking their every move and monetizing it. This is in line with Common Sense's School Privacy Zone principles and its student privacy work in the educational technology and app space.[60]

VI. Conclusion

The Commission has proposed strong privacy rules consistent with its statutory obligations to protect communications privacy. We support those rules on behalf of children, teens, families, and school and library users. Because children and teens share a lot of information online, which is sensitive, and because children and teens are less aware of their sharing and more susceptible to privacy and marketing abuses, and their information is inherently intermingled with other information on the network, it is necessary to have strong overall rules. This will protect vulnerable young users. Moreover, because schools and libraries are unique places where children and other users are particularly susceptible to harms, they too deserve strong rules that explicitly address their privacy. As separate rules are possible in the school and library context, broadband providers should only be allowed to use personal information collected from schools and libraries to provide broadband services.

We look forward to working with the FCC and other stakeholders on these issues.

Respectfully submitted,

/s/ James P. Steyer
James P. Steyer
Founder and CEO
Common Sense Media
650 Townsend St.
San Francisco, CA 94103

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

[57] *See 2015 Open Internet Order*, 30 FCC Rcd at 5621, para. 68.
[58] Common Sense has raised similar concerns in the educational technology space, not wanting schools to feel forced to "consent" to getting free or freemium products in exchange for their student's privacy. *See School Privacy Zone,* Common Sense Kids Action, https://www.commonsensemedia.org/kids-action/our-issues/a-positive-media-and-technology-world/school-privacy-zone.
[59] *Schools and Libraries (E-Rate): Selecting Service Provider,* Universal Service Administrative Company, http://www.usac.org/sl/applicants/step02/.
[60] *See School Privacy Zone, supra* n.58.