Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20554

In the Matter of	)	**Docket No. 180821780-8780-01**
	)	
Developing the Administration's Approach	)	
To Consumer Privacy	)	
	)	

COMMENTS OF COMMON SENSE

Common Sense Media
650 Townsend Street, Suite 435
San Francisco, CA 94103

2200 Pennsylvania Ave. NW, 4E
Washington, DC 20037

November 9, 2018

TABLE OF CONTENTS

I. Introduction

Common Sense Kids Action, the policy arm of Common Sense Media (collectively, "Common Sense"),[1] is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for public comment on proposed approaches that seek to advance consumer privacy while also protecting American prosperity and innovation.[2] Common Sense is a national, independent, non-partisan voice for America's children, teens, and families. For more than 15 years, Common Sense has empowered parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all children and teens' lives.

Common Sense appreciates that the NTIA is seeking comments from various stakeholders on how to better protect personal data. 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 particularly vulnerable. Most young people socialize and engage online by sharing personal information about themselves through social media applications such as Snapchat and Instagram, through entertainment platforms such as YouTube or Twitch, or through using technology for educational purposes at school. They frequently use mobile devices. They are more susceptible to advertisements. And they are unaware of how their online behavior and personal information can be monitored, stored, and used by companies.

Common Sense supports the NTIA developing principles to protect privacy and control data collection and use. However, any future privacy laws, regulations, or principles that fail to account for children and teens will leave our most vulnerable population with inadequate protections. Common Sense respectfully requests that the NTIA account for the specific needs of children and teens in the development of any privacy policies.

Any comprehensive privacy protections should take into account the needs of everyone, including children and teens. The NTIA needs to consider the vulnerabilities of young people in its proposed principles, especially the transparency, control, minimization, security, and accountability principles. The NTIA should ask that companies clearly describe their privacy practices, such as how they collect, use, disclose, and maintain information, in a manner that is accessible and understandable for children, teens, and their parents. Additionally, the NTIA

---

[1] Common Sense thanks American University Washington College of Law's Glushko Samuelson Intellectual Property Clinic's student attorneys, Zach Engleman, Hailie Ingman, Marielena Reyes, and Spencer Sanders for their work on these comments.

[2] *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sep. 26, 2018).

should encourage companies to enable young people to exercise control over what information that company can collect or disclose, given how sensitive children and teens' information can be. The NTIA can help properly safeguard this sensitive information by requiring that companies minimize the collection and use of children and teens' information, taking and using only what is necessary, and implement strict security measures. The NTIA should also promote accountability among companies. Finally, while Common Sense supports the FTC as a key enforcer of data security and collection concerns, Commons Sense believes that other federal and state authorities with expertise should also be empowered to investigate and enforce violations; and additionally, there should be a private right of action for individuals when companies mishandle their data in order to ensure appropriate redress.

II. The Federal Government, States, and Other Countries are Pushing for More Laws and Regulations to Protect Children and Teens' Privacy Because of their Vulnerabilities Online.

The current privacy regime in place to protect children includes the Children's Online Privacy Protection Act of 1998 (COPPA) and various state efforts, but none cover all teens. COPPA is the primary and only federal law in place that specifically addresses children's privacy concerns.[3] However, COPPA fails to protect teens, as COPPA only applies to children under 13 and those sites and services that target children under 13 or have actual knowledge they are collecting information from children under 13.[4] Some states are working toward filling gaps in protections for children and teens. In addition to many states which have moved to protect children in the educational context, California and Delaware have enacted more restrictive privacy legislation for companies whose services affect children and teens.[5] However, gaps in protections remain across the country, especially for teenagers.

The states that have passed laws, and attempted federal efforts, are instructive. For example, California's "Eraser Button" law, which took effect January 1, 2015, enables minors to delete postings they have made, and restricts online service providers from marketing or advertising certain products or services on websites "directed to minors."[6] Similarly, Delaware enacted the Delaware Online Privacy and Protection Act (DOPPA), which prohibits certain types of marketing or advertising "directed to children" as well.[7] Another example of California's efforts to protect children and teens' privacy can be seen in California's Consumer Privacy Act

[3] Children's Online Protection Privacy Act, 15 U.S.C. § 6501-6506 (2018).
[4] *Id.* at § 6501(1).
[5] *See* California Eraser Button Law, Cal. Bus. & Prof. § 22580 (2013); California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100-198 (2018); Delaware Online Privacy and Protection Act, 80 Del. Laws, c. 148, §§ 1-3 (2015).
[6] Cal. Bus. & Prof. § 22580(a) (2013).
[7] 80 Del. Laws, c. 148, §§ 1-3 (2015).

of 2018 (CCPA), which Common Sense co-sponsored.[8] CCPA goes into effect in 2020, and in addition to allowing all Californians rights to access and delete their personal information, gives children and teens under 16 the opportunity to opt in before their data is sold (older Californians can opt-out).[9] Many consider this new data privacy bill to be the toughest in the nation.[10] The NTIA should also look to the federal Do Not Track Kids Act.[11] Among other things, the law would extend COPPA's protections to teenagers, and require any sites and apps that direct their services to children and teens, or have actual knowledge of personal information being collected from children or teens, "to provide clear and conspicuous notice in clear and plain language" of what personal information the operator collects, how it's used, whether it is disclosed, and what safeguards are in place to ensure that children and teens' personal information is being lawfully collected.[12]

Another place to look for guidance is Europe's General Data Protection Regulation (GDPR). The GDPR recognizes that children (under 18) "merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[13] The GDPR explicitly recognizes that young people need special treatment in terms of when it is appropriate to process their information, how they can provide informed consent, and what constitutes appropriate transparency.[14]

These laws and bills demonstrate a recognition that children and teens are especially vulnerable online as compared to adults. Studies show that children (ages 6-10) demonstrate a significant lack of understanding of nontraditional advertising forms, such as movie and in-game ad placement.[15] This lack of understanding creates a child's inability to critically evaluate advertisements, which makes children especially susceptible to them.[16]

---

[8] Cal. Civ. Code §§ 1798.100-198 (2018).
[9] *Id.* at 1798.120(d).
[10] Laura Hautala, *California's New Data Privacy Law the Toughest in the U.S.*, **CNET** (June 29, 2018, 1:57PM), https://www.cnet.com/news/californias-new-data-privacy-law-the-toughest-in-the-us/.
[11] Do Not Track Kids Act of 2018, S. 2932, 115th Cong. §2 (2018).
[12] *Id.* § 5(a).
[13] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Council Directive 95/46/EC, 2016 O.J. (L 119) 1, Rec. 38.
[14] *Id.* at Art. 6, 8, 12.
[15] Laura Owen, Charlie Lewis, Susan Auty, & Moniek Buijzen, *Is Children's Understanding of Nontraditional Advertising Comparable to Their Understanding of Television Advertising?*, 32 **J. of Pub. Pol'y & Marketing** 195 (2013).
[16] *Id*.

In a similar vein, many children lack the ability to understand the implications of the personal information they share online. Most children are unable to protect their information and understand how data is collected, sold, and used because they are not as sophisticated as adult users.[17] Typically, children and teens do not understand what data they are sharing and with whom it will be shared with afterwards.[18] Both children and teens may not appreciate the sensitivity of what they are sharing online. Further, they are unlikely to adopt more complex security measures, like encryption.[19]

Additionally, children and teens are online a lot, especially on mobile and social media. There is no question that the use of the internet is a popular activity among children and teens in this country. Studies show that almost all children have used a mobile device before the age of one, and those between one to two are avid consumers of Youtube.[20] Additionally, in a 2018 study focused on teens' use of social media, 44 percent of teens reported using social media on a daily basis and 45 percent stated they used social media "almost constantly."[21] Teens surveyed reported were using a variety of social media platforms including: 72 percent using Instagram, 69 percent using Snapchat, 51 percent using Facebook, and 32 percent using Twitter.[22] Moreover, the average teen is spending over two hours and 40 minutes per day on a smartphone.[23] Therefore, the need for the protection of children and teens' privacy is one of great importance because of their continuous consumption of online content like social media through

---

[17] Common Sense Media, *Common Sense Census: Media Use by Tweens and Teens*, 17 (Nov. 3, 2015), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens.

[18] Mary Madden, et. al, *Teens, Social Media, and Privacy*, Pew Research Center & Berkman Center for Internet & Society (May 21, 2013), http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

[19] Comments of Common Sense Kids Action, Comment Letter on Developing the Administration's Approach to Consumer Privacy (May 27, 2016), https://www.commonsensemedia.org/sites/default/files/uploads/kids_action/cskabroadbandprivacycomments.pdf.

[20] Hilda Kabali et. al., *Exposure and Use of Mobile Media Devices by Young Children*, 136 **Pediatrics** 1046 (Dec. 2015), http://pediatrics.aappublications.org/content/pediatrics/136/6/1044.full.pdf (showing that 96.6% of children have used a mobile device).

[21] Monica Anderson & Jingjing Jiang, Pew Research Center, *Teens, Social Media, and Technology 2018* (May 31, 2018), http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/ (finding that 95% of teens have access to a smartphone).

[22] *Id.*

[23] Common Sense Media, *Fact Sheet: Teens and Smartphones* (2015), https://www.commonsensemedia.org/sites/default/files/uploads/pdfs/census_factsheet_teensandsmartphones.pdf (finding that among teens that use a smartphone they spend more than four hours a day using it).

devices, like their smartphones, that can collect, analyze, use, and share their personal and sensitive information.

III. NTIA's Privacy Principles Should Specifically Account For All Children and Teens

Common Sense applauds the NTIA for pursuing proactive principles that recognize the importance of privacy protections and the need for responsible data collection but believes the NTIA can go further by specifically accounting for all children and teens in the development of any federal privacy principles. Any future principles, framework, or legislation should acknowledge and protect children under 18. The NTIA can do so by looking to state and draft federal laws and regulations, like those discussed above, for guidance, both in terms of protecting children and teens and in their overall protections. For example, the NTIA should draw inspiration from CCPA not just because it protects teens, but because it comprehensively and broadly identifies what "personal information" is, which ultimately provides further protection for children and teens (and adults).[24] The ideal principles would provide across the board protection that especially account for all children and teens.

A. Transparency

Common Sense agrees with the NTIA's transparency principle that states users should easily understand how an organization collects, stores, uses, and shares everyone's personal information, but Common Sense specifically wants to ensure that children and teens' personal information is protected. The need for kids and parents to understand how organizations are collecting, using, and sharing their personal information is fundamental to safeguarding their privacy. Organizations often communicate this information through lengthy privacy policies or terms of service. As the NTIA properly notes, these notices often leave consumers with an inadequate understanding of how organizations are using their personal information. This is especially true for children and teens.

Children and teens have lower media literacy levels than adults and may not understand the implications of sharing their data.[25] Recent polling conducted by Common Sense showed that, at least in regards to social media, teens are less likely than adults to read the terms of service, with more than half almost never reading them.[26] Even when they do, they reported that

[24] *See* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(o).
[25] Sonia Livingstone, et. al., *If Children Don't Know an Ad from Information, How Can They Grasp How Companies Use Their Personal Data?*, **Media Policy Project** (July 18, 2017), http://blogs.lse.ac.uk/mediapolicyproject/2017/07/18/if-children-dont-know-an-ad-from-information-how-can-they-grasp-how-companies-use-their-personal-data/.
[26] Common Sense & SurveyMonkey, *Privacy Matters: Parents and Teens Share Attitudes and Opinions* (May 5–22, 2018),

they do not understand them.[27] This makes sense -- according to another study, the average reading level of a person that can understand these documents is that of a college sophomore because of the extent of complicated legalese contained in these policies.[28] Parents, too, who are often pressed for time, may have difficulty in understanding these documents, especially low-income parents who may not have an opportunity to afford a higher educational level. Given this, children and teens may unknowingly be allowing organizations to collect and share their personal data by consenting to terms they do not understand.

Any transparency principle, therefore, should require organizations to clearly and simply communicate what data they are collecting and how it is being used, along with what rights the consumer has over their data, in a manner in which children, teens, and their parents can easily understand—written appropriate to the age and understanding of the specific audience. This may mean using videos and other forms of communication in addition to text. For direction, the NTIA could look to the notice requirement of the draft federal legislation, The Do Not Track Kids Act, which mandates "clear and conspicuous" terms so they are easily understandable to parents and teens;[29] or the CCPA, which requires organizations to provide notice on the use and collection of personal information prior to collection and grants consumers the right to request that businesses disclose additional information about the data that they have collected;[30] or the GDPR, which requires organization provide information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[31] A federal baseline requiring that notice is clear and easy to understand would help ensure that any consent be fully informed. Transparency is important for all consumers, particularly so for children and teens, in being able to exercise reasonable control over the data they share online.

B. Control

Common Sense agrees with the NTIA that users should be able to exercise control over the collection, use, storage, and disclosure of personal information that they provide to

---

https://www.commonsensemedia.org/sites/default/files/uploads/research/commonsense-surveymonkey-privacymatters-topline_release.pdf.

[27] *Id*.

[28] Casey Fiesler & Amy Bruckman, Ga. Inst. of Tech., Copyright Terms in Online Creative Communities, (April 26 - May 01, 2014), *in* CHI'14 CHI Conf. on Human Factors in Computing Sys., at 2551, https://www.cc.gatech.edu/elc/copyright/pdf/p2551-fiesler.pdf.

[29] Do Not Track Kids Act of 2018, S. 2932, 115th Cong. § 2 (2018).

[30] *See* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.110.

[31] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Council Directive 95/46/EC, 2016 O.J. (L 119) 1, Art. 12.

organizations, especially in the case of children, teens, and parents. Given the sensitivity of children and teens' personal information, establishing a strong federal baseline for control over their data is especially important. This has been highlighted in recent state, federal, and international efforts to give children, teens, and parents greater control.[32] These legislative efforts have responded to growing public concern by ensuring that consumers - especially children, teens, and their parents - have control over the collection and use of their data, especially the right to "opt in,"[33] the right to access[34] and the right to delete.[35] (The right to "opt out" is also helpful, but the right to opt in is more privacy protective as a default.) These rights empower children and teens by giving them affirmative control over what a company may or may not do with their personal information and should be embodied in any federal baseline to support consumer control.

C. Minimization

Common Sense urges the NTIA to help ensure that organizations adequately minimize collection, use, and sharing of children and teens' information to what is necessary to complete a transaction or provide a service, defined narrowly. The administration's ideal privacy outcome of reasonable minimization should be the strictest for children and teens because, as previously discussed, they possess unique vulnerabilities online, especially to advertisements.[36] Again, for guidance, the NTIA should look to the draft federal legislation, the Do Not Track Kids Act of 2018, which requires companies to follow Fair Information Practice Principles for teens and has a flat prohibition on behavioral advertising to children under 13.[37] Additionally, the CCPA, which requires that children and teens under 16 must "opt in" to consent to the sale of their data, is a huge step forward in acknowledging the importance of limiting the spread of information.[38] The CCPA provides an mechanism for a child – through a parent – or a young teen to provide informed consent, if they so choose, but offers important protections baked in by default and gives young people an awareness as to the potential dangers of sharing their personal data online.

---

[32] *See id. at* §§ 1798.100 - 1798.198; Cal. Bus. & Prof. Code §§ 22580-22582 (2013); Do Not Track Kids Act of 2018, S. 2932, 115th Cong. § 2 (2018).
[33] *See* California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.120(a)-(b) (defining the right to "opt-in" as requiring affirmative authorization from consumers under 16, or their parents if they are under 13, before organizations may sell their personal information).
[34] *See id*. § 1798.115 (granting consumers the right to request businesses to disclose what information they collect, how it is used, and who it is shared with).
[35] *See id*. § 1798.105 (defining the right of consumers to request for the deletion of personal data that companies hold on them).
[36] Laura Owen, Charlie Lewis, Susan Auty, and Moniek Buijzen, *Is Children's Understanding of Nontraditional Advertising Comparable to Their Understanding of Television Advertising?*, 32 **J. of Pub. Pol'y & Marketing** 195 (2013).
[37] Do Not Track Kids Act 2018, S. 2932, 115th Cong. § 6 (2018).
[38] *See* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.120(a)-(b).

D. Security

Common Sense agrees with the NTIA that organizations should employ security safeguards to protect the data they collect, store, use, or share, especially in regard to children and teens. In addition to not understanding the ramifications of what they are sharing, children and teens, even more so than most adults, do not protect themselves by utilizing complex security procedures like private encryption.[39] Most children and teens would not think to use something like a VPN. And in many instances, children or teens access the internet at a place like a school where a VPN is technically impossible. Further, most teens are impulsive due to their age and tend to over share their lives online without thinking about the consequences of their actions. Additionally, children cannot comprehend the sensitivity of the information they do share.[40] Both age groups are constantly consuming technology from various internet of things devices, like mobile phones, tablets, computers, Alexa, and smart toys, all of which have the capability of collecting, sharing, and storing sensitive personal information like voice, photos, and geolocation.[41] Due to the failure of companies to adequately secure data, there have been numerous data breaches that have resulted in the leak of children and teens' intimate information such as their VTech account information (including personal messages).[42] This compounds risks

---

[39] *See also* Mary Madden & Lee Rainie, Pew Research Center, *Americans' Attitudes About Privacy, Security & Surveillance* (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ ("10% of adults say they have encrypted their phone calls, text messages or email and 9% say they have used a service that allows them to browse the Web anonymously, such as a proxy server, Tor software, or a virtual personal network.").

[40] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Bus. & Pol'y. Makers, 59 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[41] Common Sense Media, *Zero to Eight: Children's Media Use in America*, 11 (Oct. 28, 2013), https://www.commonsensemedia.org/file/zerotoeightfinal2011pdf 0/download (showing the vast increase in children's use of mobile devices); 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/ (finding that 92% of teenagers go online daily and 91% of them use their mobile device to do so and 24% report using the internet "almost constantly").

[42] Press Release, Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act, **FTC** (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated (stating that the VTech settled with the FTC after a computer hacker accessed personal information regarding children who used their Kid Connect app); *see also* Thuy Ong, *Teen-monitoring App TeenSafe Leaks Thousands of User IDs and Passwords*, **The Verge** (May 21, 2018),

for kids, who are already more susceptible to identity theft.[43] It has been long recognized that young people's information is sensitive as evidenced by COPPA and other recent state regulations and laws;[44] therefore, it makes sense to account for children and teens in NTIA's privacy principles by providing strict security measures that safeguard their data.

Simply put, any law or regulation of private organizations should have broadly applicable rules that also specifically address the security concerns of children and teens because of their cognitive capabilities and the constant influx of information devices receive from them. As guidance, the NTIA could look to California Senate Bill 327 (recently signed into law), which mandates that connected devices must be equipped with a security feature that is designed to protect personal information in the device, appropriate to the device and the nature of the information.[45] Additionally, there are federally mandated security measures for children in COPPA, which require an operator to create and maintain "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children,"[46] but it does not extend to teens. These laws are significant because they recognize the need for data security measures and require operators to establish mechanisms that protect children and teens. However, they are not strong enough as evidenced by the wide gap in the protection of teens and information that may be collected about children but not from them. Therefore, a federal privacy baseline should ensure that all age groups are accounted for and legislation be equally applied to all companies to ensure *every* individual's personal information is adequately secured, including all children and teens.

---

https://www.theverge.com/2018/5/21/17375428/teensafe-app-breach-security-data-apple-id (exposing 10,200 teens accounts linked to TeenSafe, an app that helps parents monitor their child's internet use).

[43] Kelly B. Grant, *Identity Theft isn't Just an Adult Problem. Kids are Victims, Too*, **CNBC** (Apr. 24, 2018) https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html
(explaining how over 1 million children's identities were stolen in 2017 and among those parents that received a data breach notice, 39% reported their child was the victim versus only 19% of adult victims); *see also* Mary Madden & Lee Rainie, Pew Research Center, *Americans' Attitudes About Privacy, Security and*
Surveillance (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ ("For all of the 11 entities we asked about in the fall 2014 survey – from government agencies to credit card companies to social media sites – only small minorities say they are "very confident" the records maintained by these organizations will remain private and secure.").

[44] Cal. Bus. & Prof. § 22580 (2013); 80 Del. Laws, c. 148, §§ 1-3 (2015).

[45] S. Bill No. 327 (Cal. 2018).

[46] 16 C.F.R. § 312.8 (2018) ("The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.").

E. Accountability

To assure children and teens are protected online, organizations must be held accountable. Common Sense believes it is necessary to enable agencies with subject matter expertise to enforce future federal legislation, as they have knowledge and experience in the area. Currently the FTC is the main federal enforcer of data collection misuse or abuse, including violations for children under COPPA. The FTC should continue to lead in this area. Any future legislation should reflect, for example, the FTC's current authority as instituted in COPPA, where the FTC is equipped with civil penalty authority[47] and rule-making authority.[48] The FTC should also have the resources to be a stronger enforcer. However, the FTC should not be the lone enforcer of data security and data collection concerns. Other federal agencies, as well as state Attorney Generals, and private citizens, should have jurisdiction to enforce privacy protections. This will help to ensure proper enforcement of any law or regulation against those who violate children and teens' privacy.

IV. Conclusion

For fifteen years, Common Sense has been the voice for children and teens, helping them and their families navigate media and the online space. As such, we believe it is necessary to ensure that young people are protected, and their parents are equipped with the proper tools necessary to educate and protect their families from the misuse of data collection when participating on online activities. Although the NTIA's privacy principles demonstrate an understanding of the need to provide privacy protections for individuals sharing their data online, they do not fully account for the specific concerns of children and teens. We respectfully urge

---

[47] *See* Children's Online Protection Privacy Act, 15 U.S.C. §§ 6502(c), 6505(d) (2018); *see also* Press Release, Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act, **FTC** (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated (sanctioning VTech $650,000 for violating "U.S. children's privacy law by collecting personal information from children without providing direct notice and obtaining their parent's consent, and failing to take reasonable steps to secure the data it collected."); Press Release, Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act, **FTC** (Dec. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens (penalizing two app companies amounting to $360,000 combined for creating various apps that targeted children and gave their information to third parties without the consent of the child or parent); Press Release, FTC Receives Largest COPPA Civil Penalties to Date in Settlements with Mrs. Fields Cookies and Hershey Foods, **FTC** (Feb. 27, 2003), https://www.ftc.gov/news-events/press-releases/2003/02/ftc-receives-largest-coppa-civil-penalties-date-settlements-mrs (sanctioning Mrs. Fields $100,000 because "While Mrs. Fields did not disseminate the information it collected to third parties, the company allegedly collected personal information - including full name, home address, e-mail address and birth date - from more than 84,000 children, without first obtaining parental consent.").

[48] 5 U.S.C. § 553 (2018); Children's Online Protection Privacy Act, 15 U.S.C. § 6502(b) (2018).

the NTIA to ensure that any future discussions, principles, or legislation proposed specifically consider the needs of children and teens who are particularly vulnerable. We look forward to working with NTIA and other stakeholders on these issues. Please feel free to contact Ariel Fox Johnson or Amina Fazlullah at 202-350-9992, afoxjohnson@commonsense.org, or afazlullah@commonsense.org for any additional information.