13 GOING ON 30: AN EXPLORATION OF EXPANDING COPPA'S PRIVACY PROTECTIONS TO EVERYONE

*Ariel Fox Johnson**

I. INTRODUCTION

Babies today are born into a brave new world—one in which they will be tracked and surveilled more than any generation before them. The United States is long overdue to increase protections for children, including teenagers, who are presently ignored in the eyes of the law (but not in the eyes of big data) and treated no differently than their adult counterparts. It is also long past time to offer protections for adults, who are no strangers to surveillance either. The one broadly applicable consumer federal privacy law, the Children's Online Privacy Protection Act (COPPA),[1] was passed over twenty years ago, in an era of bulky desktop computers and CD-ROMS. Legislators enacting COPPA worried that parents were losing their traditional role as gatekeepers, exposing children more directly to both physical predators and predatory marketing. COPPA primarily addresses these concerns by creating a requirement for "verifiable parental consent" before information can be collected from children under thirteen.[2] COPPA was designed to be flexible, especially through rulemaking, and the Federal Trade Commission has made valiant efforts to keep it up to date and relevant, including through a 2013 rule that brought COPPA into the age of mobile and social media.[3]

Regardless, kids continue to face a growing array of risks and harms.[4] They live in an always-on culture where they are constantly connected—and required to be so in order to get an education—and where powerful tech interests take advantage of young people's hardwired instinct to share. They are early adopters of new and often inexpensive technology, with safety and privacy features that are often an afterthought. Kids' developing brains, which have trouble comprehending the persuasive intent of advertisements and conceptualizing long-term consequences, let alone complicated data

* Ariel Fox Johnson is Senior Counsel for Policy and Privacy at Common Sense Media, where she advocates for smart practices, policies, and rules to help all kids thrive in today's wired world. Her work focuses on enhancing family privacy rights, strengthening students' educational privacy, and promoting robust consumer protections in the online world. She has helped develop laws on student privacy, consumer privacy, and the Internet of Things and frequently advises policymakers, industry, and tech experts. Ariel obtained her A.B. from Harvard College and her J.D. from Harvard Law School. Prior to joining Common Sense, she worked on privacy, media, intellectual property, and technology matters at corporate law firms and served as a law clerk to Judge Peter J. Messitte of the United States District Court for the District of Maryland.

The author would like to extend a special thanks to Jill Bronfman, Taylor Deitrick, and Jennifer Peters for their invaluable input and assistance on this piece.[1] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2018).

[2] *See* discussion of COPPA's enactment *infra* Section II.

[3] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4009 (Jan. 17, 2013) (amending 16 C.F.R. § 312).

[4] *See* discussion of children's experiences with technology *infra* Section V.

ecosystems, are no match for advanced profiling and analytics techniques. This leaves children and teenagers vulnerable to past concerns of over-commercialism and physical safety. But there are new worries as well, as children and teenagers are also at risk for heightened emotional and behavioral harms, cyberbullying, identity theft, manipulation, labeling, and limiting that can impact their current and future opportunities. Growing awareness of privacy exposure can lead young people to self-censor or to limit their attempts to engage with or understand the world. Natasha Singer of The New York Times has written about how technology can "surveil, sort and steer people on a massive scale."[5] It can also suppress speech and behavior, especially from young people.

Young people deserve the right to grow, learn, and develop without surveillance, sorting, steering, or suppression. Yet despite these growing risks, as well as a growing global movement calling for privacy laws, Congress has thus far been unwilling or unable to act. This essay proposes a simple solution that would better protect kids' privacy: extend COPPA's protections to everyone. While this is not the ideal way to improve kids' privacy protections (that would involve substantive enhancements to COPPA as well as comprehensive baseline privacy laws), it is a fairly straightforward way, and thus may be achievable even in this political climate. Additionally, it would address a major shortcoming of COPPA—namely, that it only applies to a limited class of "operators."[6] This limited application, combined with the fact that COPPA is usually the only privacy law in town, means that an outsized amount of company energy goes into avoiding COPPA, when it could go into building privacy protections instead. If COPPA applied across the board, children would benefit from default protections everywhere, even if companies did not consider their services as directed to kids or even if kids lied about their ages. If COPPA applied across the board, there would be a larger market for COPPA-compliant vendors, products, and services, making compliance easier. This would improve children's experience online. Further, there would be additional benefits as well, including potentially more incentives to create content, as well as a move away from a system that relies upon behavioral profiling and marketing to survive. These benefits would accrue to children even though there would be no new substantive provisions specifically for them.

---

[5] Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html.

[6] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4009 (Jan. 17, 2013) (amending 16 C.F.R. § 312). The Commission defines operator as "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained."

This essay (1) lays out the legislative history of COPPA and the decision to protect children "under thirteen;" (2) examines COPPA's provisions; (3) analyzes how COPPA has evolved since enactment; (4) details kids' unique vulnerabilities online and the growing risks and harms they face; (5) considers Congress' failure to act; and (6) explores how kids would benefit from extending COPPA to everyone.

II. COPPA's HISTORY

COPPA was passed in 1998, amidst broader efforts to increase consumer protections on the Internet.[7] According to a 1998 Federal Trade Commission study, 89% of children's websites collected personal information from children, many without disclosure, and only 10% offered parental control.[8] The report noted that online data collection practices posed "unique privacy and safety concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent."[9] The two main concerns were (1) children's safety and potential communication with strangers, and (2) children's vulnerability to commercial and marketing abuse. In both arenas, parents have traditionally sought to protect children.[10]

The Commission recommended that "Congress develop legislation placing parents in control of the online collection and use of personal information from their children. Such legislation would require websites that collect personal identifying information from children to provide actual notice to parents and obtain parental consent."[11] Commission Chairman Robert Pitofsky repeated this recommendation when testifying before Congress in July 1998.[12]

---

[7] *See, e.g.*, Vice President Al Gore's efforts on an "electronic bill of rights" to protect privacy and efforts to protect children from indecent material online with the Child Online Protection Act of 1998. *Gore Pushes For 'Electronic Bill of Rights'*, REPORTER'S COMMITTEE FOR FREEDOM OF THE PRESS (Aug. 24, 1998), https://www.rcfp.org/gore-pushes-electronic-bill-rights/; Child Online Protection Act of 1998, H.R. 3783, 105th Cong. (1998).

[8] MARTHA K. LANDESBERG ET AL., FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS iii (1998) (The FTC study was influenced by reports and statistics from the Center for Media Education and the Better Business Bureau's Children's Advertising Review Unit.).

[9] *Id.* at 4–5.

[10] *Id.* at 5–6.

[11] *Id.* at iii.

[12] *Consumer Privacy on the World Wide Web: Prepared Statement by the Fed. Trade Comm'n Before the Subcomm. on Telecomm., Trade and Consumer Protection of the H. Comm. on Com.*, 105th Cong. (1998) (statement of Robert Pitosky, Chairman, Federal Trade Commission).

In July 1998, a privacy bill was introduced by Senators Bryan and McCain.[13] Senator Bryan noted with introduction that "[u]nfortunately, the same marvelous advances in computer and telecommunication technology that allow our children to reach out to new resources of knowledge and cultural experiences are also leaving them unwittingly vulnerable to exploitation and harm by deceptive marketers and criminals."[14] Chairman Pitofsky testified again in the fall, reiterating that the Commission had concluded that self-regulatory efforts "have not produced an adequate level of protection" for children online.[15]

As explained by Senator Bryan:

> Web sites were using games, contests, and offers of free merchandise to entice children to give them exceedingly personal and private information about themselves and their families. Some even used cartoon characters who asked children for personal information, such as a child's name and address and e-mail address, date of birth, telephone number, and Social Security number. Much of this information appears to be harmless, but companies are attempting to build a wealth of information about you and your family without an adult's approval—a profile that will enable them to target and to entice your children to purchase a range of products. The Internet gives marketers the capability of interacting with your children and developing a relationship without your knowledge.[16]
>
> The goals of this legislation are: (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's

[13] S. 2326, 105th Cong. (1998).

[14] 144 CONG. REC. 96 (1998) (Statement of Sen. Bryan).

[15] *Electronic Commerce: The Current Status of Privacy Protections for Online Consumers*: *Hearing before the H. Subcomm. on Telecommunications, Trade, and Consumer Protection*, 106th Cong. 106–39 (July 13, 1999) (statement of Robert Pitofsky, Chairman, Federal Trade Commission). The FTC had noted in its Report that "industry association guidelines generally encourage members to provide notice of their information practices and some choice with respect thereto but fail to provide for access and security or for enforcement mechanisms." *See* LANDESBERG, *supra* note 8, at ii.

[16] 144 CONG. REC. 96 (1998) (Statement of Sen. Bryan).

> privacy by limiting the collection of personal information from children without parental consent. The legislation accomplishes these goals in a manner that preserves the interactivity of children's experience on the Internet and preserves children's access to information in this rich and valuable medium.[17]

COPPA's protections end when a child turns thirteen years old.[18] This was not the original recommendation of the Commission or intent of the sponsors.[19] The 1998 Report explored differing levels of protection for different ages:

> Children's privacy legislation also would recognize that a marketer's responsibilities vary with the age of the child from whom personal information is sought. In a commercial context, Congress and industry self-regulatory bodies traditionally have distinguished between children aged 12 and under, who are particularly vulnerable to overreaching by marketers, and children over the age of 12, for whom strong, but more flexible protections may be appropriate. In each case, the goal of legislative requirements should be to recognize the parents' role with respect to information collection from children.[20]

The Commission proposed a parental consent model for twelve-year-olds and younger, and parental notice and an opportunity to opt-out for over thirteen-year-olds.[21]

The original bill introduced by Senators Bryan and McCain included requirements that operators "use reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of twelve and under the age of 17."[22] Remnants of efforts to protect older children can also be found in the bill from Senator Markey, a House co-author of COPPA in 1998, whose bill defined children as under sixteen though specific protections were reserved for under thirteen-year-olds.[23] As he has since said, "It was too young and I knew it was too young then."[24] Senator Markey

---

17 144 CONG. REC. 151, (1998) (Statement of Sen. Bryan).

18 Children's Online Privacy Protection Act, 15 U.S.C § 6501(1).

19 LANDESBERG, *supra* note 8.

20 LANDESBERG, *supra* note 8, at 42–43.

21 LANDESBERG, *supra* note 8, at 12.

22 Children's Online Privacy Protection Act of 1998, S. 2326, 105th Cong. § 3(a) (1998).

23 *See* Electronic Privacy Bill of Rights Act of 1998, H.R. 4667, 105th Cong. § 105 (1998).

24 Julie Jargon, *How 13 Became the Internet's Age of Adulthood*, WALL ST. J. (June 18, 2019), https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-

first introduced a broader privacy bill, which turned into the House COPPA.[25] But teen protections were not part of the final bill.[26]

Parents consenting, or being able to object, on behalf of teens made a variety of diverse stakeholders nervous. Civil liberties groups were concerned with requiring a fifteen-year-old to get parental consent before he or she could visit certain websites or access certain online information.[27] Companies also opposed such rules.[28] As those involved with drafting COPPA recall, "[i]t was one of those rare situations where the interests of industry and the concerns of civil liberties groups aligned."[29] There was also a belief that it is easier to distinguish between sites targeted at young children versus a general audience than between sites meant for teens versus a general audience—indeed, a footnote in the 1998 report mentions that "[a]ccording to one source, most children's Web sites are targeting children ages eight to eleven. Teens tend to visit the same sites that adults visit."[30]

Senator Bryan explained the compromise as the bill progressed, noting its success was in part "due to revisions to our original bill that were worked out carefully with the participation of the marketing and online industries, the Federal Trade Commission, privacy groups, and First Amendment organizations."[31]

III. COPPA'S PROTECTIONS

The COPPA version that Congress passed, and that the Federal Trade Commission implemented into regulations, was designed to put parents in the driver's seat.[32] It required companies explain to parents what information they collect, how they use and share it, how they protect it, and how parents can review and delete it—before collecting any information from kids.[33] This way, parents can make informed decisions about whether or not to consent to their children using various sites and services.

COPPA has some built in limitations. First, COPPA only applies to websites, apps, and services that are directed to or targeted at kids under thirteen (because, for example, they have a lot of cartoons that would appeal to kids) or that they *know* a child is under thirteen (because, for example,

11560850201.

[25] *See* Electronic Privacy Bill of Rights Act of 1998, H.R. 4667, 105th Cong.Title II (1998).

[26] *See* H.R. 4667, 105th Cong. § 101(a); *see also* S. 2326 105th Cong. § 3(a) (1998).

[27] Jargon, *supra* note 24.

[28] Jargon, *supra* note 24.

[29] Jargon, *supra* note 24.

[30] LANDESBERG, *supra* note 8, at n. 18.

[31] 144 CONG. REC. 151, 12787 (1998) (statement of Sen. Bryan).

[32] Children's Online Privacy Protection Act, 15 U.S.C. § 6501(9).

[33] *Id.*

they ask a child's birthdate).[34] Second, COPPA requires that companies get *verifiable* parental consent.[35] This means companies must make a reasonable effort to ensure they have received consent from a parent and not a clever child, but they do not have to go to extremes to comply.[36] Methods of obtaining consent include: talking to a parent via phone or video chat, obtaining credit card information, or communicating through multiple emails.[37] Another limitation is that COPPA only prevents companies from collecting personal information online *from* kids under thirteen, not information provided by adults about kids.[38] Last, COPPA only prevents companies from collecting information from kids under thirteen if sites have not obtained parental consent. With consent, companies may collect personal information from kids, so long as they do not require more information than is necessary for a child to participate.[39] This last prohibition is an important one, and it speaks to data minimization and use limitation notions that have become more popular in the ensuing decades; however, it is rarely enforced and has not been the focus of serious rulemaking. Currently, if a company tells a parent it needs to share a child's information with advertisers in order to provide a free app and a parent provides consent, then the child's information may be shared for marketing purposes. In addition, under COPPA, sites are supposed to enable parents to approve sharing with the site itself but not with other third parties.[40] This, however, is also an under-enforced and underappreciated aspect of the law.

Enforcement is a key aspect of any law. COPPA's authors allowed for multiple types of government and self-regulatory enforcement, but the statute does not contain a private right of action. COPPA is primarily enforced by the Commission, and state Attorneys General can also bring cases.[41] While the Federal Trade Commission has brought over thirty COPPA cases,[42] states have increasingly played an active role in

[34] *See* discussion of the knowledge standard in Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 3971, 3977–78 (Jan. 17, 2013).

[35] Children's Online Privacy Protection Rule, 16 C.F.R § 312.5 (2013).

[36] Children's Online Privacy Protection Rule, 16 C.F.R § 312.5(b)(1) (2013) (requiring an operator make "reasonable efforts").

[37] 15 U.S.C. § 6501(9); *see also* 16 C.F.R. § 312.3; § 312.5.

[38] *See* 15 U.S.C. § 6501(b); 16 C.F.R. § 312.3.

[39] 16 C.F.R. § 312.3(d); § 312.7.

[40] 16 C.F.R. § 312.5(a)(2).

[41] Children's Online Privacy Protection Act, 15 U.S.C. § 6504 (1998); 15 U.S.C. § 6505(d).

[42] Joseph Simons, Chairman, Fed. Trade Comm'n, YouTube Settlement Press Conference (Sep. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543118/simons_remarks_youtube_settlement_press_conference.pdf (noting 31 cases).

enforcement.[43] Additionally, COPPA has a "safe harbor" provision, whereby third parties can apply to the Commission to offer certifications and guidelines to operators.[44] These safe harbor provisions have been criticized by some as examples of the fox guarding the henhouse.[45] Similarly, the Commission's own enforcement efforts have been criticized as lackluster, especially by advocates who have filed complaints only to receive nothing in response.[46]

Ultimately, while valid criticisms have been leveled against both COPPA's substantive protections as well as its enforcement,[47] the law has in a number of ways withstood the test of time despite rapid changes in technology.

IV. COPPA SINCE ENACTMENT

Even though COPPA's statutory text has not been touched by Congress since its passage, the rule itself has in many ways kept pace with technology. This is due to the Commission's efforts, both in terms of statutorily-required rulemaking, as well as in more informal ways, such as guidance to businesses, online Frequently Asked Questions ("FAQs"), and policy enforcement statements.[48] Through these mechanisms, COPPA has

---

[43] *See, e.g.*, *id.* (noting settlement by FTC & New York Attorney General); NYS Attorney General, *A.G. Schneiderman Announces Results of "Operation Child Tracker," Ending Illegal Online Tracking of Children at Some of Nation's Most Popular Kids' Websites*, (Sep. 13, 2016) https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online; Natasha Singer and Daisuke Wakabayashi, *New Mexico Sues Google Over Children's Privacy Violations*, N.Y. TIMES (Feb. 20, 2020) https://www.nytimes.com/2020/02/20/technology/new-mexico-google-lawsuit.html.

[44] Children's Online Privacy Protection Act, 15 U.S.C. § 6503 (1998).

[45] *See, e.g.*, Rohit Chopra, Commissioner, Fed. Trade Comm'n, Common Sense Media Truth About Tech Conference (April 2014), https://www.ftc.gov/system/files/documents/public_statements/1512078/chopra_-_truth_about_tech_4-4-19.pdf.

[46] *Protecting Innocence in a Digital World: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. 2 (2019) (statement of Angela J. Campbell, Professor, Georgetown Law).

[47] *See* Marc Rotenberg before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance, *An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA): Hearing Before the Subcomm. On Consumer Protection, Product Safety, and Insurance of the S. Comm. on Com., Sci., and Transp.*, 111th Cong. 5 (2010) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center); *see also Protecting Innocence in a Digital World: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. 2 (2019) (statement of Angela J. Campbell, Professor, Georgetown Law).

[48] *See* Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions (March 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions; Fed. Trade Comm'n, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business (June 2017),

remained relevant in a mobile, connected-everything world.

A. FTC Rulemaking

One of COPPA's biggest benefits is the Commission's rulemaking authority, which allows COPPA to stay up to date via APA-style rulemaking (a power the FTC lacks in many other arenas).[49] But even without formal rules, there are numerous informal ways the Commission has acted to ensure COPPA addresses new technology (ex ante), including via its online FAQs, more formal policy statements, blog posts, workshops, parental consent mechanism approval, and advice and guidance to businesses.[50] Because these methods may be used by the Commission as often as it sees fit, they allow the Commission to be more nimble in terms of updating guidance. Drafting a blog post, or even putting out a policy statement approved by all five Commissioners, can occur significantly more easily and quickly than formal rulemaking (let alone passing new legislation).

The Commission began a major rule update in 2010, largely in response to social media and mobile applications.[51] The revised rules were meant to ensure COPPA continued to protect kids by addressing new ways in which: (1) ad networks were following kids across sites and services, (2) mobile devices were enabling location tracking, and (3) social media companies

https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance; Fed. Trade Comm'n, Federal Trade Commission Enforcement Policy Statement Regarding the Applicability of the Children's Online Privacy Protection Act Rule to the Collection and Use of Voice Recordings (Oct. 20, 2017), https://www.ftc.gov/public-statements/2017/10/federal-trade-commission-enforcement-policy-statement-regarding.

[49] *See Oversight of the Federal Trade Commission: Prepared Statement of the Fed. Trade Comm'n Before the Subcomm. on Digital Com. and Consumer Protection of the H. Comm. on Energy and Com.*, 115th Cong. 6 (2018) (noting "the FTC lacks broad APA rulemaking authority for privacy and data security generally" but children's privacy is an exception). Under Administrative Procedure Act (APA) rulemaking, there is a more streamlined process whereby an agency typically gives notice of a proposed rule in the Federal Register, accepts public comments, and then publishes a final rule. *See* Electronic Privacy Information Center, *The Administrative Procedure Act (APA)*, https://epic.org/open_gov/Administrative-Procedure-Act.html (last visited Apr. 13, 2020); *see also*, Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979 (2015) (Since 1980, the Commission has had to undertake much of its rulemaking under far more burdensome and time-consuming Magnuson-Moss procedures).

[50] *See* Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions, *supra* note 48.

[51] Fed. Trade Comm'n, *FTC Seeks Comment on Children's Online Privacy Protections: Questions Whether Changes to Technology Warrant Changes to Agency Rule* (Mar. 24, 2010), https://www.ftc.gov/news-events/press-releases/2010/03/ftc-seeks-comment-childrens-online-privacy-protections-questions (asking "What implications for COPPA enforcement are raised by mobile communications, interactive television, interactive gaming, or other similar interactive media").

were encouraging kids to share information.[52] Importantly, under the revised rule, personal information explicitly includes screen names, persistent identifiers used to identify individuals over time and across sites (such as IP addresses or device identifiers), geolocation, and photos, videos, and audio recordings.[53] The revised rule recognizes that while a photograph would not help you contact someone in the mid-90s, it does today.[54]

B. Online FAQs

Another major way the Commission keeps the rule updated is via its online FAQs, which are helpful in terms of providing plain-language guidance to businesses and parents.[55] They also enable the Commission to be even more nimble than it could be in rulemaking.[56] For example, in 2012, just as the Commission was concluding its rulemaking, but before the ink was dry on the revised rules, children's privacy advocates were grappling with a new concern—the growing rise of EdTech (educational technology), districts outsourcing new functions, and companies collecting information from kids in school. From 1999 to 2000, one-fifth of schools had no broadband Internet, and one computer per nine students was normal.[57] In 2014, states started passing EdTech focused privacy laws, but the federal government did not act.[58] As a result, in 2015, the Commission updated the COPPA FAQs and tried to explain how COPPA can work to protect kids in schools.[59]

Specifically, the Commission attempted to clarify when schools could provide consent to EdTech vendors on behalf of parents. The Commission indicated that a school can provide consent for a parent, or can be assumed to have obtained consent on behalf of a parent.[60] Reflective of the purpose

[52] Statement of Basis and Purpose on Children's Online Privacy Protection Rule Final Rule, 78 Fed. Reg. No. 12 3972-2996 (Jan. 17, 2013).

[53] *See* Children's Online Privacy Protection Rule, 16 CFR § 312.5.

[54] Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 3971, 3981 (Jan. 17, 2013).

[55] *See* Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions, *supra* note 48.

[56] The enforcement capacity based on these FAQs is questionable, unfortunately, and updating rules with respect to EdTech was one of the Commission's stated reasons for opening a rule review in 2019.

[57] U.S. DEPARTMENT OF EDUCATION, INTERNET ACCESS IN U.S. PUBLIC SCHOOLS AND CLASSROOMS: 1994-2005, 4, 7 (2006), https://nces.ed.gov/pubs2007/2007020.pdf.

[58] *Privacy Matters: Protecting Digital Privacy for Parents & Kids*, COMMON SENSE MEDIA, at 11 https://www.commonsensemedia.org/sites/default/files/uploads/kids_action/csm_privacymatters_protecting_digital_privacy.pdf (last visited Mar. 24, 2020).

[59] Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions, *supra* note 48.

[60] These are separate concepts—in the latter, a school is expected to obtain the consent

of a school and the fact that parents trust schools with their children's education, any such consent is to be limited to the educational context, where children's information is collected solely for the use and benefit of the school. If the information is collected or used for any other commercial purpose, a school cannot consent.[61]

C. Policy Enforcement Statements & Parental Consent Mechanisms

More recently, the Commission has acted to ensure that COPPA rules addressed privacy concerns raised by connected toys and other home devices that collect information from children. Starting in 2015, high profile data breaches of connected toys, like VTech and CloudPets, became common, exposing millions of children's information, and revealing the sensitive information these devices collect, as well as their lack of basic security.[62] Some of these device makers even claimed that they fell outside of COPPA.[63]

from the parents and then pass that along to a company, in the former, the school can act in the parent's stead and provide consent. The Commission has been urged to clarify. *See Common Sense Comments on COPPA Rule Review*, COMMON SENSE MEDIA (Dec. 9, 2019), at 11–12; *see also* Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions, *supra* note 48; *see also Common Sense Comments on Children's Online Privacy Protection*, COMMON SENSE MEDIA (April 3, 2009), at 8.

[61] Complying with COPPA, *supra* note 48. As demonstrated by the Commission's recent workshop with the Department of Education, people still have questions over what exactly constitutes an educational purpose—but again, the FTC, in conjunction with the Department of Education, is endeavoring to address these—and ensure COPPA can keep protecting kids; *see also* Fed. Trade Comm'n, Student Privacy and Tech Ed, Constitution Center, Washington, D.C. (Dec. 1, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech.

[62] *See generally* Complaint at 8, United States v. Vtech Electronics Limited, No. 1:18-cv-144 (N.D Ill. Filed Jan. 8, 2018); *see also* Press Release, Fed. Trade Comm'n, Electronic Toy Mater Vtech Settles FTC Allegations That it Violated Children's Privacy Law & the FTC Act (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated (Vtech will pay a settlement to the FTC for violating COPPA by failing to get parental consent and to provide reasonable security); *see* Danny Yadron and Anjie Zheng, *Vtech Holdings: Data From 5 Million Customer Accounts Breached*, WALL ST. J. (Nov. 30, 2015), https://www.wsj.com/articles/vtech-holdings-data-from-5-million-customer-accounts-breached-1448896876 (5 million accounts, passwords, home addresses, photo/names/online chats leaked); *see also* Press Release, Sen. Warner Pushes FTC to Protect Children's Data Security with Internet-connected "Smart Toys" (May 22, 2017), https://www.warner.senate.gov/public/index.cfm/2017/5/warner-ftc-interntet-of-things-letter
(Sen. Mark Warner pressing Commission to action after noting Spiral Toys' CloudPets products reported to have exposed two million voice recordings sent between parents and children).

[63] *See* Letter from Mark Meyers, Chairman & CEO of Spiral Toys, to Sen. Bill Nelson, attached to Letter from Sen. Nelson to Chairwoman Ohlhausen, (Mar. 29, 2017) (available at https://www.warner.senate.gov/public/index.cfm/2017/5/warner-ftc-interntet-of-things-letter) (asserting that connected plush toys, CloudPets, were not subject to COPPA because the toy did not connect to the internet—only bluetooth—and COPPA covers kids sharing information online).

In 2017, the Commission put out a policy enforcement statement confirming that COPPA applied to IoT ("Internet of Things" or "smart") devices, and also explaining how some carve-outs applied.[64] Specifically, the Commission stated that when audio functions solely as a replacement for written words—such as a search a user makes to a smart-speaker that the user would have in the past typed into a search-engine—and "is briefly maintained in order to fulfill the request and then deleted almost instantaneously," the Commission would not treat this as a collection of personal information without consent.[65] Nonetheless, COPPA's other provisions applied.[66]

The Commission also has updated approved parental consent mechanisms and safe harbor practices.[67] The list of approved parental consent mechanisms shows how the law has been able to move with technology. For instance, in the original list of approved mechanisms, there is a "signed facsimile."[68] In later years, however, parental consent mechanisms that have been approved include asking knowledge-based questions (similar to what a bank may do) and using facial recognition to match an adult with a verified government ID—something that would have been unthinkable when COPPA was first passed.[69] Relatedly, safe harbors have updated their rules and requirements for their own programs.[70]

V. KIDS' EXPERIENCES WITH TECHNOLOGY HAVE CHANGED DRAMATICALLY

The past two decades have seen efforts by the Commission to keep the

---

[64] Press Release, Fed. Trade Comm'n, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings (Oct. 20, 2017), https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.

[65] Press Release, Fed. Trade Comm'n, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings (Oct. 20, 2017), https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.

[66] *Id.*

[67] *See, e.g.*, Fed. Trade Comm'n, FTC Grants Approval for New COPPA Verifiable Parental Consent Method (Dec. 23, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method; *see also* Fed. Trade Comm'n, FTC Approves iKeepSafe COPPA "Safe Harbor" Oversight Program (Aug. 6, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-ikeepsafe-coppa-safe-harbor-oversight-program.

[68] *See* Children's Online Privacy Protection Rule, 16 CFR § 312.5.

[69] Kristin Cohen & Peder Magee, *FTC Updates COPPA Compliance Plan for Business*, FED. TRADE COMM'N (June 21, 2017).

[70] Fed. Trade Comm'n, FTC Approves iKeepSafe COPPA "Safe Harbor" Oversight Program, *supra* note 67.

regulations current, no real efforts by a majority in Congress to update the law, and, perhaps most importantly, a seismic shift in the technological landscape kids face. Children and teenagers are currently left exposed to a variety of privacy risks, and some statutory updates are necessary.

Children today face surveillance unlike any other generation—their every movement, online and off, can be tracked by potentially dozens of companies and organizations.[71] Young people will spend their entire lives connected in order to get an education and participate in modern society. This extensive exposure puts them at an increased risk of privacy harms—a risk that is compounded by the fact that their brains are still developing.[72] Kids are prone to over-sharing and impulsive behavior, more susceptible to advertising, and less able to understand what may happen to their personal information.[73] Further, the mechanisms teens use to get online—often mobile—are more likely to be "always on" and have increased tracking capabilities, including location tracking.

A. An "Always On" Life

Young people spend a lot of time connected. Common Sense Research has found that nearly every child under eight years old in America (98%) has access to a mobile device at home, a rise from just over half in 2011.[74] By age eleven, a majority of kids have a smartphone.[75] Kids aged eight and under spend an average of two hours and nineteen minutes a day with screen media.[76] Teens report that they feel addicted, and a quarter of teens report using the internet constantly.[77] According to the U.K. Children's Commissioner, on average, 1,300 photos of a kid will be posted before they

[71] *See, e.g.*, Children's Comm'r, More data is collected about children growing up today than ever before (Nov. 8, 2018), https://www.childrenscommissioner.gov.uk/our-work/digital/who-knows-what-about-me/; *see also* Stephanie Simon, *The big biz of spying on little kids*, POLITICO (May 17, 2014), https://www.politico.com/story/2014/05/data-mining-your-children-106676.

[72] *See* discussion of children and teens' developing brains *infra* Section V.F.

[73] *See* Adriana Galvan et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents*, 26 JOURNAL OF NEUROSCIENCE 25 (2006); *cf.* Adriana Galvan & Kristine M. McGlennen, *Enhanced Striatal Sensitivity to Aversive Reinforcement in Adolescents versus Adults*, 25 JOURNAL OF COGNITIVE NEUROSCIENCE 2 (2013).

[74] Victoria Rideout & Michael Robb, *The Common Sense Census: Media Use by Kids Age Zero to Eight*, at 3, COMMON SENSE MEDIA (2017).

[75] Victoria Rideout, *The Common Sense Census: Media Use by Tweens and Teens*, COMMON SENSE MEDIA, at 5 (2019).

[76] Rideout & Robb, *supra* note 74, at 18.

[77] Amanda Lenhart, *Mobile Access Shifts Social Media Use and Other Online Activities*, PEW RESEARCH CENTER (Apr. 9, 2015) ("92% of teens report going online daily—with 24% using the internet 'almost constantly,' 56% going online several times a day.").

turn thirteen years old.[78] Furthermore, children themselves post an average of twenty-six times a day to social media, averaging almost 70,000 posts by eighteen-year-olds.[79]

B. Sharing

Young people can also more inclined to share more information, although they may not appreciate the sensitivity of what they are sharing.[80] And teens today live in a culture that promotes sharing,[81] which shows no signs of abatement.[82] Teens also tend to act impulsively without fully thinking through the consequences.[83] Young people often do not understand what data they are sharing and with whom it will be shared with afterwards.[84] Additionally, they are unlikely to adopt complex security procedures, like private encryption, to protect themselves.[85]

C. Early Adopters of Invasive, Unsecure Technology

Kids are early adopters of new technology that often does not prioritize privacy, including inexpensive, unsecure apps, and connected devices that lack security updates or protective features.[86] Significantly, teens, especially lower income teens, are more likely to have access to phones than computers.[87] In fact, a 2015 Common Sense report found that teens spent

[78] *Who Knows What About Me?*, CHILDREN'S COMM'R (Nov. 8, 2018), https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/

[79] *Id.*

[80] *See, e.g.*, Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke Childs, Max Van Kleek, & Nigel Shadbolt,*"I make up a silly name:" Understanding Children's Perception of Privacy Risks Online*, at 2, CHI Conference on Human Factors in Computing Systems Proceedings 2019 (May 2019), https://arxiv.org/pdf/1901.10245.pdf (teenagers "failed to perceive the potential threat of re-identification via the particular fragments they shared, e.g., images or geo-location.").

[81] Rideout, *supra* note 75; *see also* Rideout & Robb, *supra* note 74.

[82] Rideout, *supra* note 75; Amanda Lenhart, *Teens, Social Media & Technology Overview 2015*, PEW RESEARCH CENTER (Apr. 9, 2015) ("71% of teens use more than one social network site.").

[83] *Protecting Consumer Privacy in an Era of Rapid Change*, at 80, FED. TRADE COMM'N (Mar. 2012).

[84] Mary Madden et al., *Teens, Social Media, and Privacy*, PEW RESEARCH CENTER (May 21, 2013); *see also* Zhao, *supra* note 80.

[85] Madden et al., *supra* note 84.

[86] *See* Public Service Announcement Federal Bureau of Investigation, *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*, Alert Number 1-071717 (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx (toys can be particularly problematic because of their wide collection capabilities and low price point; the FBI has put out warning to families about these risks).

[87] Monica Anderson & Jingjing Jiang, *Teens, Social Media & Technology 2018*, PEW RESEARCH CENTER (May 31, 2018).

over four hours a day on mobile media.[88] The report also found that teens were two and a half times more likely to access social media via a smartphone than a computer, and three times more likely to have video game consoles as opposed to desktop computers in their bedroom.[89] The means and methods teens use to access social media appear to put them at greater risk. Mobile and connected devices collect sensitive information such as voice, video, health data, and location information, and they are often located in traditionally personal and private locations such as in the home or worn on one's body.[90] Many of these devices are used by kids whether they are designed for them or not.[91] The devices share information with each other and with the network, allowing tracking of individuals not only on one device, but across devices.[92] While this can allow for more customization and personalization, it also means companies can build a richer user profiles.[93] Often, this information collection and sharing happens without a user's—or user's parents'—knowledge or understanding.[94]

Moreover, personal information collected by these devices is often poorly protected.[95] With many device makers focused on developing the latest hit gadget, privacy and security are an afterthought.[96] Many of these

---

[88] Rideout, *supra* note 75.

[89] Rideout, *supra* note 75, at 23–24.

[90] *See* Common Sense Kids Action, *Re: Common Sense Kids Action Comments on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (Jun 2, 2016), https://www.ntia.doc.gov/files/ntia/publications/csmntiacomments6.2.16.pdf; *see, e.g.*, OWLET, https://owletcare.com/ (last visited Apr. 13, 2020) (Owlet smart sock, which wraps around a baby's foot to monitor oxygen, heart rate, and sleep and combines with a live video camera to stream from a baby's nursery); Samsung, *Smartthings-Tracker*, https://www.samsung.com/us/smart-home/smartthings-tracker/
(small device can be placed in a child's clothing or bag and used to track location) (last visited Apr. 13, 2020).

[91] For example, the Nest smart thermostat line of products, installed in homes, says they do not collect information from children under thirteen. Privacy Statement for Nest Products and Services, NEST https://nest.com/legal/privacy-statement-for-nest-products-and-services/ (last visited Apr. 13, 2020). But children under thirteen live in homes with Nest devices and their information collection still occurs.

[92] Common Sense Kids Action, *Response Comments to November 2015 Workshop on Cross-Device Tracking* (Dec. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/12/00066-99854.pdf.

[93] *Id.*

[94] *Id.*

[95] Common Sense Kids Action, *Re: Common Sense Kids Action Comments on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, *supra* note 90.

[96] Wired Brand Lab, *IOT is Coming Even if the Security isn't Ready: Here's What To Do*,
https://www.wired.com/brandlab/2017/06/iot-is-coming-even-if-the-security-isnt-ready-heres-what-to-do/ (last visited Apr. 13, 2020).

devices are cheap or not able to receive security updates, routinely hacked, and, most glaringly, security is frequently not the priority.[97] As noted above, CloudPet's connected stuffed animals compromised the personal information of over half a million users, and a cyberattack on toy company VTech exposed the data of 6.4 million kids.[98] Almost sixty percent of connected devices do not provide proper information on how they collect, use, and disclose users' personal information.[99] Indeed, the Federal Bureau of Investigation has even put out a special warning regarding the privacy and security risks of smart toys.[100] Over three-quarters of consumers polled were concerned about the security and privacy risks of kids' connected devices.[101]

D. Digital Learning

Young people are also exposed because they are often required to go online to receive an education.[102] When connecting in schools, or in libraries, there are often technical limits to how much young people can protect themselves when using privacy protective technology from prying corporate or government interests.[103] One-third of all K-12 students in U.S. schools

---

[97] *Id.*

[98] Alex Hern, *CloudPets Stuffed Toys Leak Details of Half a Million Users*, THE GUARDIAN (Feb. 28, 2017), https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults; Hayley Tsukayama, *Vtech Says 6.4 Million Children Profiles Were Caught Up In Its Data Breach*, WASH. POST (Dec. 1, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/.

[99] Que Gatineau, *Results of the 2016 Global Privacy Enforcement Network Sweep* (Sep. 22, 2016), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/.

[100] Public Service Announcement, *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*, FEDERAL BUREAU OF INVESTIGATIONS (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx.

[101] ESET AND NAT'L CYBER SEC. ALLIANCE, *Our Increasingly Connected Lives*, 1 (Oct. 24, 2016), https://cdn3.esetstatic.com/eset/US/resources/press/ESET_ConnectedLives-DataSummary.pdf.

[102] *The Common Sense Census: Inside The 21st-Centruy Classroom*, COMMON SENSE https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom-key-findings.pdf (last visited Apr. 13, 2020) (Only 5% of K-12 teachers report using no digital tools, and 8/10 have computing devices in the classroom); *The Homework Gap: Teacher Perspectives on Closing the Digital Divide*, COMMON SENSE https://www.commonsensemedia.org/sites/default/files/uploads/kids_action/homework-gap-report-2019.pdf (last visited Apr. 13, 2020) (Prior to 2020, over 40% of high school students reported needing the internet at least once a week for schoolwork); *Map: Coronavirus and School Closure*, EDUC. WEEK (Apr. 11, 2020) https://www.edweek.org/ew/section/multimedia/map-coronavirus-and-school-closures.html (With 55.1 million students affected by pandemic school closures in 2020 and remote learning being proposed for many students, this number has presumably ballooned).

[103] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Reply Comments of Common Sense Kids Action, State Educational Technology

use school-issued devices.[104] Eighty-six percent of high school students use a laptop to do schoolwork during the year.[105] Over half of elementary students report using tablets for schoolwork.[106] All this information can be used by bad actors in unexpected ways—including to determine medical procedures.[107] It can also be left unsecure for hackers and others to misuse, and this risk is exacerbated by educational data breaches.

E. Advanced Advertising & Segmenting Techniques

In addition, advertising has become more dynamic, persuasive, and personalized. Advertising, including to children and teens, can be based on any number of things: offline habits and hangouts, age, physical characteristics, family income, shows watched and stories read, and shops visited.[108] Large data brokers, tech companies, and ad networks seamlessly deliver "personalized" content to us at just the right moment, whether that is on a phone, TV, a "smart" billboard a pedestrian walks by that happens to catch their face (and identify it, or just categorize it based on age, ethnicity, or gender), or via a mailer to a teenage girl with special pregnancy-related offers.[109] Sometimes these ads are woven into native content, virtually indistinguishable to young (or old) eyes.[110] Unfortunately, the targeting and personalization is not just limited to advertisements—it is also content

Directors Association and Tech Plus, F.C.C., WC Docket No. 16-106 (2016).

[104] Frida Alim et al., *Spying on Students: School-Issued Devices and Student Privacy*, ELECTRONIC FRONTIER FOUNDATION 5 (2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy.

[105] Harris Poll, *Pearson Student Mobile Device Survey 2014 National Report: Students in Grades 4-12 34*, PEARSON(May 9, 2014), https://www.pearsoned.com/wp-content/uploads/Pearson-K12-Student-Mobile-Device-Survey-050914-PUBLIC-Report.pdf.

[106] *Id.*

[107] *See* Benjamin Harold, *Danger Posed by Student-Data Breaches Prompts Action*, EDUC. WEEK (Jan. 22, 2014), https://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html. Reports have even surfaced of mobile dentists targeting low-income youth for unnecessary procedures based on student records shared by schools.

[108] Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[109] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[110] *See, e.g.*, Dennis Shiao, *What You Need to Know About Native Advertising* (Feb. 14, 2019), https://contentmarketinginstitute.com/2019/02/about-native-advertising/ (Native advertising is when the advertisement matches the content it is placed with); Zhao, *supra* note 80 ("children remain poorly equipped to identify targeted promotional material online, including adverts and in-app promotions, exploiting tracked activity data"); *see also* Rachel Abrams & Cecilia Kang, *The Mystery of Teen Vogue's Disappearing Facebook Article*, N.Y. TIMES (Jan. 8, 2020), https://www.nytimes.com/2020/01/08/business/media/teen-vogue-facebook.html.

itself.[111] One child's search query for a school project could lead to different results than his classmate's in a wealthier ZIP code across town, and one teen's search for summer jobs could lead to different opportunities than another teen's depending on their online histories.[112]

The increasingly personalized and persuasive capabilities of companies raise a number of questions about who controls a child or teen's information, shared unknowingly as they go about their day. It also raises questions about commercialization and commodification of behavior online. Young kids themselves may be turned into unwitting marketers, as they participate in viral memes and other activities that may appear user-driven but are actually company-directed. This is particularly problematic because children under eight years old lack the cognitive ability to understand the persuasive intent of advertisements,[113] and over 75% of kids between eight to eleven years old cannot distinguish advertising from other content.[114] Older children very often confuse Google search ads with organic search results.[115] Additionally, teens may be unknowingly conscripted into being product ambassadors, encouraged to submit their own photos, and to share products and content with friends, all of which is monitored and monetized.[116] Even if an older teen has consented to share their information, they may not understand how

[111] *See* Josh Constine, *How Facebook News Feed Works*, TECHCRUNCH (Sep. 6, 2016), https://techcrunch.com/2016/09/06/ultimate-guide-to-the-news-feed/ (News feeds and search results are personalized and targeted); *see also* Nick Statt, *Google personalizes search results even when you're logged out, new study claims*, THE VERGE (Dec. 4, 2018), https://www.theverge.com/2018/12/4/18124718/google-search-results-personalized-unique-duckduckgo-filter-bubble.

[112] *See Big Data: A Tool for Inclusion or Exclusion: Comments of Common Sense Media*, COMMON SENSE MEDIA (Aug. 15, 2014), https://www.ftc.gov/system/files/documents/public_comments/2014/08/00016-92371.pdf.

[113] Samantha Graff, Dale Kunkel & Seth E. Mermin, *Government Can Regulate Food Advertising to Children Because Cognitive Research Shows That It Is Inherently Misleading*, 31 HEALTH AFFAIRS 392, 395 (2012).

[114] OFCOM, *Children and Parents: Media Use and Attitudes Report* 4, 86 (Nov. 2016), https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf. [hereinafter OFCOM 2016]

[115] OFCOM, *Children and Parents: Media Use and Attitudes Report* 8, (Nov. 20, 2015), https://www.ofcom.org.uk/__data/assets/pdf_file/0024/78513/childrens_parents_nov2015.pdf (sixteen percent of children ages eight to eleven could distinguish between a sponsored ad and an organic search result on Google). Even in 2020, companies keep pushing the envelope. Google's recent updates—before they were withdrawn based on public backlash—stood to make this even more confusing. *See* Jonathan Shieber, *Google backtracks on search results design*, TECHCRUNCH (Jan. 24, 2020), https://techcrunch.com/2020/01/24/google-backtracks-on-search-results-design/.

[116] *Generation Like*, PBS FRONTLINE (Feb. 18, 2014), http://www.pbs.org/wgbh/frontline/film/generation-like/; *see also* WORKGROUP ON CHILDREN'S ONLINE PRIVACY PROTECTION, REPORT TO THE MARYLAND GENERAL ASSEMBLY ON CHILDREN'S ONLINE PRIVACY, 17 (Dec. 30, 2013).

far the information will go and the lifelong consequences of that sharing.[117] Will the information be used by college admission officers to assess a teen's maturity? Will a teen posting about a soft drink find him or herself the target of other fast food or soda ads as other companies see what products he or she "likes?" Will insurance companies look at teens who like risky adventure sports and charge them more? We as society do not know whether information may end up in the future, and teens'—whose brains are still developing—brains certainly do not.

F. Developing Brains

Kids have trouble understanding these privacy harms as their brains are still developing. They are emotionally and cognitively different than adults, and lag behind in several areas, including: conceptualizing privacy, comprehending online data ecosystems, understanding terms of service, and recognizing ads.[118] Both young children and teens are prone to overshare, albeit for different reasons.[119] Fifty-eight percent of twelve to fifteen-year-olds think it is easy to delete their information online.[120] Children five to seven-years-old view GPS tracking favorably and not as a privacy concern, while eight to eleven-year-olds can view monitoring as positive to ensure their safety.[121] Children struggle to understand privacy policies, which can be long and full of legalese.[122] Young people have trouble understanding how their data is collected, shared, and used by companies.[123] Commercial data sharing can be particularly confusing for kids.[124] Teens are more likely to share information without thinking, focusing on the present and not considering or understanding the long-term consequences.[125] They are more

[117] See Zhao, *supra* note 80.

[118] *See* Zhao, *supra* note 80, at 1–3, 9 ("children's ability to recognize risks online remains inadequate" and children "remain unaware of . . . platforms, app designers, malicious actors, and others operating in digital ecosystems").

[119] Children may not understand what is going on, whereas teens may have a slightly better sense but be more likely to partake in risky behavior. *See* Zhao, *supra* note 80, at 2 (children have "little sense of the risks posed by the accumulation of personal data over time"); *see* Adriana Galvan et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents* 26 J. OF NEUROSCIENCE 25 (2006) (teens' brain development can bias them towards risky behaviors).

[120] OFCOM 2016, *supra* note 114.

[121] Sonia Livingstone et al., *Children's Data and Privacy Online: Growing Up in a Digital Age, An Evidence Review*, CHILD DEV. J. 18, (Dec. 2018).

[122] *Id.* at 15.

[123] *Id.*

[124] Sonia Livingstone, *What is the Children's Data and Privacy Online Project All About?*, LONDON SCH. OF ECON. (May 15, 2019), https://blogs.lse.ac.uk/parenting4digitalfuture/2019/05/15/what-is-the-childrens-data-and-privacy-online-project-all-about/.

[125] Galvan et al., *supra* note 119; Adriana Galván and Kristine M. McGlennen, *Enhanced*

subject to peer pressure, so stay and share in online communities where their friends are, even if they are no longer enjoyable.[126] Parents also feel fairly helpless when it comes to protecting kids' privacy.[127] In many instances, parents would like to make changes to protect privacy, but do not know where to begin.[128]

G. Kids are Harmed by Privacy Violations

The myth that kids do not care about privacy is just that, a myth.[129] Survey after survey shows that young people want their personal information to be better protected. U.K. research has shown that children are "outraged" when they learn what businesses are doing with the information they are collecting.[130] According to a recent consultation by the Irish Data Protection Commission, encompassing the views of some 1,200 children, sixty percent believed companies should not be allowed to use personal information to target them with ads.[131] Children found ads "annoying," "unfair," and "an invasion of privacy," and felt that "companies had no business using their

Striatal Sensitivity to Aversive Reinforcement in Adolescents versus Adults, 25 (2) J. OF COGNITIVE NEUROSCIENCE 284–296 (2013).

126 Center for Digital Democracy and the Campaign for a Commercial Free Childhood Comments before the Federal Trade Commission, *Competition and Consumer Protection in the 21st Century, Hearing #12: The FTC's Approach to Consumer Privacy (2019), at 12, citing Taylor Lorenz, Teens Are Being Bullied 'Constantly' on Instagram*, THE ATLANTIC (Oct. 10, 2018), https://www.theatlantic.com/technology/archive/2018/10/teens-face-relentless-bullyinginstagram/572164/ (teens stay on Instagram even with cyberbullying because "quitting wasn't an option").

127 Livingstone, *supra* note 121.

128 *What's That You Say? Smart Speakers and Voice Assistants Toplines*, COMMON SENSE MEDIA (May 2019), https://www.commonsensemedia.org/sites/default/files/uploads/pdfs/2019_cs-sm_smartspeakers-toplines_final-release.pdf. For example, a third of parents would like to limit data collection on smart speakers, but do not know where to begin.

129 *See, e.g.*, Zhao, *supra* note 80, at 2 ("Contrary to common expectations, children value their privacy"); Jon Henley, *Are Teenagers Really Careless About Online Privacy?*, THE GUARDIAN (Oct. 21, 2013), https://www.theguardian.com/technology/2013/oct/21/teenagers-careless-about-online-privacy (youth and social media researcher Danah Boyd noting, "what matters to [teens] is social privacy", teens are concerned about "things that might be seen by the people who have power over them: parents, teachers, college admissions officers").

130 Livingstone, *supra* note 121.

131 Know Your Rights and Have Your Say! *A Consultation by the Data Protection Commission on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the General Data Protection Regulation*, DATA PROTECTION COMM'N (Jan. 28, 2019), https://www.dataprotection.ie/en/news-media/know-your-rights-and-have-your-say-stream-two-dpcs-public-consultation-processing; *Some Stuff You Just Want to Keep Private*, DATA PROTECTION COMMISSION 3, 17 (2019) (Ir.), https://www.dataprotection.ie/sites/default/files/uploads/2019-08/Some%20Stuff%20You%20Just%20Want%20to%20Keep%20Private_Consultation%20Report.pdf.

personal data for profit."[132] The Irish DPC went on to explain, "other children recalled unsettling experiences of being 'followed' by personalized ads on the internet, and one group of eight to nine-year-olds drew parallels between TV ads and online ads, saying that online ads 'are so scary because they are pointed at you directly and not at everyone like a TV ad.'"[133] One child in the eight to twelve range said, "It feels like they're stalking you."[134]

Feelings do not differ that much across the Atlantic. According to research on American teens, more than nine in ten teens think it is important that sites clearly label what data they collect and how it will be used.[135] Almost seven in ten teens say it is "extremely important" for sites to ask permission before selling or sharing their personal information.[136] Only a third of teens agree that social networking sites and apps do a good job of explaining what they do with users' data.[137] Sixty-eight percent of teens are at least "moderately" worried that social networking sites use their data to allow advertisers to target them with ads.[138]

The risks and harms to children are multifold.[139] First, the fears that animated COPPA's authors—commercialism and safety—remain, though in many instances these fears are heightened. Today, marketers and data brokers can create dossiers beginning at birth, if not before, of a young person's interests, background, and physical characteristics, finely tuning sales pitches to impressionable audiences who may not even understand they are seeing ads, especially in complex digital environments.[140] Children's information may be used to market products to which they are particularly susceptible, leading to consumerism and family financial pressure, or the purchasing of inappropriate products.[141] Such marketing and profiling can lead to unhealthy behaviors and emotional harms, with serious consequences for a child's well-being. When advertisements for specific products are

---

132 Know Your Rights and Have Your Say!, *supra* note 131.

133 *Some Stuff You Just Want to Keep Private*, *supra* note 131.

134 *Some Stuff You Just Want to Keep Private*, *supra* note 131, at 17–18.

135 *Privacy Matters: Protecting Digital Privacy For Parents & Kids*, *supra* note 58, at 7.

136 *Privacy Matters: Protecting Digital Privacy For Parents & Kids*, *supra* note 58, at 7.

137 *Privacy Matters: Protecting Digital Privacy For Parents & Kids*, *supra* note 58, at 7.

138 *Privacy Matters: Protecting Digital Privacy For Parents & Kids*, *supra* note 58, at 7.

139 Girard Kelly et al., *Privacy Risks and Harms*, COMMON SENSE MEDIA 1 (2019), https://privacy.commonsense.org/content/resource/privacy-risks-harms-report/privacy-risks-harms-report.pdf.

140 *See Who Knows What About Me?*, CHILDREN'S COMM'R (Nov. 8, 2018); Sonia Livingstone, *YouTube's child viewers may struggle to recognise adverts in videos from 'virtual play dates.*', LONDON SCH. OF ECON. (2019), https://blogs.lse.ac.uk/parenting4digitalfuture/2019/09/25/youtubes-child-viewers-may-struggle-to-recognise-adverts/.

141 *Some Stuff You Just Want to Keep Private*, *supra* note 131, at 17. Financial pressure on families was one concern raised by children in the Irish DPC consultation.

regularly viewed by children 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.[142] Children who saw the online ads were significantly more likely to use the products.[143] Additionally, young adults, especially young women, are incredibly susceptible to advertisements related to body image.[144] After viewing these ads, women are more likely to objectify themselves.[145] Certain groups of children can be especially vulnerable. As discussed at a recent Commission workshop, research shows that more than 95% of the ads that Latino kids and African American children are seeing are for junk food, while other research confirms that children of color see proportionally more ads for food.[146]

In terms of physical safety, children continue to face physical risks of their information falling into the hands of those who want to hurt them, just as they did decades ago.[147] The constant and detailed collection of information, such as frequent postings on social media of photos with metadata information,[148] and the proliferation of devices and sensors in the home and worn on the body create particular risks.[149] Devices themselves

---

[142] Lisa Rapaport, *Teens Most Drawn to E Cigarettes by Online Ads*, REUTERS HEALTH REPORT (Apr. 2016), http://www.reuters.com/article/us-health-ecigarettes-internet-advertisi-idUSKCN0XM08T.

[143] *Id.* 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.

[144] Seeta Pai, *Children, Teens, Media, and Body Image*, COMMON SENSE MEDIA (Jan. 21, 2015), https://www.commonsensemedia.org/research/children-teens-media-and-body-image.

[145] *Id.* 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.

[146] Samantha Vargas Pope, Principal, Equity Matters, LLC, Panelist at The Future of the COPPA Rule: An FTC Workshop (Oct. 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_2_1.pdf; Lisa M. Powell et al., *Exposure to Food Advertising on Television Among US Children*, 161 ARCHIVES OF PEDIATRICS & ADOLESCENT MEDICINE, no. 6, Jan. 2007, at 553.

[147] *See* Christine Elgersma, *The Facts About Online Predators Every Parent Should Know* COMMON SENSE MEDIA (July 25, 2017), https://www.commonsensemedia.org/blog/the-facts-about-online-predators-every-parent-should-know.

[148] *Cyber Alerts for Parents & Kids Tip #1: Be Prudent When Posting Images Online*, FED. BUREAU OF INVESTIGATIONS (December 22, 2011), https://www.fbi.gov/news/stories/cyber-alerts-for-parents—kids-be-prudent-when-posting-images-online.

[149] *See, e.g.*, Joseph Venable, *Child Safety Smartwatches 'Easy' to Hack, Watchdog Says*, BBC NEWS (October 18, 2017), https://www.bbc.com/news/technology-41652742.

can be insecure, allowing someone to find your child's location[150] or to turn off your car remotely.[151] These devices can also pose risks because they are connected to a home network and can be used as an entry point to attack your smart security or other systems. Indeed, major networks have been taken down by insecure video cameras and DVRs.[152]

Policymakers and parents have concerns about newer risks and harms as well. Children face financial risks via identity theft or the ransoming of personal information.[153] Identity thieves are particularly attracted to children's clean credit history and the lower likelihood of prompt discovery of the theft.[154] Indeed, more than one million children were victims in 2017.[155] This is also connected to other harms children face online, including the use of their information to cyberbully, blackmail, or harass. The proliferation of cheap devices with cameras and more access to devices at younger ages allows children to share intimate personal information pictures or words more easily. This exposure may subject them to social and emotional harms.[156] Children who are cyberbullied are nine times more likely to be victims of identity theft.[157]

Further, algorithmic decision making, black box processing, and systems that makes guesses about and differentiate between children—to show them different results in response to a search for "summer jobs," for example, or "scholarships,"—can create further risks. Technology may label and/or limit children and cause them to miss opportunities. Or kids may be manipulated—see, for example, Cambridge Analytica and its goal of ideological manipulation of voters. Companies can employ so-called dark

150 *#WatchOut: Analysis of Smartwatches for Children*, NORWEGIAN CONSUMER COUNCIL (2017), https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf.

151 *See, e.g.*, *How auto dealers can us GPS and "starter interrupter" tech to disable your car*, CBS NEWS (Mar. 21, 2017), https://www.cbsnews.com/news/car-repossession-device-starter-interrupter-auto-dealer-car-credit-city/.

152 Nicole Perlroth, *Hackers used new weapons to disrupt major websites across U.S.*, N.Y. TIMES (October 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

153 *Cyber security: Experts warn on rise of hacker ransoms*, BBC NEWS (Mar. 14, 2017), https://www.bbc.com/news/uk-39260174. Experts predict a rise in the use of ransomware on devices, where hackers make devices—holding photos, emails, fitness information, or other information—unusable until owners agree to pay.

154 Al Pascual & Kyle Marchini, *2018 Child Identity Fraud Study, Javelin*, JAVELIN STRATEGY & RESEARCH (Apr. 24, 2018), https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study.

155 *Id*.

156 *See The Common Sense Census; Inside the 21st-Century Classroom*, COMMON SENSE (2019) https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom_1.pdf (Cyberbullying and sexting are both concerns reported by teachers especially as kids enter high school).

157 Pascual & Marchini, *supra* note 154.

patterns and nudges—using interface design to push a child towards certain selections over another, or to keep a child "hooked" with random pinging or reward loops—subverting user choice and autonomy and creating compulsive usage.[158] In terms of opportunities, one pressing concern for many families is higher education. It is therefore particularly concerning that college admissions officers are purchasing online browsing behavior to determine applicants' level of interest, intended major, and browsing of financial aid pages, and combining that with detailed parental profiles including loyalty card and shopping patterns.[159]

Ultimately, young people may temper their online exploration and self-censor their thoughts or withhold information, not wanting to engage in anything that may be deemed controversial. This is in fact reported behavior from children: when they know all their online activities are being monitored by surveillance technologies, children and students appear less likely to engage in critical thinking, political activity, or questioning of authority.[160] Thus, constant surveillance can squelch expression and limit opportunities for development. This does a disservice to young people, who need the freedom to make mistakes, try new things, and find their voices, unencumbered by the looming threat of a permanent digital record.[161]

VI. DESPITE NEW THREATS TO KIDS, CONGRESS IS UNABLE TO MOVE MEANINGFUL NEW LEGISLATION

Despite all these increased vulnerabilities, risks, and harms faced by children and teens, not to mention adults who are not immune to these harms either, the only non-sectoral federal consumer privacy law is COPPA.[162] This is despite valiant efforts by privacy champions, like Sen. Markey, who has re-introduced (typically bipartisan, bicameral) COPPA updates in no less than four of the last five Congresses.[163] Currently pending legislation,

---

158 Press Release, Senator Mark Warner, Senators Introduce Bipartisan Legislation to Ban Manipulative 'Dark Patterns' (Apr. 9, 2019) (available at https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns).

159 Douglas MacMillan & Nick Anderson, *Student Tracking, Secret Scores: How College Admissions Offices Rank Prospects Before They Apply*, N.Y. TIMES (Oct. 14, 2019), https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/.

160 *See* Duncan H. Brown & Norma Pecora, *Online Data Privacy as a Children's Media Right: Toward Global Policy Principles*, 8(2) J. OF CHILD. AND MEDIA 201–07 (2014).

161 Some California laws have put in place provisions enabling children (or everyone) to delete information. *See* discussion of the Eraser Button and CCPA laws below. Even so, these laws do not protect kids in all circumstances, as they have carve outs for others reposting information or internal uses.

162 *See, e.g.*, Singer, *supra* note 5. The United States has no consumer privacy law.

163 Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Do Not Track Kids

COPPA 2.0, which is co-authored with Sen. Josh Hawley, would extend protections to teens under sixteen, create liability when sites have constructive knowledge of the presence of young people, stop behavioral ad targeting of children, create privacy dashboard rules for connected devices, and add a new division focused on children and teens at the FTC.[164] Earlier this year, Representative Castor introduced another strong COPPA update bill, the KIDS PRIVCY Act, which, among other things, would extend protections to all teens up to eighteen years old, prohibit behavioral ad targeting to children, change the knowledge standard to include constructive knowledge, and enable parents to bring suits on behalf of their kids for violations.[165] Many of these bills have bipartisan backing.[166] And while there is always the hope that this session will be different than the last, history does not paint an optimistic picture of passage.

Congress has also failed to pass a general consumer privacy law. This is despite a groundswell of legislative introductions, especially since the 2018 Cambridge Analytica revelations, GDPR, and passage of the CCPA.[167] This is also despite the fact that approximately eight in ten Americans feel like they need more protections and that Congress should act.[168] And it is despite the fact that other countries across the world, from Europe to Brazil to Malaysia, are moving forward and passing and updating broad-based privacy protections.[169] Some of these laws recognize the unique

Act of 2015, H.R. 2734, 114th Cong. (2015); Do Not Track Kids Act of 2018, S. 2932, 115th Cong. (2018); COPPA 2.0, S. 748, 116th Cong. (2019).

[164] COPPA 2.0, S. 748, 116th Cong. (2019).

[165] *See* Press Release, Castor Introduces Kids PRIVCY Act to Strengthen COPPA (Jan. 30, 2020) (available at https://castor.house.gov/news/documentsingle.aspx?DocumentID=403195).

[166] Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Do Not Track Kids Act of 2015, H.R. 2734, 114th Cong. (2015); Do Not Track Kids Act of 2018, S. 2932, 115th Cong. (2018); COPPA 2.0, S. 748, 116th Cong. (2019).

[167] *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (numerous discussions of federal bills introduced after 2018, which SAE Analytica revelations); *see also California Becomes First State to Strengthen Consumer Data Privacy Protections*, COMMON SENSE MEDIA (Jun. 28, 2018) https://www.commonsensemedia.org/about-us/news/press-releases/california-becomes-first-state-to-strengthen-consumer-data-privacy; *see, e.g.*, Charlie Warrzel, *Will Congress Actually Pass a Privacy Bill?*, N.Y. TIMES (Dec. 10, 2019), https://www.nytimes.com/2019/12/10/opinion/congress-privacy-bill.html.

[168] Sam Sabin, *Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year*, MORNING CONSULT (Dec. 18, 2019), https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/.

[169] Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, GW L. FAC. PUBLICATIONS & OTHER WORKS 3 (September 20, 2019) (noting the "torrent" of data privacy legislation, and how a majority of over 200 countries recently

vulnerability of young people. For example, the GDPR recognizes that all children under eighteen are vulnerable and deserving of special protections.[170] It also enables E.U. countries to set their own parental consent standards anywhere between the ages thirteen and sixteen years old.[171]

As protections grow internationally, the U.S. has continued to offer only glimmers of hope towards an actual consumer privacy law. Some states, especially California, however, have picked up the slack. California passed the 2013 Eraser Button Law (SB 568), which requires sites to permit minor account holders to publicly delete information they have posted.[172] The law also prohibits advertising certain products, such as weapons, spray paint, and alcohol to minors.[173] Delaware has also passed a similar ad-targeting provision.[174] Both of these protections are reminiscent of those in Senator Markey's Do Not Track Kids legislation.[175] More recently, California passed the CCPA, which is similar to the proposed COPPA updates in that it offers heightened privacy protections to young teens and not just children under thirteen .[176] The CCPA also makes clear that the actual knowledge required to make a company responsible for protecting kids is not a strict standard, but also encompasses companies' willful disregard of a user's age.[177] More broadly, the CCPA gives all California residents access, deletion, and opt-out-of-sale rights.[178] In addition, dozens of states have passed student privacy laws addressing the collection of personal information of students by third-party EdTech companies.[179]

However, states cannot be relied upon to fill all the gaps, instead a uniform federal floor would better serve all children and families, as well as better serving the companies trying to comply. In an ideal world, Congress

surveyed have such a law). *See, e.g.*, Regulation 2016/679 of the European Parliament and of the Council of 27 Apr. 2016, General Data Protection Regulation (GDPR) (EU); Federal Law no. 13,709/2018, of Aug. 15, 2018, Brazilian General Data Protection Law (LGPD); Malaysia: Personal Data Protection Act 2010 (PDPA) (passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013).

170 *See, e.g.*, Information Commissioner's Office, *Children and the GDPR* (last visited Apr. 13, 2020) (Under the U.N. Convention on the Rights of the Child, Article 1, children are defined as anyone under 18. This applies to the GDPR); GDPR Art. 75 (all children are identified as a vulnerable population).

171 GDPR Art. 75, *supra* note 170, at Art. 8.

172 Eraser Button Law, S.B. 568, 2013 Leg., 2013-12 Sess. (Cal. 2013).

173 Eraser Button Law, S.B. 568, 2013 Leg., 2013-12 Sess. (Cal. 2013).

174 Delaware Online Privacy and Protection Act., 80 Del. Laws 148, § 1 (2019).

175 Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Do Not Track Kids Act of 2015, H.R. 2734, 114th Cong. (2015); Do Not Track Kids Act of 2018, S. 2932, 115th Cong. (2018).

176 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.120(c) (2018).

177 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.120(c) (2018).

178 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018).

179 *Privacy Matters: Protecting Digital Privacy for Parents & Kids*, *supra* note 58.

could introduce and pass comprehensive privacy legislation that includes special and strong protections for young people, like that found in Senator Markey and Hawley's COPPA 2.0 or Representative Castor's KID PRIVCY Act. That would be the best way to protect kids and families. But in a realistic world, one simpler and more attainable next step is to simply extend COPPA's protections to everyone.[180]

VII. SIMPLY EXTENDING COPPA TO ADULTS WOULD GO A LONG WAY TOWARDS IMPROVING PROTECTIONS FOR KIDS

Twenty years after introduction, COPPA remains a fairly flexible tool for addressing changing technology. Indeed, though technology has changed dramatically in the two decades since COPPA came into effect, much more than the protections themselves, the law remains relevant and useful, both to the Commission and to state Attorneys General. Within its statutory confines, the rule has largely kept pace with technology,[181] through the Commission use of a variety of mechanisms—such as regulatory rule reviews, online FAQs, and policy guidance. Additional innovations in the parental consent space have also helped keep COPPA up to date.[182] Further, though COPPA has primarily been enforced as a notice and consent law, its text actually goes further. The statute itself requires that sites use reasonable security, and it prohibits operators from conditioning a child's participation on giving up more information than is necessary.[183] It also offers access and deletion rights.[184] The regulations further provide that sites are to offer parents a right to consent to collection and use, but not further disclosure.[185]

Unfortunately, COPPA's protections currently stand alone, leaving families and businesses in a regulatory environment where it is COPPA-or-nothing, and a thirteen-year-old is essentially treated as an adult going on

[180] The FTC is currently considering whether it should update its rules and has asked the public for comment on conducting a rulemaking ahead of schedule. Tens of thousands of comments have (likely) overwhelmed the agency, and from many who make it a mission to advance consumer privacy, the better use of the FTC's limited time would be to focus on enforcing all aspects of the current Rule. If any governing text needs to change, it should be statutory text.

[181] This is not to say that enforcement has kept pace with technology, rather that COPPA is capable of enabling enforcement even on today's technology.

[182] Fed. Trade Comm'n, *FTC Grants Approval for New COPPA Verifiable Parental Consent Method* (Dec. 23, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method (the Commission has always been clear that the list of approved methods is non-exhaustive and has approved new methods as technology has changed. *See, e.g.*, the Commission's approval of knowledge-based questions in December 2013).

[183] Children's Online Privacy Protection Rule, 16 C.F.R. §§ 312.3(d) & 312.10.

[184] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.6.

[185] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(a)(2).

thirty.[186] If companies were put in a position where it was impossible to avoid COPPA—because, say, its protections applied to everyone—then time and resources that currently go into COPPA avoidance could be better directed to COPPA compliance and proactively building in privacy protections.

While the preferred way to improve privacy protections for children and teens would be for strong substantive updates to pass, preferably in a comprehensive federal privacy law, this may continue to be politically impossible.[187] The truth is, even if you kept COPPA's provisions the same, and simply extended its provisions across the board, including to adults (obviously adults would not need to get "parental" consent), that too would enhance protections for kids. Teens, obviously, would gain new rights. But even if technically children under thirteen would be offered the same protections, more sites and services would have to offer them, and more of a market would exist in which to protect privacy for kids *and* adults.[188] One of COPPA's biggest pain points lies in the fact that there exists between twelve and every older age a huge chasm in protections, so companies spend an enormous amount of time and money in trying to avoid COPPA's obligations. Companies choose not to be compliant or choose to prioritize adult content over kids' content.[189] *If* COPPA applied across the board, companies, regulators, and the public would not need to engage in any exercises to determine whether COPPA applied. It would apply. And because it applied across the board, the tech vendor industry would offer even more compliance assistance, just as have been offered for GDPR and CCPA.[190] Thus, more companies complying would lead to more technical assistance in compliance, thereby making it even easier to innovate and protect children's privacy. This would better protect kids. It would also address concerns about kids lying about their ages, another common COPPA problem, because even if kids avoided parental consent, they would still have other protections in place.[191] It would limit any privacy-related incentives to create compelling content for adults and not for children. Additionally, it does not require Congress to draft and debate lengthy pages of new

[186] Because COPPA's protections end once a child turns thirteen and there is no federal consumer privacy law that protects adults or teens, a thirteen-year old is treated the same way as a twenty-nine-year-old.

[187] While this essay focuses on how extending COPPA to adults and teens would better protect kids, there are other reasons we need a federal privacy law that covers teens and adults. We need it in order to remain competitive internationally. We need it for trade agreements. We need it because data is the new oil, and because US consumers have lost trust in the very space that consumes so much of their time and energy.

[188] See discussion of technology markets *infra* Section VII.B.

[189] *See* discussion of COPPA compliance *infra* Section VII.A.

[190] *See* discussion of vendor markets *infra* Section VII.B.

[191] *See* discussion of COPPA compliance *infra* Section VII.A.

legislation. So, if Congress cannot come up with a new law or extend substantive protections, then it should at the very least extend COPPA protections to everyone. And in so doing, it would better protect under thirteen-year-olds as well.

A. If COPPA Applied to Adults, Kids Would Gain Default Protections Everywhere—Whether or Not a Site Gets it Right, and Whether or Not Kids Lie

One of COPPA's major weaknesses is its limited application: it *only* applies to sites and services "directed to children," or to those who have "actual knowledge" they are collecting information from kids.[192] Thus, a question that drains resources around COPPA is determining who or what is a covered operator.[193] It can be hard for parents and complicated for companies to understand when COPPA applies, for example, when an operator has actual knowledge of a child or when content is child-directed, and companies often feign ignorance inappropriately.[194] It can take time for some companies to determine whether their content is directed to kids. It

---

[192] COPPA, 15 U.S.C. § 6502(a)(1).

[193] *See* Kristin Cohen, *YouTube channel owners: Is your content directed to children?*, FED. TRADE COMM'N (Nov. 22, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children (following the FTC's COPPA settlement with YouTube, one of the largest outcries was from YouTube channel operators who were unsure whether COPPA applied to their channels, a question the FTC attempted to address with online guidance); *see also*, Sarah Perez, *YouTube asks the FTC to clarify how video creators should comply with COPPA ruling*, TECHCRUNCH (Dec. 9, 2019), https://techcrunch.com/2019/12/09/youtube-asks-the-ftc-to-clarify-how-video-creators-should-comply-with-coppa-ruling/ (YouTube also asked the FTC for more guidance); *see also* Fed. Trade Comm'n, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June 2017) ,https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (numerous articles and advice are focused on helping companies determine whether COPPA applies to them. For example, the FTC's six-step compliance plan begins with determining if the rule applies); *see, e.g.*, TrustArc, *TRUSTe Children's Privacy/COPPA Assessments & Certification*, PRIVO https://www.privo.com/learn-more-about-coppa; https://trustarc.com/truste-certifications/coppa-certification/ (Last Visited Apr. 13, 2020) (COPPA safe harbors similarly offer checklists to consider if compliance is COPPA applies).

[194] John Herrman, *Who's Too Young for an App? Musical.ly Tests the Limits*, N.Y. TIMES (Sep. 17, 2016), https://www.nytimes.com/2016/09/17/business/media/a-social-network-frequented-by-children-tests-the-limits-of-online-regulation.html (for example, the Musical.ly app was widely popular with tweens, but the company claimed it was only for users over 13); *see also* Press Release, Fed. Trade Comm'n, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law (Feb. 27, 2019) (available at https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc) (years later it ultimately settled with the FTC). *See also* Fed. Trade Comm'n, *The Future of the Coppa Rule: An FTC Workshop Part 1* (Oct. 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf.

can take time for regulators and companies may lie about this or try to play games.[195] A similar problem occurs on the "actual knowledge" inquiry, and whether or not sites and services have "actual knowledge" that they are dealing with kids.[196] The Commission has traditionally defined actual knowledge fairly strictly.[197] As twenty-six state Attorneys General recently explained in a letter to the Commission, a strict actual knowledge definition "incentivizes companies to willfully ignore (or strategically refuse to cognize) information they receive about child audiences on their platforms."[198] Companies have also encouraged children to lie about their ages, despite the fact that the Commission has said COPPA requires a neutral age gate.[199] If COPPA's protections applied to everyone, companies could not simply ignore children and offer everyone else no privacy protections, as protections would be due to everyone. Companies would not need to spend time determining whether or not to comply with COPPA and could instead spend time building in place privacy protections. Even if age gates are still needed, for example to determine when parental consent or user self-consent is appropriate, companies would have less incentive to encourage children to lie. Further, if children did lie, just like if a child visited a site or service that was not "directed to children," that child would still enjoy privacy protections. All the other protections offered by COPPA—such as consent before collection and disclosure, rights to access and delete, reasonable security, not conditioning participation in a site or service on providing more information than is reasonably necessary—would still apply.

---

[195] *See infra* note 218; *see also* Fed. Trade Comm'n, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law* (Sep. 4, 2019) https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[196] *See Id.*

[197] *See* Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 12, at 3971 (Jan. 17, 2013) (explaining that they were not trying to move away from the current knowledge standard to a "constructive knowledge" standard). However, more recently with the YouTube decision some have questioned whether that strict interpretation still holds. *See, e.g.*, Phyllis Marcus, *The Future of COPPA Rule: An FTC Workshop*, FED. TRADE COMM'N (Oct. 7, 2019), https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop.

[198] Letter from Hector H. Balderas, Attorney General, New Mexico, to April Tabor, Acting Secretary, Fed. Trade Comm'n (Dec. 9, 2019) (available at http://www.marylandattorneygeneral.gov/news%20documents/120919_FTC_COPPA_Comment_letter.pdf?fbclid=IwAR0osuECgdCPwbocvQUpOf37Aa-BGsRCYuwMV1oyZmPdQd1KgXEJqBTd29Y). [hereinafter Balderas Letter]

[199] *See* Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (March 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions; *see also* Balderas Letter, *supra* note 198 ("Many operators use non-neutral age gating to encourage users to enter ages older than 12").

B. It Would be Easier for Companies to Comply with COPPA

In addition to time saved from not having to consider whether COPPA applied in the first place, companies would also find it easier to locate COPPA-compliant vendors, which is another repeated "concern" from industry.[200] It is not clear how serious this concern is, given the growing popularity of vendors like SuperAwesome, which recently told the Commission it enables twelve billion kid-safe transactions a month, and Yoti, an age verification service that reported a spike in interest following the TikTok settlement.[201] But, regardless, with broader application, even more vendors would follow.[202] The proliferation of vendors offering GDPR and CCPA compliance is testament to that.[203] Indeed, even Google has started to change its Analytics and Ads safeguards following CCPA.[204] If COPPA disallowed or disincentivized additional personal data collection, the spread of COPPA protections and growth of COPPA-compliant vendors could help move the internet more broadly away from a behavioral ad supported market in the first place, where business models are not driven by collecting and using as much personal information as possible. In fact, turning again to the example of the GDPR, some companies are finding that more traditional contextual ads, not based on an individual's profile or browsing habits, are just as if not more effective.[205] While intermediaries

---

[200] *See, e.g.*, *The App Association*, ACT https://actonline.org/what-we-know-now-coppa-and-3rd-party-services/ (last visited Apr. 13, 2020) (guidance from ACT The App Association noting that it "may be a challenging task" to find a COPPA compliant vendor).

[201] Statement of Joseph J. Simons & Christine S. Wilson, People of the State of New York v. Google LLC and YouTube, LLC (Sep. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf; Comment Submitted by Max Bleyleben, SuperAwesome, https://www.regulations.gov/document?D=FTC-2019-0054-25091 (last visited Feb. 3, 2020).

[202] Comment submitted by Max Bleyleben, SuperAwesome, https://www.regulations.gov/document?D=FTC-2019-0054-25091 (last visited Feb. 3, 2020) (SuperAwesome notes that the COPPA rule has "spur[red] investment and innovation in kidtech—infrastructure technology and services that allows operators to build privacy-enhanced digital experiences for kids").

[203] *See, e.g.*, *2019 Privacy Tech Vendor Report V.3.2*, IAPP https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf (last visited Feb. 3, 2020). Vendor-driven privacy protections are not necessarily a good thing, so it would still be useful to build in strong substantive and detailed rules. *See* Ezra Ari Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773 (2019).

[204] *See, e.g.*, Allison Schiff, *Google Will Let Companies Limit Ad Personalization To Facilitate CCPA Compliance*, (Nov. 22, 2019) https://www.adexchanger.com/privacy/google-will-let-companies-limit-ad-personalization-to-facilitate-ccpa-compliance/.

[205] Jessica Davies, *After GDPR, The New York Times Cut Off Ad Exchanges in Europe - and Kept Growing Ad Revenue*, AD EXCHANGER (Jan. 16, 2019), https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/; *see also* Veronica Marotta, Vibhanshu Abhiskek & Alessandro Acquisri, *Online Tracking and Publishers' Revenues: An Empirical Analysis,* TECHCRUNCH (May 2019);

may make more from contextual ads, those purchasing the ads see little return in revenue especially compared to the outsized costs.[206] In addition, companies have found that privacy compliance offers additional benefits.[207]

C. Kids Would Get Additional Benefits

If COPPA applied to everyone, there would be additional benefits for kids besides strictly "privacy" ones. All those who say COPPA reduces the availability of kid's content or the market for children would be silenced, as kids sites would be placed on equal footing with others.[208] It would not be beneficial to claim your site did not target children, because all sites would be required to protect privacy under COPPA's terms. Any market for creating children's content would be subject to the same rules as all other markets, and thus to any extent COPPA has suppressed content—a questionable claim—such negative externalities would disappear.[209] Consistent with broader global requirements, companies operating in the U.S. would have to stop building products that maximize data collection and rely upon behavioral ads.[210]

This move away from a behavioral ad supported model overall would further help kids, as they would not be subject to the same harms from personally targeted ads, whose persuasive intent they have trouble understanding.[211] This is all the more important given the confusing nature of advertisements online, and the growing mix of ads masquerading as news or facts in the guise of thinly-veiled sponsored stories.[212] Further, children

Natasha Lomas, *Targeted ads offer little extra value for online publishers, study suggests*, TECHCRUNCH (May 31, 2019) (cited by SuperAwesome in COPPA comments).

206 Comment Submitted by Max Bleyleben, SuperAwesome, https://www.regulations.gov/document?D=FTC-2019-0054-25091 (last visited Feb. 3, 2020) (SuperAwesome notes gains from targeted advertisements have been overstated).

207 Robert Waitman, *Companies Worldwide Recognize Business Benefits of Privacy*, IAPP (Feb. 19, 2019), https://iapp.org/news/a/companies-worldwide-recognize-business-benefits-of-privacy/? ("Most companies (97 percent) say they are receiving auxiliary benefits today from their data privacy investments beyond just meeting compliance requirements, and most companies identified multiple areas of benefit.").

208 *See, e.g.*, Presentation by Morgan Reed, *The Future of the COPPA Rule: An FTC Workshop Part 2* (Oct. 7, 2019) https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_2_1.pdf.

209 *Id.*

210 *See, e.g.*, Davies, *supra* note 205 (The GDPR has, for example, pushed companies away from behavioral ad targeting, not always at a cost to the companies' bottom line); *see also GDPR and Data Privacy Regulations Continue to Impact Audience-based Advertising*, ZVELO https://zvelo.com/gdpr-data-privacy-regulations-continue-impact-audience-based-advertising/ (Last Visited Apr. 13, 2019).

211 *See* discussion *supra* Section V.E.

212 *See, e.g.*, Rachel Abrams & Cecilia Kang, *The Mystery of Teen Vogue's Disappearing Facebook Article*, N.Y. TIMES (Jan. 8, 2020),

would benefit if they were not subject to other nudges and practices that use their personal information to subvert their autonomy and decision-making function, or that attempt to create compulsive sharing behavior online.[213] Indeed, nudges using personal information, as well as commercial profiling, could soon be prohibited in the U.K. with their age appropriate design code.[214] Children and teens would benefit if they were not subject to this type of manipulation. They should be able to make choices for themselves, without feeling pressured or tricked by technology. They should be able to grow and develop free from corporate interests whose motives and goals do not prioritize a child's best interests but are instead all too focused on the bottom line. Applying COPPA across the board in the U.S. could move the market away from such practices, even without putting in place specific prohibitions against them as in the U.K.

Indeed, if we view what children do online, both in the classroom and at home, as their work because they are required to be connected in order to learn, get a job, or apply to colleges (or because you consider data as labor),[215] it is particularly important to make sure they are protected from manipulation and overwork. We have long put in place rules for kids in the labor context, including very specific and granular detail about what practices are okay and what are not.[216] This stems from a recognition that children deserve a place to learn and develop. Just as we do not force children to work in factories for ten hours a day, we should not force children to be commercially exploited and manipulated as they attempt to obtain an education for ten hours a day. Labor laws attempt to protect childhood and prevent injury, and privacy laws could do the same, and simply extending COPPA could bring many of these benefits.

D. Adults Will Not Be "Treated Like" Children

Extending COPPA to adults would also not mean that adults are treated like children or restricted in what content they can access. First, under the envisioned expansion, adults, and teens as appropriate, could consent on

https://www.nytimes.com/2020/01/08/business/media/teen-vogue-facebook.html.

213 *See, e.g.*, U.K.'s Age Appropriate Design Code, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/ (last Visited Feb. 3, 2020) (standards 5 and 13, prohibiting detrimental uses of data and nudges that "lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.").

214 *See id.*

215 Jaron Lanier & E. Glen Weyl, *A Blueprint for a Better Digital Society*, HARV. BUS. REV. (Sep. 26, 2018).

216 Fair Labor Standards Act of 1938, 29 U.S.C. § 213(5)(A) ("In the administration and enforcement of the child labor provisions of this chapter, employees who are 16 and 17 years of age shall be permitted to load materials into, but not operate or unload materials from, scrap paper balers and paper box compactors.").

their own behalf. Second, COPPA does not actually put in place prohibitions regarding content.[217] What COPPA's extension would do is limit the amount of tracking and targeting adults face, because tracking and targeting requires personal information and personal information could not be collected as a default and without consent. In some ways, companies argue this could limit the "relevance"—to use the companies' parlance—of things visitors see.[218] But "relevant" or "personalized" is not an unqualified positive. Especially given concerns over "filter bubbles" and polarization, exposing individuals to different viewpoints could help public discourse as well as individual well-being.[219] We all deserve the opportunity to learn new points of view and be exposed to new ideas.

E. Congress Can Handle This Lift

Simply extending COPPA to teens and adults has another important benefit—the statute is already drafted, there are implementing regulations, and there is a growing body of interpretation under FTC enforcement[220] as well as actions by state Attorneys General.[221] At least some companies have

---

[217] COPPA does not put in rules about what content can be shown on a site. However, this can be a common misconception. *See, e.g.*, Harsimar Dhanoa and Jonathan Greengarden, *Misinformed YouTubers Are Undermining the Fight for Children's Privacy Online*, SLATE (Nov. 27, 2019), https://slate.com/technology/2019/11/youtube-coppa-google-ftc-settlement-children-privacy.html (noting "misinformed" YouTube creators' concerns: "Some claim that YouTube will have to ban certain types of content, such as videos about the popular game *Roblox*.")

[218] Proponents of behavioral ads have said that they are more relevant because they are more tailored to an individual. For example, Facebook tells advertisers they can add "interests" of individuals to ad parameters and "make your targeted ads more relevant." *See* Facebook for Business, https://www.facebook.com/business/ads/ad-targeting (last visited Apr. 13, 2020).

[219] Jennifer Dutcher, *Eli Pariser: Beware Online "Filter Bubbles"*, DATASCIENCE@BERKLEY BLOG (Mar. 11, 2014), https://datascience.berkeley.edu/eli-pariser-beware-online-filter-bubbles/

("Filter bubbles" is a coined termed by Eli Pariser to describe the isolated experiences individuals experience online).

[220] *See, e.g.*, United States v. Musical.ly Corp., Case No. 2:19-cv-1439, Stipulated Order (C.D. Cal. 2019), https://www.ftc.gov/system/files/documents/cases/musical.ly_proposed_order_ecf_2-27-19.pdf;

United States v. VTech Electronics Ltd., Case No. 1:18-cv-114, Stipulated Order (N.D. Ill. 2018), https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf; United States v. Lisa Frank, Inc., Civ. No. 01-1516-A (E.D. Va. 2001), https://www.ftc.gov/enforcement/cases-proceedings/012-3050/frank-lisa-inc-us.

[221] *See, e.g.*, Press Release, New York State Office of the Attorney General, A.G. Schneiderman Announces Results of "Operation Child Tracker" Ending Illegal Online Tracking of Children at Some of Nation's Most Popular Kids' Websites (Sep. 13, 2016) (available at https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online); Press Release, New Jersey Office of the Attorney General, Operator of Teen Social Website Breached by Hacker Agrees to Close Site

built in compliance structures. This seems like an attainable lift even for a Congress who has been unable to pass a comprehensive privacy law for adults, despite growing requests from consumers, businesses, and international partners,[222] as well as unable to pass substantive COPPA updates, despite children's privacy champions' tireless efforts and repeated reintroduction of bills.[223]

VIII. CONCLUSION

COPPA was passed almost a decade before any of its current under thirteen-year-olds beneficiaries were born, driven by fears of online safety and over-commercialization. Despite its age and shortcomings, the law remains relevant today. Indeed, it may be increasingly relevant given the federal government's failure to otherwise act to protect consumers' privacy. Luckily, COPPA is a flexible tool, offering key definitions (such as "personal information" and "verifiable parental consent") that are intended to change with the times and technology, under the guidance of an expert agency. This is especially critical given that young people's experiences with technology today are vastly different than they were over twenty years ago. The internet is in many ways no longer something kids actively connect into, like dialing up a modem, but rather an ever-present connection that surveils them and their devices as they move through homes, stores, and schools. Young people experience many of their most important moments online, but their brains are still playing catch up. Digital advertising and data brokers are concepts young minds do not fully understand. And yet Congress has thus far been unable to offer up new consumer privacy protections, to children, teens, or anyone else. How then to improve

& Reform Practices to Settle Allegations it Violated Children's Online Privacy Protection Act (Aug. 3, 2018) (available at https://nj.gov/oag/newsreleases18/pr20180803a.html).

[222] *See, e.g.*, Sam Sabin, *Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year*, MORNING CONSULT (Dec. 18, 2019) https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/; Press Release, U.S. Chamber of Com. U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law (Feb. 13, 2019) (available at https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law); Shiva Stella, *Civil Rights, Consumer and Privacy Organizations Unite to Release Principles for Privacy Legislation*, PUBLIC KNOWLEDGE (Nov. 13, 2018), https://www.publicknowledge.org/press-release/34-civil-rights-consumer-and-privacy-organizations-unite-to-release-principles-for-privacy-legislation/; Lauren Cerulus & Mark Scott, *Europe Seeks to Lead a New World Order on Data*, POLITICO (Jun. 7, 2019), https://www.politico.eu/article/europe-trade-data-protection-privacy/.

[223] Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Do Not Track Kids Act of 2015, H.R. 2734, 114th Cong. (2015); Do Not Track Kids Act of 2018, S. 2932, 115th Cong. (2018); COPPA 2.0, S. 748, 116th Cong. (2019); Protecting the Information of our Vulnerable Children and Youth Act, H.R. 5703, 116th Cong. (2020).

protections?

In an ideal world, legislators would offer children substantively improved protections in COPPA, inserted into an actually comprehensive federal privacy law. The U.S. lags behind a growing number of countries on this front. However, given the world we live in, a thing to do to get actual protections now would be to extend COPPA's current protections across the board. Older users, who may also have trouble understanding digital marketing and online ad ecosystems, would gain important privacy protections that they currently lack. And younger people would gain more privacy-protective defaults. An extension of COPPA could also improve the marketplace for privacy-protective offerings and ease compliance burdens. It may also offer young people additional benefits in terms of more appropriate content, and less digital manipulation. And it would be a smaller ask of Congress. While simply extending COPPA to everyone is not a perfect or hopefully final answer to the problem of children's privacy, it would still offer a plethora of benefits quickly, and with a modest cost.