Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule	

COMMENTS OF

Campaign for a Commercial-Free Childhood

The Center for Digital Democracy
Alana Institute
American Academy of Pediatrics
Badass Teachers Association
Berkeley Media Studies Group
Consumer Action
Consumer Watchdog
Defending the Early Years
Electronic Frontier Foundation
Obligation, Inc.
P.E.A.C.E. (Peace Educators Allied For Children Everywhere)
Parent Coalition for Student Privacy
Parents Across America
Parents Television Council
Public Citizen
Story of Stuff
TRUCE (Teachers Resisting Unhealthy Childhood Entertainment)
U.S. PIRG

Laura Moy, Angela Campbell, Lindsey Barrett
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535

Counsel for Campaign for a Commercial-Free Childhood and Center for Digital Democracy

December 11th, 2019

Introduction and Summary

Campaign for a Commercial-Free Childhood (CCFC), Center for Digital Democracy (CDD), Alana Institute, American Academy of Pediatrics, Badass Teachers Association, Berkeley Media Studies Group, Consumer Action, Consumer Watchdog, Defending the Early Years, the Electronic Frontier Foundation, Obligation, Inc., P.E.A.C.E. (Peace Educators Allied For Children Everywhere), Parent Coalition for Student Privacy, Parents Across America, Parents Television Council, Public Citizen, Story of Stuff, TRUCE (Teachers Resisting Unhealthy Childhood Entertainment), and U.S. PIRG appreciate that the Federal Trade Commission (FTC) has undertaken an early review of the Children's Online Privacy Protection Act Rule. We believe, however, that the Rule, as amended in 2013, is fundamentally sound. The main problem is that the FTC has not adequately enforced it.

The FTC's inadequate enforcement is illustrated by the FTC's recent action against YouTube. The FTC has long been aware that many channels on YouTube are directed to children. Under the COPPA Rule, as amended in 2013, operators of these channels are strictly liable for COPPA compliance.[1] Yet the FTC took no action until earlier this year, when it filed a complaint against YouTube for violating COPPA because it hosts numerous child-directed channels and had "actual knowledge that [these channels] collect personal information, including persistent identifiers for use in behavioral advertising, from viewers of channels and content directed to children under 13 years of age."[2]

While we agree that YouTube is liable, so too are the channel owners. Indeed, the 2013 amendments make plain that content provider are strictly liable for compliance with COPPA.[3] The large number of comments from content creators in this proceeding

[1] Statement of Basis and Purpose, 78 Fed. Reg. 3972, 3975–77 (Jan. 17, 2013) [hereinafter 2013 Statement of Basis and Purpose].
[2] Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at ¶¶28–42, 44, FTC v. Google LLC and YouTube, LLC, Case No. 1:19-cv-02642 (Sept. 6, 2019) [hereinafter YouTube Complaint].
[3] 2013 Statement of Basis and Purpose, *supra* note 1 at 3975–77.

suggests, however, that many did not realize they were responsible for complying with COPPA. Had the FTC acted sooner to enforce the COPPA Rule against YouTube and the creators of child content, these problems could have been minimized.

As we show below, noncompliance with COPPA is widespread. This is not surprising, given that in the 20 years COPPA has been in effect, the FTC has brought only 31 enforcement actions.[4] Even when the FTC does act, it takes a long time and the penalties are simply seen as the cost of doing business. Thus, the most important thing that the FTC could do to protect children's privacy is to more aggressively enforce its existing Rules. In particular, the FTC should do more to ensure that operators do not collect more information from a child than is reasonably necessary and require operators to protect the confidentiality, security, and integrity of personal information collected from children. It should also revise Rules to encourage increased enforcement by safe harbor organizations.

This is not to say that the COPPA Rule could not be improved. It is true that recent developments in technology and marketing have increased privacy risks to children. But at present, we do not believe that the FTC has sufficient information to address these new threats. For this reason, we have written a separate letter urging the FTC to use its 6(b) authority to study how children's information is being collected and used.[5] The FTC should gather and analyze this information before proposing any changes to the COPPA Rule.

Until such studies are conducted, many questions raised in the FTC's Request for Comment cannot be answered. Nonetheless, we do have some suggestions about how

---

[4] Dissenting Statement of Comm'r Rebecca Slaughter 1 n.1, FTC v. Google LLC and YouTube, LLC, Case No. 1:19-cv-02642 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542971/slaughter_google_youtube_statement.pdf [hereinafter Slaughter YouTube Dissent] [https://perma.cc/6J7X-X6AX].

[5] Campaign for a Commercial-Free Childhood et al., Comment in Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, Dkt. FTC-2019-0054 (filed Dec. 5, 2019) (on file with the Institute for Public Representation).

the COPPA Rule should or should not be amended to better protect children's privacy. In particular:

- **The FTC should not permit general audience platforms to rebut the presumption that the users of child-directed portions of their services are children.** Any portion of a general audience service that is child-directed must treat users of that portion of the site as children who are protected under COPPA. Moreover, there is no good way for platforms to reliably sort under-13 users from over-13 users on a user-by-user basis. Many children use general audience services via their parents' devices, sometimes logged in to their parents' accounts. If the FTC were to permit general audience platforms to rely on user profiles to rebut the presumption that patrons of their child-directed offerings are children, it would lead to widespread mislabeling of children as adults and large numbers of under-protected children.

- **The FTC should retain its enforcement policy statement for voice recordings.** The FTC's existing enforcement policy allows children to use voice commands with connected devices while protecting their privacy. There is no need to codify this exception.

- **The FTC should strengthen protections for student privacy.** At present neither existing COPPA guidance nor the Family Educational Rights and Privacy Act (FERPA) sufficiently protects the privacy of children in schools. The FTC should outright prohibit the commercial use of data collected from students in educational settings. The Commission should also provide more clarity for parents, school officials, and educational technology ("ed tech") vendors by clearly defining what constitute "educational" and "commercial" purposes under COPPA.

- **The FTC should tighten and more effectively define "support for the internal operations of the Web site or online service."** The COPPA Rule currently defines certain circumstances under which an operator may collect personal information from a child and incur fewer obligations under COPPA. The current definition is so broad and vague that it creates incentives for operators to claim that children's personal information—especially persistent identifiers—is used only for internal purposes even when it is not. The FTC should require operators to only retain information collected under the internal operations exception for a short period of time. The FTC should also clarify that permissible personalization of content applies only to personalization that is user-driven. Finally, the FTC should make clear that advertising attribution is not included under the definition of support for internal operations, a point acknowledged even by advertisers.[6]

- **The FTC should strengthen its policies protecting children's privacy by expanding the definition of "personal information."** The FTC should clarify that COPPA's protections extend to biometric data and to personal information that is inferred about, but not directly collected from, children.

- **The FTC should develop new COPPA Rule provisions implementing neglected sections of the statute.** COPPA has long been treated as a notice and comment framework by the FTC, but it is much more. COPPA also requires the FTC to promulgate regulations that 1) prohibit conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity and 2) require operators to protect the confidentiality, security, and integrity of personal

[6] *See generally* INTERACTIVE ADVERT. BUREAU, GUIDE TO NAVIGATING COPPA (2019), https://www.iab.com/wp-content/uploads/2019/10/IAB_2019-10-09_Navigating-COPPA-Guide.pdf [https://perma.cc/A96Q-2VCZ].

information collected from children. To better protect children's privacy, the FTC should develop Rules implementing these underutilized provisions of COPPA.

Table of Contents

I. Children's privacy threats and related harms are on the rise

Since the FTC last invited comments on COPPA seven years ago, collection and use of children's information have increased exponentially, due to the growth of services focused on children.[7] Online tracking—and the personalized content and ads that tracking facilitates—are also on the rise due to ongoing developments in data-driven marketing.[8] Meanwhile, based on recent academic research and other studies, the companies conducting such tracking of children often fail to comply with the law.

At the same time, the growth and evolution of technology in homes and schools have also increased threats to children's privacy. Voice-enabled connected devices now collect vast amounts of private information from intimate environments such as children's homes and bedrooms. Schools' widespread adoption of ed tech, many of which collect large amounts of student data, has resulted in new and significant privacy risks for children.

The existing legal and regulatory environment does not protect children, due in large part to insufficient enforcement of the COPPA statute by the FTC. Many child-directed sites and services participate in safe harbor programs, but those safe harbor programs have not been effective. In the ed tech sector, neither the FTC's existing COPPA guidance nor FERPA sufficiently protects children's privacy in schools.

A. Over the last seven years, collection and use of children's information have intensified

Since the FTC last invited comments on COPPA seven years ago, collection and use of children's information have intensified due to several factors.

First, the amount of time that young children spend online using apps and websites that collect their personal information has increased dramatically over the past

[7] *See* Elizabeth Foster, *Smart Toys Expected to Grow Through 2022*, KIDSCREEN (Nov. 13, 2019), http://kidscreen.com/2019/11/13/smart-toys-expected-to-spark-growth-through-2022/?utm_source=newsletter&utm_medium=email&utm_campaign=smart-toys-expected-to-spark-growth-through-2022&_u=L%2bdJqA4GMeY%3d [https://perma.cc/V37K-TCG3].
[8] *See generally* WARC, *What We Know About Personalisation, in* WARC BEST PRACTICES, JANUARY 2019 (2019).

several years. Technology that creates and collects data about children and teenagers has become inextricable from life as a young person in 2019. Roughly 97% of children and teens live in a house with a computer or smartphone, and between 2010 and 2015, the percentage of children who live in a household with a tablet or smartphone increased from 25% to 89%.[9] Nearly one in five 8-year-olds now has a smartphone of their own,[10] as do 69% of twelve-year-olds– a significant increase from just 4 years ago.[11] The amount of time children spent watching online videos has also risen considerably. The percentage of 8- to 12-year-olds who said they watch online videos "every day" jumped from 24% four years ago to 56% now, and children who watch report taking in an average of 56 minutes per day—more than double the 25 minutes that children reported watching four years ago.[12]

When the COPPA Rule was strengthened seven years ago, some industry commenters argued the changes would impede the growth of children's online sites and services. They were wrong. By any measure, digital offerings for children have continued to proliferate. Amazon's app store has been estimated to offer 17,190 apps for children.[13] Similar public estimates are not available for the Google and Apple app stores, but in light of these two companies' dominance of the app market, it is likely their children's offerings far exceed Amazon's. A 2018 study of the "most popular" children's apps in the Google Play Store found that the top 5,855 children's apps had a

---

[9] *See Percentage of Children Ages 3 to 18 Living in Households with a Computer, By Type of Computer and Selected Child and Family Characteristics: Selected Years, 2010 Through 2017*, NAT'L CTR. FOR EDUC. STAT. (Jan. 2019), https://nces.ed.gov/programs/digest/d18/tables/dt18_702.10.asp?current=yes [https://perma.cc/52G6-H36K]; *Student Access to Digital Learning Resources Outside of the Classroom-Indicator 1L Prevalence of Computer Access at Home,* NAT'L CTR. FOR EDUC. STAT. (Apr. 2018), https://nces.ed.gov/pubs2017/2017098/ind_01.asp#fig_1_1 [https://perma.cc/VJ5U-8TMZ]

[10] VICTORIA RIDEOUT & MICHAEL ROBB, COMMON SENSE MEDIA, THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS, 2019 at 7 (2019), https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-census-8-to-18-key-findings-updated.pdf [https://perma.cc/D7JE-8RKP].

[11] *Id.*

[12] *Id.* at 5.

[13] Appfigures, *Number of Available Children's Apps at Amazon Appstore from 1st Quarter 2015 to 3rd Quarter 2019*, STATISTA, https://www.statista.com/statistics/804809/number-of-available-childrens-apps-in-the-amazon-appstore-quarter/ [https://perma.cc/LF2K-K96U].

combined 4.8 billion downloads, and were created by 1,889 unique developers.[14] It does not appear that the 2013 changes have created a significant barrier to creating apps for children.

The last seven years have also seen growth in child-directed offerings distributed by large platforms, as well as new and expanded streaming services and gaming applications. These platforms that do not appeal exclusively to children have had strong profit-driven incentives to launch products and services directed to kids. For example, companies like YouTube have sought out content creators that cater to children (all while steadfastly denying the presence of children on their services).[15] Indeed, a recent Pew study found that videos directed to children on YouTube's general audience site received more views than any other video category.[16]

The past seven years have also seen new privacy challenges to children and their parents, due to the complex array of services, devices and machine-driven data applications. Even when they are not on computers, tablets, or smartphones, many children play with smart toys that record their voice or location.[17] Apps and sensor-embedded objects are sold for parents to monitor their children's development and growth from the earliest stages, in the form of wearables and other connected devices.[18]

---

[14] Irwin Reyes et al., *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, 2018 PROC. PRIVACY ENHANCING TECHS. 63 (2018), https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf [https://perma.cc/PZ2C-4GEH].

[15] YouTube Complaint, *supra* note 2 at ¶28.

[16] Patrick Van Kessel et al., *A Week in the Life of Popular YouTube Channels*, PEW RES. CENTER (July 25, 2019), https://www.pewinternet.org/2019/07/25/a-week-in-the-life-of-popular-youtube-channels [https://perma.cc/RE9C-3HZ2]; s*ee also PwC Kids Digital Media Report 2019 Estimates Global Kids Digital Advertising Market Will Be Worth $1.7bn by 2021,* SUPERAWESOME (June 11, 2019), https://www.superawesome.com/2019/06/11/pwc-kids-digital-media-report-2019-estimates-global-kids-digital-advertising-market-will-be-worth-1-7bn-by-2021/ (noting YouTube as one of the "biggest winners of kids digital ad spend expansion. . . .") [https://perma.cc/F4DS-88NM].

[17] The prevalence of sensors, microphones, cameras, data storage, and other multimedia capabilities, such as speech recognition and GPS options, in children's toys has led the Federal Bureau of Investigation to warn consumers about the privacy and safety risks these features may pose. *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*, FED. BUREAU OF INVESTIGATION (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx [https://perma.cc/947X-6R5M].

[18] *See, e.g.*, Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 New Media & Soc'y 780, 783 (2017), https://journals.sagepub.com/doi/pdf/10.1177/1461444816686328 [https://perma.cc/2QJ6-65PM];

B. Voice-enabled connected devices pose a growing risk to children's privacy

Not only has tracking and profiling of children through websites and apps increased, but children today also use their voices to interact with more devices than ever before, and this trend is only likely to continue. These technologies, which listen to and record children's voices, offer companies unprecedented access to children. Often these interactions take place in a child's home, where children may share intimate details about their lives without understanding the implications of sharing this information.[19]

As handheld devices have become more common, the prevalence of digital voice assistants has similarly increased. Phones and tablets are often sold equipped with an assistant such as Apple's Siri, Google Assistant, Microsoft's Cortana, and Samsung's Bixby. Children also increasingly use voice commands while playing videogames or watching TV.[20]

Children are also increasingly engaging with voice-enabled smart speakers. Last year alone, there were nearly two smart speakers for every child under 14 in the United States.[21] Today, nearly one in three homes own a smart speaker, up from 8% three years ago.[22] Approximately three-quarters of smart speaker owners report that their children

---

Kidizoom Smartwatch DX2, VTECH, https://www.vtechkids.com/product/detail/18025/KidiZoom_Smartwatch_DX2_Blue [https://perma.cc/LF8B-4VS8].

[19] *See* Kate Raynes-Goldie, *Is That New Doll Spying on Your Kids?*, PHYS.ORG (Oct. 23, 2018), https://phys.org/news/2018-10-doll-spying-kids.html [https://perma.cc/RSZ5-2AZQ]

[20] *See, e.g., Samsung Smart TV,* SAMSUNG, https://www.samsung.com/us/explore/smart-tv/highlights/ [https://perma.cc/6MM7-Q39D]; *What Can I Say Using Digital Assistants on Xbox One?*, XBOX SUPPORT, https://support.xbox.com/en-US/xbox-one/voice-and-digital-assistants/what-can-i-say-using-digital-assistants [https://perma.cc/9AYG-J97W].

[21] *See* NATIONAL PUBLIC MEDIA, THE SMART AUDIO REPORT (WINTER 2018) 5 (2019), https://www.nationalpublicmedia.com/wp-content/uploads/2019/01/Smart-Audio-Report-Winter-2018.pdf (118.5 million smart speakers) [https://perma.cc/H7Y4-M5ZJ]; *Child Population by Age Group in the United States,* KIDS COUNT DATA CTR., https://datacenter.kidscount.org/data/tables/101-child-population-by-age-group#detailed/1/any/false/37/62,63,64/419 (60.9 million children under 14) [https://perma.cc/ZDV3-HRV2].

[22] Press Release, Danielle Cassagnol, Consumer Tech. Ass'n, Smart Speakers See Largest Gain in U.S. Household Ownership, Says CTA Study (May 9, 2019), https://www.cta.tech/News/Press-Releases/2019/May/Americans-Adopt-AI-Smart-Speakers-See-Largest-Gai.aspx [https://perma.cc/PW4E-264K].

are using these devices.[23] Almost half of parents with smart speakers report that their children use them to play music and 43% say their 6- to 8-year-olds use the devices for homework help.[24] Over half of smart speakers are placed in a common room or living room where children can access them.[25]

Some smart speakers are even marketed specifically for use by children. Since 2018, Amazon has offered the Echo Dot Kids Edition: a regular Echo Dot bundled with access to skills specifically designed for children. Google similarly offers a suite of child-directed content and allows parents to program the voice assistant to recognize their child's voice.

Increasingly, toys come equipped with the technology needed to listen and interact with children. The industry is still relatively young, but the market for smart toys is expected to grow to $18 billion by 2023.[26] Examples of connected toys include Woobo, a "fuzzy robot version of an imaginary friend that every child dreams of. Woobo can answer questions, express feelings, sing songs, and play games."[27] Vector is a toy robot has built-in Amazon Alexa functionality, plus a camera, a touch sensor, and "an Infrared laser scanner that lets him listen and respond to you and maneuver his

[23] NATIONAL PUBLIC MEDIA, THE SMART AUDIO REPORT (SPRING 2018) 38 (2018), https://www.nationalpublicmedia.com/wp-content/uploads/2018/07/Smart-Audio-Report-from-NPR-and-Edison-Research-Spring-2018_Downloadable-PDF.pdf [https://perma.cc/7CXH-XA5A].
[24] Press Release, Common Sense Media, Common Sense/SurveyMonkey Poll Reveals Privacy Is a Top Concern for Families Who Use Smart Speakers and Voice-Activated Assistants (Mar. 28, 2019), https://www.commonsensemedia.org/about-us/news/press-releases/common-sensesurveymonkey-poll-reveals-privacy-is-a-top-concern-for [https://perma.cc/9C9J-GAUQ].
[25] NATIONAL PUBLIC MEDIA, THE SMART AUDIO REPORT (SPRING/SUMMER 2017) 6 (2017), https://www.nationalpublicmedia.com/wp-content/uploads/2017/10/The-Smart-Audio-Report-from-NPR-and-Edison-Research.pdf [https://perma.cc/M3X8-ZA9N].
[26] Press Release, Juniper Research, Smart Toy Revenues to Grow by Almost 200% from 2018 to $18 Billion by 2023 (May 8, 2018), https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-grow-almost-200pc-by-2023 [https://perma.cc/2YC4-5ECN].
[27] WOOBO, https://www.woobo.io/ [https://perma.cc/XJA6-KZP3].

way through your house while avoiding obstacles."[28] Vector also has the capacity to recognize faces.[29]

Because children often engage in imaginary play with toys and confide in dolls and stuffed animals, interconnected toys may record large amounts of sensitive personal information.[30] Even more than many other types of data, these recordings risk turning children's natural curiosity into data-rich portraits of their hopes, fears, and preferences replete with intimate details about their lives. The expansive growth of always-on devices and IoT offerings for children must be met with additional protections to preserve children's privacy in the home and beyond. Yet concerningly, security on these devices is often lacking.[31]

C. Ed tech is ubiquitous in schools and poses significant risks to children's privacy

The rapid rise and widespread adoption of ed tech have transformed schools. This new ed tech market, which is served by hundreds, if not thousands, of providers, facilitates the tracking and quantification of children on an unprecedented scale. Many collect large amounts of student data, resulting in significant privacy risks for children.

---

[28] Timothy Taylor, *Amazon Slashes $50 Off the Adorable Vector Toy Robot with Built-In Alexa*, DIGITAL TRENDS (Aug. 1, 2019, 10:44 AM), https://www.digitaltrends.com/dtdeals/vector-toy-robot-amazon-deal/[https://perma.cc/NJA3-8VBE].

[29] *Privacy Policy*, ANKI (Oct. 5, 2018), https://anki.com/en-us/company/privacy.html ("Both Vector and Cozmo (with the Cozmo App) can translate faces they see into encoded facial features, a set of numbers not recognizable by a person ('Facial Features Data').") [https://perma.cc/6V7C-2FXP].

[30] *See generally* Emily McReynolds et al., *Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys*, *in* PROCEEDINGS OF THE 2017 CONFERENCE ON HUMAN FACTORS COMPUTING SYSTEMS 5197 (2017), https://techpolicylab.uw.edu/wp-content/uploads/2017/10/Toys-That-Listen_CHI-2017.pdf (describing the privacy risks of toys that listen, like CogniToys Dino and SmartToy Monkey, for children) [https://perma.cc/2FL6-NS6K].

[31] *See generally* Gordon Chu et al., *Security and Privacy Analyses of Internet of Things Toys*, 6 IEEE INTERNET OF THINGS J. 978 (2019), https://arxiv.org/pdf/1805.02751v1.pdf [https://perma.cc/ZKH6-TKVZ]. The "smart pet" the paper tested is a Cloudpet, which Amazon and other retailers subsequently pulled due to its security vulnerabilities. Alfred Ng, *Amazon Will Stop Selling Connected Toy Filled with Security Issues*, CNET (June 5, 2018, 9:59 AM), https://www.cnet.com/google-amp/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/[https://perma.cc/XSB8-5N49]; Nick Feamster (@Feamster), TWITTER (June 5, 2018, 4:13 PM), https://twitter.com/feamster/status/1004093897268703236 [https://perma.cc/4TGS-NHKC].

This leads to privacy threats, many of which are not well understood by schools, parents, and children ill-equipped to consider and protect against these threats.

Products referred to broadly as "ed tech" are ubiquitous. Students today use interactive games, apps, animations, computer-based assessments, and adaptive software to assist in the learning process in the classroom, all of which rely on varying forms of data collection.[32] Schools also adopt apps and other digital tools for administrative functions and to facilitate communications with families regarding in-school performance, coordination of extracurricular activities, and more. Some teachers even use apps to track children's behavior in school.[33] In the 2018–2019 school year, each U.S. school district used an average of 703 different ed tech products every month, a 28% increase from the 2017-2018 school year.[34] In 2017, 63% of K-12 teachers reported using technology in the classroom daily, and 58% reported that they use educational apps.[35] In 2018, the number of teachers using tablets or laptops daily in the classroom reached 73%.[36]

The technology used in the educational system facilitates the quantification, analysis, and tracking of children on a scale and with an ease that has never previously

---

[32] *See* NAT'L SCI. BOARD, *Instructional Technology and Digital Learning*, in SCIENCE AND ENGINEERING INDICATORS 2018, at 86 (2018), https://nsf.gov/statistics/2018/nsb20181/assets/nsb20181.pdf [https://perma.cc/PBX9-WVBT]

[33] *See* Heather Kelly, *School Apps Track Students from Classroom to Bathroom, and Parents Are Struggling to Keep Up*, WASH. POST (Oct. 29, 2019), https://www.washingtonpost.com/technology/2019/10/29/school-apps-track-students-classroom-bathroom-parents-are-struggling-keep-up/ [https://perma.cc/UD8D-SSKQ];
Natasha Singer, *Privacy Concerns for ClassDojo and Other Tracking Apps for Schoolchildren*, N.Y. TIMES (Nov. 16, 2014), https://www.nytimes.com/2014/11/17/technology/privacy-concerns-for-classdojo-and-other-tracking-apps-for-schoolchildren.html [https://perma.cc/9PCC-9RL2].

[34] *New Research Reveals These are the 40 Most Accessed EdTech Tools in America*, LEARNPLATFORM (June 18, 2019), https://learnplatform.com/blog/edtech-management/new-research-shows-these-are-the-40-most-popular-edtech-tools-in-america-ANlnc (based on research conducted across 1,000 schools in the U.S., covering more than one million teachers and students) [https://perma.cc/ZP4W-B5G2].

[35] Meghan Bogardus Cortez, *Classroom Tech Use Is on the Rise [#Infographic]*, EDTECH MAG. (Sept. 6, 2017), https://edtechmagazine.com/k12/article/2017/09/classroom-tech-use-rise-infographic [https://perma.cc/M6EU-JG2Q].

[36] David Nagel, *Study: Most Teaching and Learning Uses Technology Nowadays*, J. (July 10, 2018), https://thejournal.com/articles/2018/07/10/study-most-teaching-and-learning-uses-technology-nowadays.aspx?m=1 [https://perma.cc/M6F3-5QHJ].

been possible.[37] Some products, like Google's G Suite for Education, serve as a sort of digital file cabinet—G Suite had over 70 million student and teacher users worldwide in 2017 and is a popular resource among teachers to post homework assignments, answer questions for students outside of class, and provide feedback on assignments.[38] Other products assist teachers in pedagogical activities like quiz apps, math games, and the like; others support school logistical functions rather than serving a specifically pedagogical purpose, such as scheduling apps.[39]

This ubiquity of ed tech has led to serious privacy threats for students whose data is being tracked, sold to third parties, and then used in opaque ways they and their parents don't understand and can't control. Almost every aspect of a student's life can be recorded, quantified, and analyzed, from their health, to fitness, cognitive profile, learning abilities or disabilities, sleeping habits, sexual activity, prescription drug use, and disciplinary matters.[40] For example, when a student goes to the cafeteria for lunch, she may use her ID that contains her name or allergies.[41] The software may also link to the family's financial information and track what the student eats and drinks, as well as any other purchases she makes while at school.[42] That same student may be asked to wear a heart-rate monitor or Fitbit-style wrist band in gym class to record how hard she is working out, as a part of her grade for the class.[43] If the student gets in trouble, the school principal may use discipline software that automates discipline consequences

---

[37] *See* Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 15, 2014, 5:05 AM), https://www.politico.com/story/2014/05/data-mining-your-children-106676?o=1 [https://perma.cc/WRN4-X6VM].

[38] Frederic Lardinois, *Google Says Its G Suite for Education Now Has 70M Users*, TECHCRUNCH (Jan. 24, 2017, 10:00 AM), https://techcrunch.com/2017/01/24/google-says-its-g-suite-for-education-now-has-70m-users/ [https://perma.cc/WRN4-X6VM].

[39] *See, e.g.*, CONEXED, https://www.conexed.com/ [https://perma.cc/8NE9-T62E]; PLANBOOK, https://www.planbook.com/ [https://perma.cc/GJD2-ATC4].

[40] *See* Khaliah Barnes, *Student Data Collection Is Out of Control*, N.Y. TIMES (Dec. 19, 2014, 12:33 PM), https://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data-collection-is-out-of-control [https://perma.cc/HS9A-ERK5].

[41] Adriene Hill, *A Day in the Life of a Data Mined Kid*, MARKETPLACE (Sept. 15, 2014), https://www.marketplace.org/2014/09/15/day-life-data-mined-kid/ [https://perma.cc/4LRL-HHVY].

[42] *Id.*

[43] *Id.*

and records it.[44] ClassDojo, for example, allows teachers to set categories of behavior worthy of commendation and punishment—"bad" behavior results in the subtraction of points, while "good" behavior adds them.[45] As the company describes it, "teachers give feedback to students for any skill, like 'Working hard' and 'Being curious.'"[46]

In many cases, parents and students are not even aware of what data is being collected, why it is being collected, who is collecting it, or where it is being stored. This data is often used to build behavioral profiles that allow third parties to create more effective marketing campaigns, targeted advertisements, and, ultimately, psychological manipulation of other children.[47] Without more rigorous limits on data collection and data retention by ed tech providers, and stricter requirements for verifiable parental consent, students remain monetizable fonts of data for ed tech companies.

II. As threats to children's privacy are on the rise, children are insufficiently protected

As children's privacy threats and related harms are on the rise, the existing legal and regulatory framework has proved insufficient. One major problem is that even though violations are widespread, the FTC does not enforce COPPA enough. The COPPA safe harbor system has not proven effective. In schools, neither FERPA nor the existing COPPA Rule adequately protects children.

A. COPPA violations are widespread and the law is not well enforced

A major reason that children's privacy is insufficiently protected is because COPPA is not well enforced. Noncompliance with COPPA is widespread, yet the FTC

---

[44] *Id.*

[45] *See* Singer, *supra* note 33.

[46] CLASSDOJO, HOW DOES CLASSDOJO BUILD A POSITIVE SCHOOL COMMUNITY? 1, https://static.classdojo.com/docs/TeacherResources/SchoolLeaderPack/ClassDojo-SchoolLeaderPack.pdf [https://perma.cc/53DS-TN4P].

[47] *See, e.g.*, David Derigiotis, Comment in Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, Dkt. FTC-2019-0054 (filed July 25, 2019), https://www.regulations.gov/document?D=FTC-2019-0054-0002 [https://perma.cc/2R2U-VBF7].

has brought only 31 enforcement actions in the 20 years that COPPA has been in effect.[48]

Several studies have found widespread noncompliance with COPPA. For example, a study conducted at Oxford University found that most apps on the US and UK Google Play Store contained a variety of tracking, but that child-directed apps contained the most third-party trackers of any category.[49] Another study by computer scientists at UC Berkeley examined 5,855 of the most popular free children's apps in the Google Play store.[50] It found that a majority were potentially in violation of COPPA, mainly due to their incorporation of third-party software development kits (SDKs). The researchers also noted that while many of these SDKs offer configuration options to respect COPPA by disabling tracking and behavioral advertising, the majority of apps examined either did not make use of these options or incorrectly propagated them across mediation SDKs.[51] Nearly one-fifth of children's apps examined by the UC Berkeley team were found to collect identifiers or other personally identifiable information via SDKs whose terms of service outright prohibited their use in child-directed apps.[52]

Other studies have found widespread security weaknesses in internet connected toys and gadgets used by children, likely in violation of COPPA and of public-facing commitments to protect security. For example, computer scientists at Princeton conducted case studies of three commercially available products targeted to children: a hydration tracker, a smart pet, and a fitness band.[53] The researchers discovered several

---

[48] Slaughter YouTube Dissent, *supra* note 4.

[49] Reuben Binns, et al., *Third Party Tracking in the Mobile Ecosystem, in* PROCEEDINGS OF THE 10TH ACM CONFERENCE ON WEB SCIENCE 6 (2018), https://arxiv.org/pdf/1804.03603.pdf [https://perma.cc/NQS8-JQKU].

[50] Irwin Reyes et al., *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, 2018 PROC. PRIVACY ENHANCING TECHS. 63 (2018), https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf [https://perma.cc/PZ2C-4GEH].

[51] *Id.* at 71-2.

[52] *Id.* at 63.

[53] Gordon Chu et al., *supra* note 31 at 979–83. The researchers found that the hydration tracker, which consisted of a water bottle along with a mobile app running on a smart phone, communicated with 12 remote hosts and requested, among other things, user profile pictures that were unencrypted and

publicly undisclosed vulnerabilities such as a lack of data encryption, lack of authentication, sensitive user information in crash reports, and secret keys in source code. They concluded that the "[l]ack of industry-standard security practices, especially encryption/authentication of communications with first-party cloud services, leaves personal data unprotected and constitutes violations of manufacturer privacy policies and federal COPPA regulation" and that the "use of common third-party analytics services across smart toys could allow cross-device tracking of child behavior." [54]

Commenters have a lot of experience reviewing children's privacy policies, and have found that many fail to meet COPPA requirements. For example, the COPPA Rule requires that children's privacy policies contain specific information; be clearly and understandably written and complete; and contain no unrelated, confusing, or contradictory material. Yet privacy policies for children's online services rarely meet even that modest bar. The privacy policies frequently contain conflicting information that would make it difficult for a reader to understand whether personal information was in fact being collected, and if so, what type of information, and to whom it was being disclosed.[55] They are hard to locate, and written at a complex reading level that

---

unauthenticated. *Id*. at 980–81. The smart pet, a plush toy in which a smart phone equipped with an app is inserted, had numerous vulnerabilities involving constant storage, encryption, and authentication. *Id.* at 982. The fitness tracker wristband communicated with third party analytic platforms such as Yahoo's Flurry Analytics, Google Analytics and Unity 3D statistics. *Id*. at 983. In fact, all three smart toys communicated with a set of third-party analytics and performance monitoring platforms, suggesting that "a small set of platforms have high visibility into a broad set of smart toys. Coupled with over-reporting of personally-identifiable information to analytics services, . . . these platforms could be receiving and storing more sensitive data than users expect." *Id.*; *see also* Daniel Cooper, *Researchers Find Another Smart Toy That's Easy to Hack*, ENGADGET (Dec. 8, 2017), https://www.engadget.com/2017/12/08/tekstatoucan-can-listen-to-kids-researchers-security/ [https://perma.cc/E4UZ-3WMD]; Lorenzo Franceschi-Bicchierai, *Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings*, MOTHERBOARD (Feb. 28, 2017), https://www.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings [https://perma.cc/N7QE-JFL9]; Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children*, GUARDIAN (Nov. 26, 2015), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children [https://perma.cc/53G8-LEUM].

[54] Gordon Chu et al., *supra* note 31 at 978–79.

[55] *See, e.g.*, *Privacy Policy*, FUNBRAIN, https://www.funbrain.com/privacy-policy, [https://perma.cc/47FX-5TQH]; Modified Cars Privacy Policy, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.helloworld.arabamodifiye&hl=en_US [https://perma.cc/3J44-EUKN].

makes them difficult to understand.[56] On top of all the barriers parents already face in attempting to protect their children's privacy, the companies are frequently failing to provide them with the most basic information about their children's data in a clear and accessible way, as COPPA requires them to do.

One reason for widespread noncompliance with COPPA is that the risk of violations being caught is miniscule and the FTC is seen as weak, unresponsive to public complaints, and slow to act. Many requests for investigation into COPPA violations have been filed with the FTC without any public response from the agency. CCFC and CDD, represented by IPR, alone have filed 15 requests for investigation of COPPA violations. Commenters are aware of other complaints filed by groups like the Electronic Privacy Information Center, Electronic Frontier Foundation, and the Children's Advertising Review Unit (CARU). Yet except for CCFC and CDD's complaint against YouTube and CARU's complaint about Musical.ly, Commenters are not aware of any public complaints that resulted in FTC enforcement actions.

Even in the rare instances when the FTC takes an enforcement action, it often has been slow to act. When the FTC does not act swiftly to curb COPPA violations, those violations may proliferate and become entrenched, presenting greater threats to children's privacy. Slow enforcement also makes it more difficult and costly to address violations later on. The Commission was told for many years that YouTube was violating COPPA, and yet it failed to act until just recently. As a result, this docket is being flooded with comments from YouTube content creators objecting to the changes the platform is adopting to attempt to comply with COPPA. But a large part of the problem YouTube creators are facing is that YouTube flagrantly violated COPPA—a

[56] IPR used The Gunning Fog index, which measures the number of years of formal education that a person would likely be required to have in order to easily understand a text on the first reading, to examine the readability of a few privacy policies for popular children's online services, and on the site's general privacy policy when there was no child-specific policy. The average score for the apps *Monster Trucks Game for Kids 2*, *Modified Cars*, and *Thomas & Friends: Race On!*, and the websites *Funbrain*, *Stardoll*, and *Neopets* was 14.77, meaning that a person would need almost 15 years of formal education to comfortably read the policies.

law older than the platform itself—for years, and the platform is only just being compelled by the Commission to come into compliance.

In its limited enforcement actions, the FTC has to date always negotiated a settlement with the violator. Typically, these consent decrees merely direct the party to comply with COPPA, and even if they do contain additional injunctive relief, it is only binding on the parties to the decree.

In all but one settlement, the FTC has also imposed civil penalties, but these fines, which have ranged from a low of $10,000 to a high of $170 million in its recent settlement with Google and YouTube, have been woefully insufficient. [57] For example, the $170 million civil penalty against Google is far less than the agency could have imposed.[58] Moreover, given Google's revenues, the extensiveness of its violations, and the substantial profits gained from these violations, this penalty has been seen by many as an inadequate deterrent.[59]

---

[57] *See* Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations [https://perma.cc/8Y6C-8QBJ]; Press Release, Fed. Trade Comm'n, Popcorn Company Settles FTC Privacy Violation Charges (Feb. 14, 2002), https://www.ftc.gov/news-events/press-releases/2002/02/popcorn-company-settles-ftc-privacy-violation-charges [https://perma.cc/3FZE-ZBLN].

[58] As CCFC and CDD explained in their Request for Investigation of YouTube, the FTC could have fined YouTube tens of billions of dollars. Inst. for Pub. Representation, Request for Investigation, *In re* Google's YouTube Online Service and Advertising Practices for Violating COPPA, at 26 (Apr. 9, 2018) [hereinafter IPR's Request to Investigate YouTube]. The FTC has authority to assess up to $41,484 per COPPA violation. *See* 16 C.F.R. § 312.9 (2019); 5 C.F.R. § 1.98 (2019). CCFC and CDD urged the FTC to impose the maximum penalties because Google's violations were particularly egregious, it had actual knowledge of both the large number of child-directed channels on YouTube, Google collected personal information from nearly 25 million children in the U.S over a period of years, made a vast amount of money using children's personal information as to target advertising through the Google ad network and by taking 45% of the advertising revenues from the child-directed YouTube channels, and because Google is the second wealthiest company in the world, with a net worth totaling $101.8 billion. IPR's Request to Investigate YouTube at 26–27.

[59] Press Release, Susan Grant, Dir. of Consumer Prot. and Privacy, Consumer Fed'n of Am., The FTC's Google/YouTube Settlement Lacks Teeth to Deter Continued Children's Privacy Violations (Sept. 4, 2019), https://consumerfed.org/press_release/the-ftcs-google-youtube-settlement-lacks-teeth-to-deter-continued-childrens-privacy-violations/ [https://perma.cc/TZ4H-AQF6]; Brian Barrett, Fines Alone Aren't Enough to Slow Down Big Tech, WIRED (Sept. 4, 2019, 2:51 PM), https://www.wired.com/story/youtube-ftc-fines-alone-arent-enough/ ("For YouTube's parent company, Alphabet, [$170 million] works out to roughly two days' worth of profit. That's not a slap on the wrist; it's a gentle tap. With a feather. In zero gravity.") [https://perma.cc/SCT3-VBAQ]; Peter Kafka, *The US Government Isn't Ready to Regulate the Internet. Today's Google Fine Shows Why*, VOX: RECODE (Sept.

Other seemingly large COPPA fines are unlikely to act as a deterrent for the large and wealthy companies. For example, the $5.7 million civil penalty against Musical.ly[60] is modest in comparison to the valuation of Musical.ly's parent company Bytedance, at $75 billion.[61] Similarly, a $3 million civil penalty against Playdom likely had no effect on the parent company the Walt Disney Corporation.[62] Such penalties may be seen as simply the costs of doing business, and thus do not provide sufficient incentives for COPPA compliance.

The FTC's recent consent decree with Google and YouTube also illustrates shortcomings of the FTC's enforcement of COPPA. For example, by setting the compliance date four months after entry of the order, the FTC allowed YouTube to continue its unlawful collection and use of children's information for a significant amount of time.[63] Nor does the consent decree require YouTube to delete children's personal information that it has been unlawfully collecting for over five years. Moreover, Google and YouTube may continue to disclose, use, and benefit from the personal information collected from children for an additional 90 days after the compliance date.[64]

The reporting requirements in the Google YouTube consent decree are also inadequate. The consent order only requires the submission of a single Compliance

---

4, 2019), https://www.vox.com/recode/2019/9/4/20849143/youtube-google-ftc-kids-settlement-170-million-coppa-privacy-regulation [https://perma.cc/68HH-LX3T].

[60] 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), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc [https://perma.cc/F5BC-BDU7].

[61] *Bytedance Is Said to Secure Funding at Record $75 Billion Value*, BLOOMBERG NEWS (Oct. 26, 2018), https://www.bloomberg.com/news/articles/2018-10-26/bytedance-is-said-to-secure-funding-at-record-75-billion-value [https://perma.cc/BYW5-4DEB].

[62] *See* Press Release, Fed. Trade Comm'n, Operators of Online "Virtual Worlds" to Pay $3 Million to Settle FTC Charges That They Illegally Collected and Disclosed Children's Personal Information (May 12, 2011), https://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-million-settle-ftc-charges [https://perma.cc/5MFA-UN6Y]. In 2019, Disney was ranked as having the 8th most valuable brand in the world, with a brand value of 52.2 billion. *The World's Most Valuable Brands List*, FORBES, https://www.forbes.com/powerful-brands/list/#tab:rank [https://perma.cc/M4XM-E2UC].

[63] The compliance date is January 10, 2019, four months after the entry of the order. *See* Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 4, FTC v. Google LLC and YouTube, LLC, Case No. 1:19-cv-02642 (Sept. 10, 2019).

[64] *Id.* at 12.

Report to the FTC.[65] It does not mandate the participation of any outside, independent auditors. And it does not hold any of Google's or YouTube's senior executives personally liable for the extensive COPPA violations.[66]

Finally, the FTC took no enforcement action against the many child-directed channels on YouTube, including those run by sophisticated and highly profitable companies. The FTC's complaint alleged that YouTube hosts numerous channels directed to children under the COPPA Rule, including Mattel, Cartoon Network, Hasbro and EvanTubeHD.[67] It further alleged that Google and YouTube violated COPPA because they had "actual knowledge that they collect personal information, including persistent identifiers for use in behavioral advertising, from viewers of channels and content directed to children under 13 years of age."[68] Implicit in this allegation is that all the child-directed channels on YouTube were also violating COPPA; under the COPPA Rule, child-directed content sites are strictly liable for COPPA compliance.[69] Yet even though child-directed YouTube channels are strictly liable for the data collection from children without parental notice and consent, the FTC has not taken enforcement actions against these channels.

B. The COPPA safe harbor system is not effective

Not only has FTC enforcement of COPPA been insufficient, but the FTC cannot rely on the COPPA safe harbor system to fill the gap. The FTC asks in its most recent

---

[65] *Id.* at 15–17.
[66] *See* Dissenting Statement of Comm'r Rohit Chopra, FTC v. Google LLC and YouTube, LLC, Case No. 1:19-cv-02642 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf [https://perma.cc/5U6J-SNEM]; Dissenting Statement of Comm'r Rebecca Slaughter, FTC v. Google LLC and YouTube, LLC, Case No. 1:19-cv-02642 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542971/slaughter_google_youtube_statement.pdf [https://perma.cc/SQ55-NVU5].
[67] YouTube Complaint, *supra* note 2 at ¶28.
[68] *Id.* at ¶44.
[69] Statement of Basis and Purpose, *supra* note 1 at 3975.

Request for Comment whether the safe harbor process has been effective in enhancing compliance with the COPPA Rule.[70]

During the last COPPA Rule review, the FTC strengthened its oversight of safe harbor programs requiring them to conduct a comprehensive review of each member at least once each year, and to provide the aggregate results of these comprehensive review in an annual report to the FTC.[71] The FTC now has six years of annual reports for the seven approved safe harbor programs. These reports include information necessary to assess the effectiveness of these programs, such as the number of members, number of complaints received, the number of disciplinary actions for non-compliance, the number of members suspended, as well as descriptions of any compliance issues found and disciplinary actions undertaken. Unfortunately, the FTC has refused to make most of this information public,[72] or even to summarize the contents of these reports, thus making it difficult for Commenters to fully assess effectiveness. The evidence that is available suggests, however, that safe harbor programs are not effectively protecting children's privacy.

First, it appears that very few companies that offer child-directed websites, apps or other online service, participate in a safe harbor program. Safe harbor programs typically do not make their member lists public, so it is impossible to determine how many companies are members. At the FTC's COPPA workshop on October 7, however, CARU's Dona Fraser stated that the total was likely less than 10%.[73]

---

[70] Request for Public Comment on the FTC's Implementation of the COPPA Rule, 84 Fed. Reg. 35,842, 35,847 (July 25, 2019) (to be codified at 16 C.F.R. Pt. 312) [hereinafter 2019 COPPA RFC].
[71] *Id*. at 3996; *see also* 16 C.F.R. § 312.11(b)–(d) (2019).
[72] CDD and CCFC have requested copies of all safe harbor annual reports for the years 2014 through 2018. *See, e.g.*, FOIA Request Letter from Ctr. for Dig. Democracy, Campaign for a Commercial-Free Childhood & Inst. for Pub. Representation, to the Federal Trade Commission (Apr. 15, 2019) (on file with the Institute for Public Representation). The FTC released redacted documents for 2014 and 2015, but has not responded to the request filed on April 15, 2019, for the subsequent years.
[73] Dona Fraser, Vice President, Children's Advertising Review Unit, Remarks 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_1_1.pdf (transcript) ("The problem is that between the seven safe harbors you have in the United States, we may represent probably less than 10% of the entire market.") [https://perma.cc/HXD7-UJT7]; *see also* Irwin Reyes et al., *supra* note 50 at 75 (estimating that 257 of 5,855 free children's apps for Android participated in a safe harbor program). We examined the websites of the safe harbors to try to determine

Even if more companies participated in safe harbors, these programs would not be effective because the FTC has not imposed a high bar for approving safe harbors. To meet the requirement, safe harbors must adopt guidelines providing protections for children that are the same as or greater than those in the COPPA Rule. Most safe harbor applications have simply adopted language identical or similar to the Rule. As a result, the same problems that exist with COPPA—for example, overreliance on parental consent when parents do not or cannot know enough to make an informed decision—also exist with the safe harbor programs. One study that found that children's Android apps were likely violating COPPA at a broad scale found that apps from companies that belonged to safe harbors were just as likely to illegally transmit identifiers as the ones that were not.[74]

One argument for including the safe harbor provision was that safe harbors would empower industry to react more quickly to changes in technology than the government can, to ensure that children would be protected.[75] However, Commenters are not aware of any evidence that safe harbors have acted more quickly in response to changes in technology or the market place than the FTC. Indeed, apart from TRUSTe, which as described below amended its guidelines for a different reason, only one safe harbor amended its guidelines since 2014.[76]

---

the number of participants in each. IKeepSafe reported that it had 40 members representing 51 products, KidSAFE reported that said it had 89 websites or apps, and Privo listed 234 children's websites and apps. *See Products*, IKEEPSAFE, https://ikeepsafe.org/products/ [https://perma.cc/68HH-VTNA]; *Certified Products*, KIDSAFE, https://kidsafeseal.com/certifiedproducts.html [https://perma.cc/E3ZF-X9RX]; *myPrivo Directory*, PRIVO, https://my.privo.com/ng/index.htm#/ng/service-directory *[https://perma.cc/G4S5-QV7Z]*. Four (Aristotle, CARU, ESRB, and TRUSTe) did not disclose how many members participated in their programs.

[74] Irwin Reyes et al., *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, 2018 PROC. PRIVACY ENHANCING TECHS. 76 (2018), https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf [https://perma.cc/PZ2C-4GEH] ("In terms of transmitting personal information without consent, there is little (or no) difference between the certified apps and the DFF corpus").

[75] FED. TRADE COMM'N, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A REPORT TO CONGRESS 4 (2007), https://www.ftc.gov/sites/default/files/documents/reports/implementing-childrens-online-privacy-protection-act-federal-trade-commission-report-congress/07coppa_report_to_congress.pdf [https://perma.cc/5EQX-MAUK].

[76] ESRB proposed to modify its safe harbor program in March 2018. *See* Entertainment Software Rating Board's COPPA Safe Harbor Program Application to Modify Program Requirements, 83 Fed. Reg. 14,611 (Apr. 5, 2018). CCFC and CDD jointly opposed numerous modifications that would have weakened

There also is little evidence that COPPA safe harbors actually enforce their guidelines. In 2014, the FTC filed a complaint against TRUSTe alleging it had "failed to conduct promised annual recertifications of companies participating in its privacy seal program more than 1,000 times between 2006 and 2013."[77] The complaint did not identify how many of the companies were in TRUSTE's COPPA safe harbor program, but the consent decree required TRUSTe to maintain comprehensive records about COPPA-related safe harbor activities for 10 years and to provide detailed information to the FTC in its annual report.[78] Nonetheless, a few years later, the New York Attorney General found that TRUSTe had violated COPPA by failing to prevent illegal tracking technology from being used on some of the most popular children's websites including Roblox.com and Hasbro.com.[79] As part of this settlement, New York required that TRUSTe adopt new measures to strengthen its privacy assessments.[80] When the FTC

---

privacy protections for children. *See* Letter from Inst. for Pub. Representation, to the Federal Trade Commission Opposing Entertainment Software Rating Board's Application to Modify Program Requirements (May 7, 2018), https://www.law.georgetown.edu/wp-content/uploads/2018/08/Comments-by-CDD-and-CCFC-IPR-May-2018.pdf [https://perma.cc/XW8L-WE88]. The FTC required ESRB to amend its proposal to address these concerns. *See* Letter from the Fed. Trade Comm'n, to Entertainment Software Rating Board Approving the Entertainment Software Rating Board's Modifications to its Children's Online Privacy Protection Rule Safe Harbor Program (Aug. 13, 2018), https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-modifications-video-game-industry-self-regulatory-coppa-safe-harbor-program/p024526_commission_letter_approving_modified_esrb_program_and_exhibit_a.pdf [https://perma.cc/KJ8T-JTTZ].

[77] Press Release, Fed. Trade Comm'n, FTC Approves Final Order in TRUSTe Privacy Case (Mar. 18, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-truste-privacy-case [https://perma.cc/8S6Z-X2FV]. The complaint also alleged that TRUSTe misrepresented its status as a non-profit entity. Complaint at ¶¶17–23, *In re* True Ultimate Standards Everywhere, Inc., Dkt. No. C-4512 (Mar. 18, 2015), https://www.ftc.gov/system/files/documents/cases/150318trust-ecmpt.pdf [hereinafter TRUSTe Complaint] [https://perma.cc/CNX6-MPW4]; *Id.* The settlement included a $200,000 civil penalty. Decision and Order at 4, *In re* True Ultimate Standards Everywhere, Dkt. No. C-4512 (Mar. 18, 2015), https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf [hereinafter TRUSTe Consent Order] [https://perma.cc/6XPP-N4BS].

[78] *See* TRUSTe Complaint, *supra* note 77; TRUSTe Consent Order, *supra* note 77 at 3.

[79] Truman Lewis, *TRUSTe Pays Penalty, Stiffens Standards in Agreement with New York*, CONSUMER AFF. (Apr. 7, 2019), https://www.consumeraffairs.com/news/truste-pays-penalty-stiffens-standards-in-agreement-with-new-york-040717.html [https://perma.cc/X9QW-GNRQ].

[80] Letter from TRUSTe, to Fed. Trade Comm'n Submitting TRUSTe's Proposed Post-Approval Modifications to its Children's Privacy Program under 16 CFR §312.11(e) 3 (Mar. 22, 2017), https://www.ftc.gov/system/files/attachments/press-releases/ftc-seeks-comment-proposed-changes-trustes-coppa-safe-harbor-

sought public comments on TRUSTe's changes to the safe harbor program, several children's advocacy organizations argued that the changes were insufficient, but the FTC approved them anyway.[81]

When members are non-compliant, safe harbors do not appear to discipline them—or do so only rarely. An analysis of documents and data about the safe harbor programs by Commissioner Chopra's staff revealed that few safe harbors disciplined or suspended operator for noncompliance.[82] While the COPPA Rule provides several ways for safe harbors to discipline members for non-compliance, including public reporting of any action taken against subject operators,[83] Commenters know of no case where a safe harbor program publicly reported actions taken against its members for violating COPPA. Indeed, in the prior COPPA review, the safe harbor industry opposed the FTC's proposal to include the names of violators in the annual reports going to the FTC, and the FTC decided to only require the aggregate number of enforcement actions.[84] Nor are Commenters aware of any safe harbor member utilizing any of the other enforcement mechanisms in the COPPA Rule.

The lack of safe harbor enforcement does not appear to be due to a lack of violations. A systematic comparison of free children's apps on Google Play found the majority of child-directed apps were likely not in compliance with COPPA. In addition,

---

program/truste_childrens_privacy_program_amendments_31211e_ftc_submission_package_22mar2017.pdf [https://perma.cc/9XNU-9NPD].

[81] *See* Inst. for Pub. Representation, Comment in Response to the Request For Public Comment on TRUSTe Application for Modifications to Safe Harbor Program Requirements, Project No. P024526 (filed May 24, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/05/00017-140837.pdf [https://perma.cc/5KVP-HTJ4]; Letter from Fed. Trade Comm'n to TRUSTe Approving Application of TRUSTe for Approval of Modifications to its COPPA Safe Harbor Program (July 27, 2017), https://www.ftc.gov/system/files/documents/public_statements/1235693/p024526_commission_letter_approving_truste_application_07272017.pdf [https://perma.cc/NP4H-X5WC].

[82] Rohit Chopra, Cmm'r, Fed. Trade Comm'n, Address at Truth About Tech Conference (Apr. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1512078/chopra_-_truth_about_tech_4-4-19.pdf (prepared remarks) [hereinafter Chopra Truth About Tech Address] [https://perma.cc/3T3N-MQZ4].

[83] 16 C.F.R. § 312.11(b)(3)(i)–(v) (2019).

[84] Statement of Basis and Purpose, *supra* note 1 at 3996.

the percentage of non-compliance did not seem to be affected by whether the app participated in a safe harbor.[85]

Consistent with Commenters' evaluation of COPPA safe harbors, an analysis of documents and data about the safe harbor programs by Commissioner Rohit Chopra's staff revealed that "the programs generally received very few, often zero, complaints, even though many safe harbor programs have specific guidelines to give parents the ability to file complaints directly with them."[86] They noted that it was sometimes difficult to find out how to file a complaint, or that the forms were confusing or cumbersome. This analysis also found that few safe harbors disciplined or suspended operators for noncompliance.[87] Commissioner Chopra stated, and Commenters agree, that the FTC must "always be asking whether privatized policing mechanisms primarily see entities as clients, rather than companies they must watch over."[88]

Even if other aspects of the safe harbor program were not so flawed, this system would not achieve the goal of enhancing parental control over children's privacy because parents do not understand the safe harbors. In order for this system to work, parents must be able to easily find the seal that indicates any given website or online service participates in a safe harbor, understand what the seal means, know that they have a right to complain and have their claim resolved, and have sufficient incentives to file a complaint if they believe the website or online service is violating COPPA. None of these conditions are present.

In reviewing child-directed services, we found that it was often difficult to tell if the website or app is a safe harbor participant. For example, even though many Disney properties, including the website for Disney's popular Frozen movies (frozen.disney.com), participate in the Privo Safe Harbor, there is no Privo seal displayed on the home page of that website. A parent would need to scroll to the bottom of that page and click on the link for the children's privacy policy. That link goes

[85] Irwin Reyes, et al., *supra* note 50 at 75.
[86] Chopra Truth About Tech Address, *supra* note 82.
[87] *Id.*
[88] *Id.*

to Disney's generic children's privacy policy. To determine whether the Frozen website is covered, the parent must then click on the seal and scroll through the "gallery" of more than 75 covered services to see if Frozen is included.[89]

Even the presence of a COPPA safe harbor seal may not be instructive. There are seven different COPPA safe harbor seals, some of which have only been around a few years. It is unlikely that parents will be familiar with them all. This problem is exacerbated by the fact that some of the COPPA safe harbor programs have a range of seals that look similar, but signify different things, as shown in Exhibit B. Parents may erroneously believe that the presence of a seal means that the website or service collects no personal information from children, when it merely signifies that the service complies with COPPA's requirements.

B. Existing COPPA guidance does not adequately protect children's privacy in schools

Children also are insufficiently protected in the face of increasing privacy threats that result from schools' adoption of ed tech. The FTC has never brought a case against an ed tech company, despite privacy violations under COPPA being brought to its attention.[90] In addition, the FTC's guidance on the applicability of COPPA to the use of ed tech in schools suffers from two major limitations. First, it does not adequately distinguish educational purposes from commercial purposes. Second, it does not

---

[89] *See* Exhibit A. We also found, for example, that while Aristotle claimed ABCya.com as a member, ABCya.com's site displays the seal for the kidSAFE safe harbor. *Compare ABCya Certfication*, ARISTOTLE: INTEGRITY, https://privacy.integrity.aristotle.com/verify.aspx?id=76fe0fc0-b788-4e27-84b0-dcf4555d2718 [https://perma.cc/AKH7-552Q] *with* ABCYA, https://www.abcya.com/ [https://perma.cc/6CU3-NVGT]. Similarly, Aristotle lists Coolmath Network of websites as participants, but those sites do not display any safe harbor seal. *Compare e.g., Privacy Policy*, COOLMATH.COM, https://www.coolmath4kids.com/privacy-policy [https://perma.cc/QXB5-MNQ2] *with Coolmath Network Certification*, ARISTOTLE: INTEGRITY, https://privacy.integrity.aristotle.com/verify.aspx?id=40d913b7-f416-43e8-b843-1ea37c9b2b61 [https://perma.cc/XV7A-MESM].

[90] *See* Elec. Frontier Found., Comment in Advance of the Federal Trade Communication and Department of Education Student Privacy and Ed Tech Workshop on December 1, 2017, at 3 (filed Nov. 17, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/11/00034-141966.pdf [https://perma.cc/XRX8-2TMP].

address the use of boilerplate contracts by ed tech companies that enable more expansive use of children's data than schools or parents realize.

The FTC's guidance on the applicability of COPPA to ed tech appears to provide a limited exception to COPPA's requirement for verifiable parental consent. According to the FTC's COPPA Frequently Asked Questions, schools may consent on behalf of parents in limited situations when an ed tech company collects the personal information of students under the age of 13. Under existing guidance, a school may act as parents' agents and consent to the collection and use of information in the "educational context"—but only to the extent that the information is "for the use and benefit of the school, and for no other commercial purpose."[91] For commercial purposes, ed tech operators must obtain verifiable parental consent before collecting students' information.

However, the FTC's guidance does not clearly indicate how specific uses should be sorted into these two categories. The term "commercial purpose" is not clearly defined either in the COPPA statute or in the COPPA Rule. The FTC's guidance indicates that commercial uses are those "not related to the provision of the online services requested by the school," but this distinction is more procedural rather than substantive.[92] The guidance's overall definition effectively defines an educational purpose as any purpose "related to the provision of the online services requested by the school" as long as there is some benefit to the school.[93] Depending on the contract presented to a school by the ed tech provider, one could argue, for instance, that this includes online behavioral advertising or building user profiles of students in a particular grade—activity that clearly should be classified as a commercial, not educational, purpose.[94] This ambiguity opens the door to abuses of children's data in the ed tech context.

---

[91] *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMMISSION (Mar. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions (Question M.1) (emphasis added) [https://perma.cc/DRW4-Z5NM].
[92] *Id.* (Question M.2) (emphasis added).
[93] *Id.* (Question M.5) (emphasis added).
[94] *Id.* (Question M.5).

Nor can consent alone be trusted to protect children from inappropriate collection and use of private information by ed tech providers. The weaknesses of consent as a safeguard against privacy abuses are well-documented,[95] and are compounded in circumstances under which parents or teachers may feel pressured to consent to the data practices of ed tech providers that other parties have already selected. Overwhelmed parents also may not understand what they're reading, especially when their children's teachers or schools adopt numerous ed tech products at one time.[96] This framework is conducive to abuses of student data that parents may not understand and cannot effectively prevent. This is especially the case when privacy policies and notices mix together information about how children's data will be used both for educational and non-educational purposes.

For example, LearnBoost, an ed tech startup that allows teachers to upload notes on student attendance, performance, and behavior, describes data uses in its privacy policy that clearly have no educational objective. LearnBoost's privacy policy states that the company may "determine the approximate location of your device from your IP address," "access information stored on your mobile device via our mobile apps," and also "share information about you with third party vendors . . . that assist us with our marketing efforts."[97] Additionally, information may be used to "further develop and improve our Services."[98] But even though parents may have reservations or concerns about LearnBoost if they're aware that the company may use children's data for non-

---

[95] *See, e.g.,* Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV 1879 (2013); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019).

[96] In one school district, for example, parents received an "Online Digital Tools Consent Form" from their child's school at the beginning of the year containing a list of 46 different ed tech services and asking for parental consent to allow their child to use these tools in class. *See, e.g.*, Laura Moy (@lauramoy), TWITTER (Oct. 11, 2019, 9:00 AM), https://twitter.com/lauramoy/status/1182642230844112896/photo/1 [https://perma.cc/DMU2-TDBZ]. Each of these services also contain their own privacy policies that have very obtuse and conflicting language making it very time-consuming and difficult for parents to understand what information is actually being collected from their child and how that information is being used. *See, e.g., Privacy Policy*, GOOSECHASE, https://www.goosechase.com/privacy/ [https://perma.cc/FB9Q-MWBQ].

[97] *Privacy Policy*, AUTOMATTIC, https://automattic.com/privacy/ [https://perma.cc/8RU3-KYT9].

[98] *Id.*

educational purposes, LearnBoost's Terms of Use Agreement states that by agreeing to its terms, "Member is consenting to the use and disclosure of their personally identifiable information and other practices described in our Privacy Policy Statement."[99] The company also enables teachers to download and implement the software without the school administration even being aware of it.[100]

Several other commonly used ed tech services similarly rely on opaque or vague language in their privacy policies, language often inscrutable enough to violate COPPA's clear notice requirement. Under §312.4(a), an operator must provide notice that is "clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials."[101] However, many ed tech operator privacy policies are filled with very confusing, unclear, and conflicting language. Quizlet and Quizizz, for example, both of which are online study tools widely-used by children, include almost identical, opaque language in their privacy policies regarding the collection and sharing of student information. Both policies state that they do "not accumulate personal information about any child . . . for distribution, sharing, or selling, *except as described in this privacy policy*" [102] (emphasis added). This type of circular and indirect language is not uncommon, and places an emphasis on the non-collection of data rather than identifying those specific situations in which data is being collected from a child. In order to identify what those exceptions are, a parent must then take a deep dive into the obtuse language of the privacy policy just to understand how their child's data is being used. The main purpose of COPPA is to inform parents about how

[99] *Terms of Use*, LEARNBOOST (June 27, 2018, 2:03 AM), https://web.archive.org/web/20180627020354/https://www.learnboost.com/terms (accessed by searching for LearnBoost in the Internet Archive index) [https://perma.cc/NUJ4-XZ82].
[100] Simon, *supra* note 37. LearnBoost posted a notice on its website informing its users that the service will retire as of November 1, 2019, without any explanation. *LearnBoost is Retiring*, LEARNBOOST, https://www.learnboost.com/learnboost-is-retiring [https://perma.cc/U5Z5-YNQ3]. However, the company does not provide any information as to what will happen to the student data it collected from over 140,000 schools. *See Schools Index*, LEARNBOOST, https://www.learnboost.com/schools-list/[https://perma.cc/T9AS-3VY7].
[101] 16 C.F.R. § 312.4(a) (2019).
[102] *Privacy Policy*, QUIZIZZ, https://quizizz.com/privacy [https://perma.cc/7DC4-4LEC].

their child's data is being collected and such opaque language is an impediment to that goal.

The COPPA Rule also places an obligation on ed tech operators to obtain verifiable parental consent before collecting personal information from students for non-educational purposes.[103] However, in practice, many ed tech operators use boilerplate contracts to shift the onus of securing parental consent onto the school. In situations where a school is not authorized under COPPA to provide consent on a parent's behalf, companies rely on contract terms stating that the school is required to secure parental consent before allowing students to access the services.[104] For example, under COPPA, an ed tech provider like Google is generally responsible for providing parents with notice and obtaining verifiable parental consent for its G Suite for Education service.[105] Instead, Google uses contract terms that attempt to shift this responsibility onto schools. Google states, "We contractually require that schools using G Suite for Education get the parental consent required by COPPA. Our services can be used in compliance with COPPA as long as a school has parental consent."[106] With these types of provisions, ed tech companies essentially require the school to certify that it will comply with COPPA on the company's behalf.[107] Placing the burden of compliance onto the school to obtain verifiable parental consent when collecting student data for non-educational purposes is an inappropriate evasion of responsibility that belongs to the companies, not overburdened schools.

Some ed tech services even seem to misstate COPPA, specifically the situations in which it is appropriate for a school to provide consent on behalf of parents. Thinglink, a popular ed tech platform that allows students to alter images, videos, and create virtual tours, exemplifies this type of confusion in its privacy policy. Thinglink states, "Where the Service is used by a child for educational purposes, the educational institution may

---

[103] *See* 16 C.F.R. § 312.4(a).
[104] *See* Elec. Frontier Found., *supra* note 90 at 6.
[105] *Id.*
[106] *G Suite for Education FAQ*, GOOGLE SUPPORT, https://support.google.com/a/answer/139019?hl=en#COPPA [https://perma.cc/7ZSE-A5BB].
[107] *See* Elec. Frontier Found., *supra* note 90 at 6.

act as an agent of the parent for purposes of providing verifiable consent."[108] This policy misstates the FTC guidance regarding when schools can provide consent on behalf of parents. According to the FTC, "the school's ability to consent for the parent is limited to the educational context – where *an operator* collects personal information from students for the use and benefit of the school, and for no other commercial purpose."[109] In contrast, Thinglink's policy seems to incorrectly interpret this guidance to mean that a school may provide consent on behalf of a parent as long as the student is using the service for an educational purpose. Under this interpretation, Thinglink implies that there are situations in which an ed tech operator can collect a child's information for a commercial purpose without having to obtain verifiable parental consent. Given that the majority of ed tech services are used by children in schools for an educational purpose, Thinglink's apparent interpretation would open the door to allow ed tech operators to circumvent parental consent in far more circumstances than are actually permitted.

These terms also complicate efforts to vindicate breaches of students' privacy. For a company that collects and uses students' information beyond what a school could consent to, the company could claim that it relied on the school's implicit representation that it had secured consent. However, because schools are beyond the FTC's jurisdiction, charges of an alleged violation cannot be brought against the school. Thus, the contract potentially acts as a shield against a potential enforcement action for companies while redirecting blame toward a target outside of the FTC's reach. This combination of burden-shifting contract terms and the unclear scope of the FTC's definition of "educational purpose" puts student privacy at risk.

C. FERPA does not sufficiently protect children's privacy in schools

Unfortunately, the FTC also cannot rely on FERPA to protect children's privacy in schools. Although it was intended to protect the privacy of children in the

[108] *Privacy Policy*, THINGLINK, https://www.thinglink.com/privacy#id.pxnuitu1v2w [https://perma.cc/5S9M-2ED4].
[109] *Complying with COPPA: Frequently Asked Questions*, *supra* note 91 (emphasis added).

educational context, FERPA falls short in the ed tech era. A key cause of the statute's inefficacy is that FERPA is generally more permissive when schools share student information with third parties acting as "school officials," but the definition of "school official" is vague and has no clear standard. As a result, the exception for sharing of information with school officials is susceptible to abuse by companies that want to profit from student data, even when they have not demonstrated the need for the data in order to serve a true educational purpose.

FERPA generally prohibits the disclosure of student information to third parties without parental consent, but contains an exception for information that is shared with third parties that are acting as school officials. To qualify as a "school official":

- the third party must perform an institutional service or function for which the school would otherwise use its own employees;
- the third party's use and maintenance of student information must be under the school's direct control;
- the school must determine that the third party serves "legitimate educational interests"; and
- the third party cannot use student information for any other purpose than the educational purpose for which it was disclosed by the school.[110]

One significant challenge that arises in application of the school official exception is that no clear standard exists to determine when a party has "legitimate educational interests."[111] Schools are required to regularly report the criteria they apply in determining who constitutes a "school official" and what constitutes a "legitimate

[110] *See* 20 U.S.C. § 1232(g) (2012); 34 C.F.R. Pt. 99 (2019); PRIVACY TECH. ASSISTANCE CTR., DEPT. OF EDUC., SCHOOL RESOURCE OFFICERS, SCHOOL LAW ENFORCEMENT UNITS, AND THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) 11 (2019), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs_2-5-19_0.pdf [https://perma.cc/ZUP2-Q3NR].

[111] *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies - 4.B. Defining "Legitimate Educational Interests"*, NAT'L CENTER FOR EDUC. STAT., https://nces.ed.gov/pubs2004/privacy/section_4b.asp [https://perma.cc/B9H9-WY3K].

educational interest."[112] But there is little guidance to help schools define those criteria. As the National Center for Education Statistics (NCES) notes, criteria for a school official can be as simple as "a person . . . under contract to the agency or school to perform a special task."[113] A school official may be determined to have a legitimate educational interest if it is "necessary for that official to perform appropriate tasks that are specified in his or her position description or *by a contract agreement*."[114]

Schools and third parties appear to have interpreted this to mean that the question of whether a third party is considered a "school official" with "legitimate educational interests" may be resolved merely by forming a contract between the school and the third party. But contracts between third parties and schools often do not make clear that the third party has been designated a "school official" under FERPA and will abide by the requirements applicable to these parties. In a review of 100 popular ed tech applications and services, Common Sense Media found that 75% of the evaluated services were non-transparent about whether the company offering the service was designated "school officials" under FERPA.[115] In addition, these contracts are typically formed without either party making any independent showing that the third party does in fact have legitimate educational interests, and that information collected in the furtherance of those interests is strictly restricted to use for that purpose. For example, in its G Suite for Education contract, Google states that "[it] will be considered a 'School Official'" to the extent that it receives data protected under FERPA.[116] However, no

---

[112] This is required as part of the school's annual process of providing FERPA-required notification to parents regarding their rights under FERPA. DEPT. OF EDUC., THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT: GUIDANCE FOR PARENTS 5 (2011), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/for-parents.pdf [https://perma.cc/W7TD-VULD].

[113] *Id.*

[114] *Id.* (emphasis added).

[115] GIRARD KELLY, JEFF GRAHAM & BILL FITZGERALD, COMMON SENSE MEDIA, 2018 STATE OF EDTECH PRIVACY REPORT 107 (2018), https://www.commonsensemedia.org/sites/default/files/uploads/research/cs_state_of_edtech_privacy_report-2018.pdf [https://perma.cc/LG67-SN5F]

[116] *G Suite for Education (Online) Agreement*, GOOGLE FOR EDUCATION, https://gsuite.google.com/intl/en/terms/education_terms.html (Section 7.4) [https://perma.cc/UWK9-BMAT].

information is given regarding the educational purpose for which Google is provided with the student data, effectively undermining one of the criteria intended to limit the "school official" exception.

In fact, contracts between schools and third parties often allow ed tech companies to subvert FERPA's protections by enabling broad access to student data under boilerplate provisions. In 2013, researchers at Fordham Law School who reviewed cloud computing practices in twenty school districts found that 95% of responding districts were relying on cloud services, but *fewer than 7%* of the contracts between school districts and tech companies handling student data explicitly restricted the sale or marketing of student information.[117] Many of these agreements also allow tech companies to change the terms without providing notice to the school.[118]

In another example, Autodesk, a provider of educational design software, states in its Terms of Use that it will be considered a "school official" but further adds that "it will not maintain, use, or disclose Student Data except as set forth herein *and in the Autodesk Privacy Statement*, as authorized by you or permitted or required by applicable law or a judicial order."[119] However, Autodesk's Privacy Statement allows it to disclose a student's personal information to service providers, who may use it for marketing purposes, and to its "channel partners (resellers)."[120]

The problem of permissive contracts giving ed tech companies access to far more student data than is necessary is exacerbated by schools' lack of resources and professional development training in privacy and technology. System administrators in charge of deploying devices and software at schools along with teachers are often ill-equipped to properly vet an ed tech provider's privacy policies and terms of use. In 2018, only four out

---

[117] JOEL REIDENBERG ET AL., CTR. ON LAW & INFO. PRIVACY, PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 5 (2013), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip [https://perma.cc/H99T-CQHH].
[118] *Id.*
[119] *Education Providers and the Family Educational Rights and Privacy Act (FERPA)*, AUTODESK, https://www.autodesk.com/company/legal-notices-trademarks/access-use/website-terms-of-use/ferpa-terms (emphasis added) [https://perma.cc/5PQQ-W8HK].
[120] *Privacy Statement*, AUTODESK, https://www.autodesk.com/company/legal-notices-trademarks/privacy-statement#personal-data [https://perma.cc/9N2A-H4P5].

of ten K-12 teachers considered their professional development in ed tech training to be "very" or "extremely effective."[121] Other teachers have voiced concerns about the lack of awareness by entire school districts regarding student privacy in conjunction with the use of ed tech in the classroom. One teacher at a public school in Florida noted that her school district "does not seem to be deliberately ignoring privacy concerns, but just lacks general knowledge about ongoing discussions about student privacy."[122] A system administrator in charge of maintaining Google devices and software for a rural public school district of about 10,000 students admitted, "We don't know where this student data is going."[123] Many parents have become acutely aware of the lack of training and general unawareness about privacy issues in schools. Some have even described the use of ed tech in schools as "the wild west," or "a ticking time bomb, with faculty just "winging it."[124]

D. Lack of enforcement exacerbates the weaknesses of both FERPA and COPPA

The potential for abuse that COPPA's and FERPA's loopholes offer is reinforced by lack of enforcement or oversight by the agencies that oversee those statutes. For FERPA, the standard for what would constitute a violation is already relatively high: FERPA does not impose direct accountability on schools for individual violations. Instead, schools or districts must exhibit a "policy or practice" of denying parents or students their statutory rights before any enforcement action may be brought.[125] Thus, while the Department of Education retains the right to Rule that a school official did not

---

[121] VANESSA VEGA & MICHAEL ROBB, COMMON SENSE MEDIA, THE COMMON SENSE CENSUS: INSIDE THE 21ST-CENTURY CLASSROOM (2019), https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom-key-findings.pdf (compiling data from a nationally representative survey of over 1,200 K-12 teachers) [https://perma.cc/8HNN-9NJ9].

[122] Gennie Gebhart, *Spying on Students: School-Issued Devices and Student Privacy*, ELEC. FRONTIER FOUND. (Apr. 13, 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy [https://perma.cc/J5PV-FMB8].

[123] *Id.*

[124] *Id.*

[125] Elana Zeide, *The Limits of Education Purpose Limitations*, 71 U. MIAMI L. REV. 494, 502 (2017).

actually have a "legitimate educational interest" in accessing student information, it has never done so.[126] In fact, in the statute's forty-five-year history, the Department of Education has never exercised its option to withdraw federal funding as a result of a FERPA violation.[127] This lack of enforcement combined with the abuse of schools' discretion under the "school official" exception through the use of boilerplate contracts has significantly undermined FERPA's protections.

The FTC's lack of oversight compounds the problem—the agency has never brought a case against an ed tech company, despite having been alerted to privacy violations by ed tech providers.[128] Companies operating in a lucrative space have very little reason to devote resources to compliance and to ensuring that they're engaging in best privacy practices when there is little risk that breaking the law will have practical consequences for their business. The lack of oversight from both the Department of Education and the FTC creates exactly the wrong incentives for companies, which we urge the FTC to rectify.

III. The FTC should focus greater resources on enforcing the COPPA Rule

In light of widespread COPPA noncompliance, the most important thing for the FTC to do to protect children's privacy is to focus greater resources on enforcement. It also should dismiss YouTube content creators' resistance to enforcement.

A. The FTC should move more quickly to hold accountable violators of all parts of COPPA

As it conducts studies to better understand how children's information is collected and used, and alongside its review of the COPPA Rule, the FTC should focus greater resources on the easiest way to better protect children's privacy: fully enforcing the existing COPPA Rule, so that industry actors understand that compliance is not

---

[126] *See* Newsroom, *Joel Reidenberg on FERPA Overhaul*, FORDHAM L. NEWS (Apr. 28, 2015), https://news.law.fordham.edu/blog/2015/04/28/joel-reidenberg-on-ferpa-overhaul/ [https://perma.cc/HFT4-2YYF].
[127] *See id*.
[128] *See* Elec. Frontier Found., *supra* note 90 at 3.

optional. Taking commercial advantage of children can be quite lucrative. There are numerous online services and websites directed to children or with actual knowledge of children using their services, and as discussed above, COPPA noncompliance among these sites and services is widespread.[129] Operators of child-directed sites and services have rationally concluded that the likelihood of facing enforcement action is extremely small, and the FTC must take action to remedy that.

To better enforce the COPPA Rule, the FTC should begin by reviewing outside research indicating that hundreds, if not thousands, of apps and toys likely are in violation of COPPA.[130] Increasing strategic and public enforcement against major players would help send a clear message to industry that the Rule is not just words on paper, but must be followed.

The FTC also should routinely and publicly act on COPPA complaints filed by members of the public. The FTC's typical response to these complaints—silence—adds to the public perception that the FTC does not enforce COPPA. It appears that, at least in some cases, the FTC has investigated, but does not disclose the fact of the investigations or any action taken, even after investigations are closed. This information was gleaned from the FTC's response to a FOIA request filed by CCFC and CDD.[131] CCFC and CDD sought documents relating to the closing, determination, or disposition of FTC investigations relating to potential violations of COPPA. The request explicitly asked for information about 12 requests filed by CCFC and CDD, investigations made by FTC staff, and investigations requested by federal agencies, legislative bodies, and parties outside of the government. The FTC's response indicated that it had conducted, but ultimately closed investigations, concerning five of the 12 requests filed by CCFC and CDD. Yet the FTC never even issued closing letters that would have at least put the industry on notice that the agency actively investigates complaints.[132] Since some

[129] *See* discussion *supra* Section II.A.
[130] *See id.* (summarizing research produced by teams at Oxford University, UC Berkeley, and Princeton).
[131] FOIA Request Letter from Ctr. for Dig. Democracy & Campaign for a Commercial-Free Childhood, to the Federal Trade Commission (June 5, 2019) (on file with the Institute for Public Representation).
[132] *See* Elec. Privacy Info. Ctr., Complaint and Request for Investigation, Injunction, and Other Relief, *In re* Genesis Toys and Nuance Communications (filed Dec. 6, 2016) (the Commission closed its investigation

materials were withheld or redacted, it is possible that the FTC has undertaken other investigations that were not disclosed. But the apparent failure of the FTC to act in response to public requests, and to even disclose after the fact when it has conducted an investigation, creates disincentives for companies to comply with the law.

When the FTC does take enforcement action against companies for violating the COPPA Rule, it should do so swiftly. Swift action would help prevent misplaced investment in unlawful activities. For example, the YouTube content creators currently flooding this docket with objections to COPPA are reacting to the fact that YouTube facilitated widespread COPPA violations on its platform for years, and now is adopting abrupt changes to attempt to come into compliance following its recent settlement with the FTC over COPPA violations. But the FTC could have prevented this state of affairs merely by taking action against YouTube earlier, before thousands of content creators grew accustomed to benefiting from unlawful behavioral advertising to children without parental consent.

Finally, the FTC should ensure that any COPPA-related enforcement actions it undertakes are strong enough to dispel any notion that the consequences of noncompliance may merely be absorbed as a cost of doing business. More specifically, the FTC should not enter into consent decrees with companies for penalty sums outweighed many times over by the profits generated by the COPPA-infringing behavior. Doing so only validates COPPA violators' assessment of COPPA as worth violating. The FTC also should force COPPA violators to delete any and all children's data collected in violation of COPPA, as well as to submit subsequently to close and ongoing oversight to ensure that the offending behavior does not recur.

---

on April 13, 2018); Ctr. for Dig. Democracy, Complaint and Request for Investigation of Disney's MarvelKids.com's Violation of COPPA (filed Dec. 18, 2013) (the Commission's investigation closed on September 19, 2014); Ctr. for Dig. Democracy, Complaint and Request for Investigation of Sanrio's Hello Kitty Carnival's Violation of COPPA (filed Dec. 18, 2013) (the Commission's investigation closed on September 19, 2014); Ctr. for Dig. Democracy, Complaint and Request for Investigation of Nickelodeon's Spongebob Diner Dash's Violation of COPPA (filed Dec. 17, 2012) (the Commission's investigation closed on March 19, 2013); Ctr. for Dig. Democracy, Complaint and Request for Investigation of Mobbles Corporation's Violation of COPPA (filed Dec. 11, 2012) (the Commission's investigation closed before 2013).

In sum, the FTC could better protect children's privacy simply by more actively enforcing the existing COPPA Rule. If companies believed that there was an actual risk of getting caught and having to pay substantial penalties for violating COPPA, they would be much more likely to comply with the law and protect children's privacy.

B. The FTC should view the YouTube content creators' resistance to enforcement of COPPA with skepticism

The FTC should be skeptical about industry resistance to enforcement of the COPPA Rule. The objective of COPPA is first and foremost the protection of children's privacy, not the profitability of companies that monetize violations of it. As in other areas of consumer protection, Congress made a judgment that children's well-being merits limitations on industry practices that are lucrative for companies, but harmful for vulnerable children.[133] Congress passed COPPA to rein in the use and collection of children's personal information with the full understanding that these practices are profitable for companies.[134] The Congressional record makes clear that the protection of children is the objective of the law first and foremost, and the FTC's Rules must reflect Congress's judgment.[135]

In particular, the FTC should approach the more than 173,000 comments filed by YouTube content creators objecting to COPPA with skepticism. As an initial matter, content creators' comments contain large amounts of misinformation. Commenting in this docket, some content creators have incorrectly declared that children's content will

---

[133] For example, Congress authorized the Food and Drug Administration to set exacting quality controls for baby food. *See* 21 U.S.C. § 350a(b) (2012). Similarly, it authorized the Consumer Product Safety Commission to regulate toys, cribs, and other products to ensure that they do not pose undue risks to children. *See* 15 U.S.C. § 2056a.

[134] 144 CONG. REC. S8482–83 (daily ed. July 17, 1998) (statement of Sen. Bryan).

[135] 144 CONG. REC. S12787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan) ("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 privacy by limiting the collection of personal information from children without parental consent.").

be banned from YouTube or that no advertising whatsoever will be permitted on children's content, and blame COPPA for these straw men concerns.[136]

Content creators' focus on COPPA is also misplaced. To the extent that changes on the platform designed to protect children's privacy are disruptive to creators, the genesis of this problem is that YouTube deliberately facilitated and participated in widespread violations of COPPA—a law older than YouTube itself—for years, and a number of creators shared in the profits borne out of that noncompliance. For many years, YouTube has continually made changes to its policies to enable creators to better monetize their content.[137] But by deliberately denying that children under 13 were on its platform in order to avoid having to comply with COPPA, YouTube enabled an illegal market to develop: large portions of its service that are child-directed and that collect children's personal information for advertising purposes without parental consent, in violation of COPPA. Only now that it has been subjected to enforcement action, YouTube is finally adopting changes to its platform in an attempt to bring the platform into compliance.

In its communications to content creators and the public about the changes it is adopting, YouTube has omitted key facts. Without parental consent, the operation of behavioral advertising on child-directed portions of YouTube *was always illegal*—and YouTube simply and brashly violated the law for years.[138] The content creators' concerns about YouTube's sudden shift in its policies are understandable, but the object of their ire should not be the Rules protecting children's privacy, but YouTube. Given that YouTube has also raised concerns about the viability of children's content without

---

[136] *See, e.g.*, KreekCraft, *YouTube Banning Roblox Videos... HOW TO STOP THIS! | Roblox Jailbreak*, YOUTUBE (Sept. 27, 2019), https://www.youtube.com/watch?v=uTcDagCLNgc [https://perma.cc/SQK6-L3T3].

[137] *See e.g.*, Vasiliki Kanistra & Devon Storbeck, *A Friendly Reminder and Monetization Advice*, YOUTUBE: CREATOR BLOG (Feb. 21, 2013), https://youtube-creators.googleblog.com/2013/02/a-friendly-reminder-and-monetization.html [https://perma.cc/VN8C-HALB].

[138] *See* Susan Wojcicki, *An Update on Kids and Data Protection on YouTube*, YOUTUBE: OFFICIAL BLOG (Sept.4, 2019), https://youtube.googleblog.com/2019/09/an-update-on-kids.html [https://perma.cc/4LB8-DWGA].

the revenue from illegal tracking, perhaps it could consider taking less than 45% percent of the revenue that its content creators earn.

IV. If the FTC adopts changes to the COPPA Rule, it should strengthen children's privacy protections

Commenters again urge the FTC to undertake 6(b) studies to better understand how children's data is collected and used before undertaking any Rule revisions. We note, however, based on what is already known, it is clear that children need stronger privacy protections and that the existing COPPA Rule should not be weakened in any way.

If the Commission does consider changes to the COPPA Rule, commenters urge the FTC to:

- not permit general audience platforms to erect age gates for child-directed content;
- retain its enforcement policy statement for voice recordings;
- strengthen protections for student privacy;
- tighten and update its definition of "support for the internal operations of the Web site or online service";
- expand the definition of "personal information"; and
- promulgate new Rule revisions implementing neglected sections of the statute.

A. The FTC should not permit general audience platforms to rebut the presumption that users of child-directed portions of their services are children

The FTC asks if it should permit general audience platforms that identify and police child-directed content to "rebut the presumption that all users of the child-directed third-party content are children thereby allowing the platform to treat under and over age 13 users differently."[139] It should not. General audience platforms that

[139] 2019 COPPA RFC, *supra* note 70 at 35,846.

knowingly operate child-directed portions of their services should be required to treat consumers of the child-directed offerings as children under COPPA.

Large portions of general audience platforms are obviously and indisputably child-directed. Though accessed through general audience platforms, these child-directed offerings are intended for consumption by children and offer no appeal for most adults. As the FTC observed in its September 2019 COPPA complaint regarding YouTube, "YouTube hosts numerous channels that are 'directed to children' under the COPPA Rule."[140] Child-directed offerings include ChuChuTV, which describes itself as "designed to engage children through a series of upbeat nursery rhymes and educational songs with colorful animations,"[141] and BabyTV, "the world's leading baby and toddler network from FOX."[142]

It is possible that some adults like to consume content specifically designed for preschoolers and babies. But until the Commission conducts 6(b) studies that uncover industry data demonstrating how often adults consume children's content and how general audience platforms are able to identify when a viewer of child-directed content is an adult, the FTC should not make changes to how general audience sites treat child-directed content.

It would be particularly troubling if the FTC were to permit general audience platforms to "rebut the presumption" that patrons of their child-directed offerings are children based on users' self-identified ages as described in user profiles. Many families share accounts, devices, and apps among family members—especially with young family members not yet old enough to read online instructions and terms, select appropriate profiles, navigate complex menus, type in their own details, or own their own devices. As a result, children undoubtedly will patronize child-directed content on their parents' devices, logged in to their parents' profiles. Platforms should not be able

[140] YouTube Complaint, *supra* note 2 at ¶28.
[141] *ChuChu TV Nursery Rhymes & Kids Songs*, YOUTUBE, https://www.youtube.com/user/TheChuChuTV/about [https://perma.cc/PP6K-9J8M].
[142] *BabyTV*, YOUTUBE, https://www.youtube.com/user/BabyTVChannel/about [https://perma.cc/A6NG-4A5Q].

to treat consumers of child-directed content as adults simply because they are logged in as adults.

B. The FTC should retain its enforcement policy statement for voice recordings

Since 2017 the FTC has operated under guidelines set forth in an enforcement policy statement addressing the use of audio files containing a child's voice.[143] The FTC now asks if it should amend the COPPA Rule to specifically include such an exception.[144] It should not. The FTC's existing enforcement policy allows children to use voice commands with connected devices while protecting their privacy. There is thus no need to codify this exception. However, if the FTC does amend the Rule to include an exception for children's voice files, under no circumstances should it, as the FTC asks, permit an operator to "be able to de-identify these audio files and use them to improve its products."[145] Rather, the FTC should codify the existing safeguards, including a strict policy that prohibits retention even of supposedly "de-identified" children's voice data. The FTC asks if de-identification of audio files is effective at preventing re-identification.[146] It is not. Therefore the FTC should not adopt a carve-out for de-identified voice recordings used for product improvement or any other purpose.

1. The enforcement policy statement allows children to utilize voice commands while protecting their privacy

There is no need to codify the FTC's enforcement policy statement because it already effectively allows children to utilize voice commands while also protecting children's privacy. As the FTC recognizes, an audio file of a child's voice used solely as a replacement for written words constitutes "collection" as that term is defined in the

---

[143] *See generally* Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, 82 Fed. Reg. 58,076 (Dec. 8, 2017) [hereinafter Voice Recording Policy].
[144] 2019 COPPA RFC, *supra* note 70 at 35,845.
[145] *Id.*
[146] *Id.*

COPPA Rule.[147] At the same time, the FTC acknowledges that there is value to using voice for performing search and other functions on interconnected devices.[148] It therefore adopted a policy that it would not take an enforcement action against an operator for collecting an audio file of a child's voice without first obtaining verifiable parental consent, if the audio file is used solely as a replacement for the written word, such as to perform a search of fulfill a request, and the operator maintains the file only for the brief time necessary for that purpose.[149] Additionally, the FTC also identified critical limitations on how operators may use these voice recordings:

- requests for information via voice that would otherwise be considered personal information are excluded;
- companies must provide clear notice of their collection and deletion policies in their privacy policy;
- children's voice recordings may not be used for any purpose other than completing the child's instruction or request; and
- the enforcement policy does not affect a company's other obligations under COPPA if it also collects other types of personal information from children.[150]

The safeguards set forth in the enforcement policy mirror COPPA's emphasis on data minimization. For example, allowing children's voices to be used for voice recognition or purposes beyond executing the voice command mirrors the data minimization principle underlying Section 312.7.[151] Similarly, Section 312.10 requires operators to only retain personal information collected by children only for as long as is reasonably necessary to fulfill the purpose for which the information was collected.[152] The enforcement policy implements this requirement by requiring a child's voice

[147] Voice Recording Policy, *supra* note 143 at 58,076; *see also* 16 C.F.R. § 312.2 (2019).
[148] *Id*.
[149] *Id*.
[150] *See id*. at 58,076–77.
[151] *See* § 312.7 (2019).
[152] § 312.10.

recording only be retained for the brief period necessary to execute the command and then immediately deleted.[153]

In addition, the enforcement policy recognizes the challenges these devices pose for acquiring consent from parents of children who do not live in the home with the voice-enabled device. A child visiting the home of a friend that has a smart speaker or similar device may have their voice recorded without their parents ever being notified or asked for consent. Further, even if the parents knew that their child's voice was recorded, they would have no way to review or delete these recordings. The prevalence of this problem is increasing as these devices proliferate. The number of smart speakers in U.S. households grew by 78% between December 2017 and 2018, and the trend shows no sign of slowing down.[154] The enforcement policy statement addresses this problem by imposing strict controls on how personal information may be used or retained. In doing so, it minimizes the children's privacy risk presented by playdates in homes with voice-enabled devices.

Because the existing enforcement policy statement effectively protects children's privacy while allowing them to take advantage of voice-enabled interconnected devices, there is no need to amend the COPPA Rule.

2. Should the FTC codify its enforcement policy statement, it must include the same safeguards and limitations without a de-identified data or product improvement exception

In the event that the FTC nevertheless decides to codify its enforcement policy statement in the COPPA Rule, it is critical that the FTC include in the Rule the same protections that it has included in the enforcement policy statement. Under no circumstances should the FTC allow operators to retain and use de-identified voice

---

[153] *See id*.; Voice Recording Policy, *supra* note 143 at 58,076.

[154] *See* NATIONAL PUBLIC MEDIA, THE SMART AUDIO REPORT (WINTER 2018) 5 (2019), https://www.nationalpublicmedia.com/wp-content/uploads/2019/01/Smart-Audio-Report-Winter-2018.pdf (118.5 million smart speakers) [https://perma.cc/H7Y4-M5ZJ]; *Child Population by Age Group in the United States,* KIDS COUNT DATA CTR., https://datacenter.kidscount.org/data/tables/101-child-population-by-age-group#detailed/1/any/false/37/62,63,64/419 (60.9 million children under 14) [https://perma.cc/ZDV3-HRV2].

recordings to "improve [their] products." Such an exception would vastly undermine those protections.

De-identified data is generally susceptible to re-identification, and given the multiple dimensions of human speech, voice recordings are especially vulnerable.[155] In 2014, the President's Council of Advisors on Science and Technology (PCAST) recognized that while de-identification was somewhat useful as an added safeguard, the strategy was vulnerable to future re-identification methods. Ultimately, it concluded that de-identification was not "a useful basis for policy."[156] Similarly, a 2015 report by the National Institute of Standards and Technology (NIST) found that while the "purpose of de-identifying data is to allow some uses of the de-identified data while providing for some privacy protection by shielding the identity of the data subjects, . . .there is a trade-off between the amount of de-identification and the utility of the resulting data."[157]

Today, as data sets grow larger and contain more indirect identifiers, the risk of re-identification similarly grows. Researchers recently concluded that 99.98% of Americans would be correctly re-identified in any dataset using just fifteen demographic attributes.[158] As data sets become increasingly high-dimensional—containing enough data points about each individual that their records are likely to be unique—de-identification alone is no longer a sufficient privacy safeguard.[159]

---

[155] *See* Slobodan Ribarić & Nikola Pavešic, *De-identification for Privacy Protection in Biometrics*, *in* USER-CENTRIC PRIVACY AND SECURITY IN BIOMETRICS 305–09 (Claus Vielhauer ed., 2017), https://bib.irb.hr/datoteka/923532.PBSE0040_Vielhauer_Chapter13_Proof-1.pdf [https://perma.cc/9BFQ-5YAS].

[156] EXEC. OFFICE OF THE PRESIDENT: PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 39 (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/9HUB-EN8E].

[157] SIMSON L. GARFINKEL, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, DE-IDENTIFICATION OF PERSONAL INFORMATION 11 (2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf [https://perma.cc/52T2-5JYN].

[158] Gina Kolata, *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html [https://perma.cc/2FPT-N94M].

[159] *See* ANN CAVOUKIAN & DANIEL CASTRO, BIG DATA AND INNOVATION, SETTING THE RECORD STRAIGHT: DE-IDENTIFICATION *DOES* WORK 3 (2014), http://www2.itif.org/2014-big-data-deidentification.pdf ("In the

How a child speaks can also reveal information about them and be used to identify them in other contexts. Prosodic features—features that describe how content is delivered orally, such as intonation, speech rate, and intensity—can be used to identify a person regardless of what they actually say.[160] These recordings can be used to create a voiceprint that allows for otherwise de-identified voice recordings to be linked even if they were made across different devices or covered different topics.[161] Further, these features can be used to infer additional information about the speaker, such as their emotional state and degree of expressed emotion[162], their gender,[163] or even their physical strength.[164] This information creates additional indirect identifiers that increases the risk that the recording could be re-identified.[165]

---

case of high-dimensional data, additional arrangements may need to be pursued, such as making the data available to researchers only under tightly restricted legal agreements.") [https://perma.cc/4TXT-C5TN].

[160] *See* Leena Mary & B. Yegnanarayana, *Prosodic Features for Speaker Verification*, *in* PROCEEDINGS OF INTERNATIONAL CONFERENCE ON SPOKEN LANGUAGE PROCESSING 917 (2006), https://pdfs.semanticscholar.org/fc96/e14ac456fee4c3c6349dca4d717f6ea0def7.pdf [https://perma.cc/H83R-7KU7].

[161] *See generally* Andrew Boles & Paul Rad, *Voice Biometrics: Deep Learning-Based Voiceprint Authentication System*, *in* 12TH SYSTEM OF SYSTEMS ENGINEERING CONFERENCE (SOSE) (2017), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7994971 [https://perma.cc/URH2-UR8R]; Penghua Li et al., *A Spectrogram-Based Voiceprint Recognition Using Deep Neural Network*, *in* THE 27TH CHINESE CONTROL AND DECISION CONFERENCE (2015), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7162425 [https://perma.cc/8CGH-P98W]; *cf.* Abigail Tracy, *Facebook Has Your Faceprint, Here's Why That Matters*, FORBES (June 24, 2015), https://www.forbes.com/sites/abigailtracy/2015/06/24/facebook-has-your-faceprint-heres-why-that-matters/#6f95de8d18eb (discussing how Facebook uses a faceprint to identify users even in photos in which they are not tagged) [https://perma.cc/X6PL-HDPU].

[162] Amazon recently announced that it would be using this technology to understand a user's tone and inflection. *See* Viktor Rozgic, *Using Adversarial Training to Recognize Speakers' Emotions*, AMAZON ALEXA (May 21, 2019), https://developer.amazon.com/blogs/alexa/post/2d8c2128-eec9-44cc-9274-444940eb0a4d/using-adversarial-training-to-recognize-speakers-emotions [https://perma.cc/FZ9J-B8MX].

[163] *See* Hadi Harb & Liming Chen, *Voice-Based Gender Identification in Multimedia Applications*, 24 J. INTELLIGENT INFO. SYS. 179, 179 (2005), https://link.springer.com/content/pdf/10.1007%2Fs10844-005-0322-8.pdf [https://perma.cc/5X3B-7C8U].

[164] *See* Aaron Sell et al., *Adaptations in Humans for Assessing Physical Strength from the Voice*, 277 PROC. ROYAL SOC'Y 3509, 3510 (2019), https://royalsocietypublishing.org/doi/pdf/10.1098/rspb.2010.0769 [https://perma.cc/TR3V-9RFE].

[165] For example, one study of emotional categorization of voice recordings identified 62 features that were independent of the content of the speech or the speaker. If 99.98% of Americans would be correctly re-identified using just fifteen attributes, the 62 features used to identify emotion alone could pose a significant risk of re-identification. *See* Keshi Dai et al., *Recognizing Emotion in Speech Using Neural Networks*, *in* PROCEEDINGS OF THE IASTED INTERNATIONAL CONFERENCE ON TELEHEALTH/ASSISTIVE

Even if de-identification worked, the FTC should not permit an operator the latitude to use voice recordings to "improve its products." This "exception" could be broadly interpreted by operators in ways that violate children's privacy. In addition, allowing an operator to use the data across a suite of products could give large platform companies a competitive advantage over smaller companies. Thus, the FTC should limit the use of children's voice recordings to simply fulfilling the child's request or command and nothing else.

The enforcement policy statement's protections are a critical foundation that should not be eroded when updating COPPA to address the expansion of voice-enabled connected devices. The FTC needs to ensure that these principles are incorporated in an exception as faithfully as possible to the original enforcement policy statement. To do otherwise, such as by allowing the use of de-identified voice recordings for product improvement, would undermine these protections.

C. The FTC should modify the COPPA Rule and its enforcement approach to better protect children in the ed tech context

As the use of ed tech becomes more pervasive, the FTC acknowledges that the COPPA Rule may require modification, noting "questions . . . have arisen about the Rule's application to the educational technology sector."[166] In addition to the specific questions posed in the Request for Comment, the FTC more broadly seeks comment on "whether certain sections should be retained, eliminated, or modified."[167] Commenters again urge the Commission to use its 6(b) authority to further study the ed tech sector, but also urge the Commission to consider developing revisions to the COPPA Rule to protect the privacy of students under 13 in the ed tech context. As noted above, at present neither existing COPPA guidance nor FERPA sufficiently protects the privacy of children in schools. The FTC should extend COPPA more robustly over the ed tech

---

TECHNOLOGIES 31–36 (2008), http://www.ccis.northeastern.edu/home/daikeshi/papers/iasted08.pdf [https://perma.cc/84DQ-87PP].

[166] 2019 COPPA RFC, *supra* note 70 at 35,842.

[167] *Id*.

context by clearly defining what constitute "educational" and "commercial" purposes under COPPA and by outright prohibiting the commercial use of data collected from students in the educational context.

1. The FTC should not create an exception to parental consent for the use of education technology in schools

The FTC asks whether it should "consider a specific exception to parental consent for the use of education technology used in the schools."[168] Unless and until the privacy and education standards applicable to ed tech providers are dramatically improved upon, the FTC must not consider such an exception. As discussed above, ed tech enables the tracking, recording, and potentially even the sale of children's private information. The countless providers available vary widely in the extent of their data collection, the rigor of their privacy protections, and the educational value of their services. Under the current circumstances, parents simply cannot trust that ed tech providers selected by their children's schools or teachers will appropriately limit collection and retention of private data, sufficiently protect the data they do collect, use children's data only for educational purposes, and offer an educational benefit to children that outweighs any potential privacy concerns that parents may have. Parents must retain the right to be notified of information that sites and services wish to collect about their children, as well as the right to refuse the requested collection of information when they are not satisfied with the privacy practices or educational value of the collecting entity.

The FTC also asks specifically about creating an exception to parental consent based on the "school official" exception found in FERPA.[169] In no event should the FTC use the FERPA school official exception as a model. As discussed at length above, FERPA's school official exception is deeply flawed.[170] In particular, although only parties with "legitimate educational interests" are supposed to qualify as school

[168] *Id.* at 35,845.
[169] *Id.* at 35,845.
[170] See discussion at *supra* Section II.C.

officials, no clear standard exists to make this determination, and the lack of enforcement of both COPPA and FERPA invites abuse of the designation.

2. The FTC should clearly define "educational context" and "commercial purpose" under COPPA

In its original guidance, the FTC properly recognized that while schools have some authority to consent on parents' behalf, that authority is restricted to the educational context.[171] However, as discussed above, one major reason that COPPA currently fails to protect children's privacy in schools is that the definition of "educational context" is unclear. This invites definitional creep and, in the worst cases, even abuse of student information. To address this problem, the FTC should clearly define the scope of acceptable uses that can be justified in the name of the school's educational context.

A number of states have provided examples of what a narrower and more specific "educational purpose" could look like. California's Student Online Personal Information Protection Act ("SOPIPA"), for example, provides an exception that allows ed tech providers to use student information if it is for "K-12 school purposes." Under SOPIPA, "K-12 school purposes" are narrowly defined as those that "customarily take place at the direction of the K–12 school, teacher, or school district or aid in the administration of school activities, including . . . instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school."[172] Very similar variations of this definition have also been adopted by Connecticut and Delaware.[173]

In contrast to the FTC's guidance, which merely limits educational purposes to those in which an operator collects personal information from students "for the use and benefit of the school," the definitions that have been used by these states significantly

---

[171] *Complying with COPPA: Frequently Asked Questions*, *supra* note 91 (Section M).
[172] Student Online Personal Information Protection Act (SOPIPA), CAL. BUS. & PROF. CODE § 22584(j) (West 2016).
[173] *See* CONN. GEN. STAT. ANN. § 10-234aa(8) (West 2016); DEL. CODE ANN. tit. 14, § 8102A(7) (West 2016).

clarifies and narrows the scope of an educational purpose may include.[174] This is in contrast to the broad interpretation of educational purpose that some ed tech providers have applied. For example, under the vague definition of "educational context" provided in the COPPA FAQs, some commenters have contended that product improvement should fall under the umbrella of educational purposes, because improved versions of the product would be better at performing the functions the product was meant for, and would thereby benefit both students and the school.[175] But a company collecting student information to improve its product, and certainly other products it offers, is often not in service of pedagogical improvement. A more personalized product based on lots of student personal data may be more tailored and more profitable to the company without providing a better educational outcome. The use of students' data to determine how to better advertise to students, or to get them to spend longer on the platform, would similarly provide benefits primarily to the company, with the benefit to students being ancillary at best, all while presenting an additional privacy risk.[176]

Moreover, at present the only guarantee that an ed tech company will in fact collect, use, and retain children's data strictly for educational purposes is its word—and in an ecosystem in which lack of transparency, lack of enforcement, and the profitability of data create incentives to collect as much data as possible, relying solely on that word would be foolhardy. The FTC should follow the lead of SOPIPA, which clarifies that using student information to improve the product is not a purpose that

---

[174] *Compare, e.g.*, CAL. BUS. & PROF. CODE § 22584(j) *with Complying with COPPA: Frequently Asked Questions*, *supra* note 91.

[175] *See, e.g.*, Computing Technology Industry Association, Comment in Advance of the Federal Trade Commission and Department of Education Student Privacy and Ed Tech Workshop on December 1, 2017, at 2 (filed Nov. 17, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/11/00033-141965.pdf [https://perma.cc/Y6FZ-RYZL]; Future of Privacy Forum, Comment in Advance of the Federal Trade Commission and Department of Education Student Privacy and Ed Tech Workshop on December 1, 2017, at 5 (filed Nov. 17, 2017), https://www.ftc.gov/policy/public-comments/2017/11/17/comment-00036 [https://perma.cc/ME85-XQBH].

[176] *See, e.g.*, Elec. Frontier Found., *supra* note 90 at 3.

customarily takes place at the direction of the school, nor does it aid in the administration of instruction in the classroom.[177]

3. The FTC should prohibit the commercial use of data collected from students even with parental consent

To further protect children's privacy in the ed tech context, the FTC should prohibit the commercial use of data collected from students by providers that identify themselves as ed tech providers. The state privacy laws discussed above provide a helpful baseline to identify those purposes in which using student information should be strictly prohibited. Under SOPIPA, ed tech operators are specifically prohibited from "knowingly using, disclosing, compiling, or allowing a 3rd party to use, disclose, or compile the personal information of a minor for the purpose of marketing or advertising specified types of products or services."[178] The Connecticut Student Data Privacy Act of 2016 similarly prohibits ed tech operators from using student information for the purposes of "targeted advertising on the operator's Internet web site, online service or mobile application, or . . . targeted advertising on any other Internet web site, online service or mobile application."[179] The Idaho student privacy law requires schools entering into contracts with private vendors to either ensure that their contracts include a provision that requires private vendors to disclose any secondary uses of student data, or place an outright prohibition on private vendors against "any secondary uses of student data . . . including . . . sales, marketing or advertising, but permitting the private vendor to process or monitor such data solely to provide and maintain the integrity of the service."[180]

These state privacy laws illustrate how a narrower use standard can help prevent abuses of student information by tech companies. Clarifying and narrowing the standard for what practices serve an "educational purpose" would eliminate confusion

---

[177] CAL. BUS. & PROF. CODE § 22584(j).
[178] S.B. 1177, 2015 Leg., Reg. Sess. (Cal. 2015) (codified at CAL. BUS. & PROF. CODE § 22584(j)) (Legislative Counsel's Digest).
[179] CONN. GEN. STAT. ANN. § 10-234cc(b)(1) (West 2016).
[180] IDAHO CODE § 33-133(m)(3)(b)(vi) (2014).

among ed tech companies, and it would enable schools to better understand the full extent to which they can consent on behalf of parents. Prohibiting commercial use of data collected from students in schools would likely be the most effective way to prevent student data from being exploited, given the lack of transparency over corporate practice, under-enforcement, and the failures of consent as a privacy guardrail.

4. The FTC should prohibit ed tech companies from relying on contractual terms that put the onus on schools to secure parental consent

The FTC also must not permit operators that are required to obtain verifiable parental consent for the collection and use of children's information to offload that responsibility onto already overwhelmed schools. This practice is widespread at present, and it undermines one of COPPA's primary objectives: providing parents with greater control over their children's information. The shift in responsibility from ed tech operators to schools in effect gives ed tech operators an unfair advantage as they are able to profit from collecting student information while pushing their legal requirements onto the very schools that are providing a captive audience for their services.

Three commonly used ed tech platforms, Edulastic, Remind, and Goosechase, all have policies that place the onus of obtaining verifiable parental consent on schools. The FTC's COPPA FAQs permits an ed tech company to accept the school's consent in place of a parent only when the collection of information is used only in the educational context—but these are three examples of companies that have interpreted the FTC's guidance to allow them to almost completely wash their hands of COPPA responsibility. "If you are a school, district, or teacher, you represent and warrant that you are solely responsible for complying with COPPA," states the Remind privacy policy.[181] This behavior constitutes an abuse of the FTC's attempt to permit schools to

[181] *See Terms and Policies*, REMIND (Aug. 30, 2019), https://www.remind.com/terms-of-service ("If you are a school, district, or teacher, you represent and warrant that you are solely responsible for complying

provide consent on behalf of parents, which was intended for the convenience of schools, not ed tech operators.

In the absence of more rigorous limitations placed on ed tech providers' use of student information for non-educational purposes, children's information is subject to unacceptable privacy risks in the hands of these companies. The FTC therefore should clarify that ed tech companies cannot transfer their responsibility for ensuring parental consent to schools. The FTC should also clarify that contractual terms do not mitigate a company's responsibility for ensuring it has gotten verifiable parental consent for every student under 13 whose information it wishes to collect. By shifting responsibility back onto companies, the FTC can ensure that the goal, in the words of Senator Markey, is "to help scholars make the grade, not help companies make a sale."[182]

D. The FTC should strengthen and modernize its definition of "support for the internal operations of the Web site or online service"

The FTC should revise its definition of "support for the internal operations of the Web site or online service," which defines certain circumstances under which an operator may collect personal information from a child and incur fewer obligations under the COPPA Rule. The exceptions under the Rule for information collected to provide support for internal operations rest on the theory that in these circumstances, information is only being collected and used to deliver critical functionality. The current definition is so broad and vague that it creates incentives for operators to claim that

---

with COPPA, meaning you must obtain consent from all parents or guardians whose children under 13 will be accessing the Services.") [https://perma.cc/SDF7-MBSB]; *see also, e.g.*, *Privacy Policy*, EDULASTIC (May 30, 2019), https://edulastic.com/privacy-policy/ ("If you are a school, district, or teacher, you represent and warrant that you are solely responsible for complying with COPPA, meaning that you must obtain advance written consent from all parents or guardians whose children under 13 will be accessing the Services.") [https://perma.cc/8NBJ-GBDV]; *Seesaw Privacy Policy*, SEESAW (Sept. 3, 2019), https://web.seesaw.me/privacy-policy ("We require that teachers or schools get parental consent before using Seesaw with children who are under the age when they can grant consent on their own.") [https://perma.cc/3HSS-MX7E]; *Terms of Service*, GOOSECHASE (Nov. 12, 2018), https://www.goosechase.com/terms-of-service/ ("[Organizer] shall have obtained all the requisite consents required under applicable law in respect of the use of the Service from the parents or guardians of such individuals.") [https://perma.cc/6BDZ-TS24].

[182] *See* Simon, *supra* note 37.

children's personal information—especially persistent identifiers—is used only for internal purposes even when it is not. The FTC should define time limitations on information retained for support purposes. The FTC should also clarify that permissible personalization of content applies only to personalization that is user-driven. Finally, the FTC should not expressly include advertising attribution under the definition of support for internal operations.

The current definition of support for internal operations is too broad and vague which enables operators to avoid or minimize their COPPA obligations. Clarifying this definition will require additional information about the changing marketplace that the FTC can obtain using its 6(b) authority. For example, what is meant by information necessary to "maintain or analyze the functioning of the Web site or online service"? How does cross-device tracking fit in? Does this include information retained indefinitely to assess ebbs and flows in app popularity across various geographic regions, and among specific demographic and ethnic groups? Does this or the use of information to "personalize content" permit an operator to collect information for the purpose of evaluating and improving the appeal of its content for children? Can information about a child be retained indefinitely for the purpose of capping the total number of times she will see a particular ad on various devices over a long period of time? Is there always a clear difference between contextual advertising (which is permitted under support for internal operations) and behavioral advertising (which is expressly excluded)? For example, Google's support page explaining "How ads are targeted to your site" offers explanations of "contextual targeting," "placement targeting," "personalized targeting," and "run of network targeting."[183] Which of these practices constitute behavioral advertising and thus are excluded from the definition of support for internal operations? Does personalized distribution of branded content that is not labeled as an advertisement constitute permissible "personalization" or

[183] Advertisers may not always offer services that neatly align with these categories. For example, Google's support page explaining "How ads are targeted to your site" offers explanations of "contextual targeting," "placement targeting," "personalized targeting," and "run of network targeting." *How Ads Are Targeted to Your Site*, GOOGLE SUPPORT, https://support.google.com/adsense/answer/9713?hl=en [https://perma.cc/2KAU-SJRT?type=image].

impermissible "behavioral advertising" under support for internal operations? Recent changes to contextual marketing techniques appear to have further blurred the line between behavioral and contextual advertising.[184]

Without greater clarity, operators are likely to adopt a very broad reading of support for internal operations. This is particularly the case because when persistent identifiers are collected to provide "support for the internal operations of the Web site or online service," the operator is not even required to disclose the information collection.[185] This renders it much more difficult for interested users even to detect that excessive information collection and use is taking place, let alone to contest it.

For example, ABCmouse, a widely-used early learning program that targets children between the ages of two and eight years old, contains very ambiguous language when describing its practice of collecting a child's information for the purpose of supporting "internal operations." Its privacy policy states, "The information collected through these technical methods on the child-directed portions of the Services are used only to support the internal operations of the Services."[186] However, because ABCmouse never identifies what those internal operations are, parents are left wondering exactly how broad the scope of this collection really is. Quizlet, another very popular ed tech service, similarly utilizes a vague "internal operations" justification for collecting information from child-users. Quizlet's privacy policy states, "Where necessary, we use restricted versions of our third-party services (for example, Google Analytics) that limit data sharing and tracking on areas of our site and mobile apps that are accessed by children to support our internal operations."[187] However, Quizlet never discloses what those internal operations include.[188] Vague references to "internal

---

[184] Paul Sawers, *YouTube Taps Machine Learning to Serve the Best Contextual Ads for Each User*, VENTUREBEAT (Sept. 23, 2019, 3:40 AM), https://venturebeat.com/2019/09/23/youtube-taps-machine-learning-to-serve-the-best-contextual-ads-for-each-user/ [https://perma.cc/32WS-8ALY].
[185] *See* 16 C.F.R. § 312.5(c)(7) (2019).
[186] *Privacy Policy*, ABCMOUSE (July 16, 2019), https://www.abcmouse.com/privacy [https://perma.cc/9XSF-6YWX].
[187] *Privacy Policy*, QUIZLET, https://quizlet.com/privacy [https://perma.cc/XZ59-JPXE].
[188] *See COPPA Policy*, QUIZALIZE (May 18, 2018), https://www.zzish.com/COPPA-policy ("We may also collect IP address, device identifier or a similar unique identifier from users of our App and Site, including children; we only use such identifiers *to support the internal operations of our Site and App* and we

operations" are no substitute for meaningful compliance that would inform parents about actual data collection and use practices.

If the FTC decides to update the definition of "support for the internal operations of the Web site or online service," it should narrow the definition to deliver greater clarity and specificity. First, the FTC should define time limitations on information retained for support purposes. For example, a persistent identifier collected to facilitate website analytics should only be considered to fall within the support for internal operations exception when it is retained for a brief period of time (e.g. one session, one day, or one week) and then deleted. Without a time limitation, this exception could be read to extend to persistent cookies, some of which do not expire for several years, and may be used to track users' behavior across the web for the entire lifespan of the cookie.

The FTC also should clarify that personalization designed to maximize user engagement is not permitted under the exception. At present the definition of support for internal operations extends to information collected to "personalize the content" on a site or service.[189] The FTC's Frequently Asked Questions document regarding the COPPA Rule explains: "The inclusion of personalization within the definition of support for internal operations was intended to permit operators to maintain *user driven* preferences, such as game scores, or character choices in virtual worlds."[190] But the FTC must clarify that many personalization methods popular today are not consistent with maintaining users' preferences. Other types of personalization, such as personalization designed to maximize user engagement, thereby keeping children on a platform as long as possible, should therefore not be considered to fall within the definition of support for internal operations. Personalization that is not driven by users is not integral to a service, and parents have a right to know, and a right to decline, when a site or service wishes to use their child's information for that purpose.

---

do not use such identifiers to collect information about the child outside of our Site or App.") (emphasis added) [https://perma.cc/6LEY-CK2Y].

[189] 16 C.F.R. § 312.2.

[190] *Complying with COPPA: Frequently Asked Questions*, *supra* note 91 (Question I.8) (emphasis added).

Finally, and especially in light of the overbreadth of the current definition of support for internal operations, the FTC should not further expand the definition by expressly including advertising attribution. To accurately attribute the purchasing behavior of a child or her family to a particular ad or campaign, operators would need to conduct detailed tracking of discrete individuals' behavior across websites and services as well as devices. In the words of one advertising executive,

> Attribution and identity are book ends in our opinion. Your attribution with bad identity leads to fragmented or bad attribution, whether Dave is one person or two, if you see him as two, then you're going to get double counts on what works or half counts where it did and didn't work. For us, identity and attribution go hand-in-hand.[191]

The FTC should not create a carve-out from verifiable parental consent for advertisers that wish to identify and track individual children for the purpose of accurate ad attribution.[192]

In accordance with the goals of COPPA, the FTC should be working to decrease, rather than increase, the data gathered from children via commercial content—and to increase, rather than decrease, parents' awareness of marketers' collecting their children's information. The purpose of advertising attribution is to assess the effectiveness of sponsored and other content so that it can be made more appealing, more persuasive, potentially more manipulative, and even more addictive to children.

---

[191] Carl Madaffari, Senior Vice President, Database Solutions at Epsilon-Conversant, Remarks at Back to Basics: Understanding Identity, Data, Attribution and Platforms (Feb. 12, 2019), https://www.conversantmedia.com/resources/back-to-basics-adweek-video (transcript) [https://perma.cc/GS8K-U2EU].

[192] There is some evidence that advertisers may presently believe that attribution is permissible. For example, Disney's "Luminate" advertising suite offers a range of products, including attribution, "across Disney's brands including ABC, ESPN, Freeform and the Disney Channels." *See* Ben Munson, *Disney Intros Luminate, A New Data-Driven Targeted Ad Platform*, FIERCEVIDEO (May 11, 2018), https://www.fiercevideo.com/video/disney-intros-luminate-a-new-data-driven-targeted-ad-product [https://perma.cc/FY7V-YRLZ]. But as even the IAB acknowledges, attribution does not currently fall under the definition of support for internal operations, which is quite limited in scope. *See* INTERACTIVE ADVERT. BUREAU, *supra* note 8 at 17.

The FTC noted back in 1998 that "the Web offers an easy way to collect large amounts of detailed marketing data from and about children," and argued that children's privacy legislation would "ensure that parents have knowledge of, and control over, the collection of information from their children."[193] Consistent with its concerns in 1998, the FTC should not extend an exception over this marketing-related use of children's information, thereby hiding collection of children's information for advertising attribution purposes from parents who may well be concerned about excessive and harmful advertising.

E. The FTC should expand the definition of "personal information"

The FTC asks if the COPPA definition of "personal information" should be expanded.[194] In the event the FTC considers substantive modifications to the COPPA Rule, it should add types of information to the list of enumerated categories of "personal information" named in the Rule. COPPA extends the definition of "personal information" to "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[195] Accordingly, the Commission should expand "personal information" to include additional types of information that companies collect that can be used to contact a specific individual:

- **Genetic data, fingerprints, retinal patterns, and other biometric data.** Children indisputably can be identified based on information collected from their bodies, including these and other categories of biometric data.[196] At the same time, genetic fingerprinting has become much faster and cheaper than it once was, and surfaces and cameras that capture fingerprints and retinal patterns have become

[193] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS iii–iv, 4 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/M7HL-WU9R].
[194] 2019 COPPA RFC, *supra* note 70 at 35,844.
[195] 15 C.F.R. § 6501(8)(F) (2012).
[196] *See* Heather Kelly, *Fingerprints and Face Scans Are the Future of Smartphones. These Holdouts Refuse to Use Them*, WASH. POST (Nov. 15, 2019), https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them/ [https://perma.cc/6DFT-2GWY].

more sophisticated. As a result, the collection and use of genetic and biometric data are on the rise. For example, consumer products increasingly use biometrics to identify and authenticate users.[197] While there are some types of personal information that people may be able to change to help protect their own privacy, biometrics do not change. Genetic data, fingerprints, retinal patterns, and other biometric data captured today may be used to identify and contact specific children for the rest of their lives. The COPPA Rule should be revised to clearly extend protections to biometric data.

- **Personal information that is inferred about, but not directly collected from, children.**[198] The Rule covers a number of categories of private information regarding children when collected directly from the children themselves, but it is less clear whether the Rule protects those same types of information when they are inferred from other types of information, rather than directly collected from a child. For example, non-geolocation ambient data collected by a mobile device operating system does not constitute an independently enumerated category of personal information under the current iteration of the COPPA Rule. But a savvy analyst could use data collected by a mobile device to infer specific geolocation or other details that clearly *would* fall under the COPPA Rule definition of personal information.[199] This is particularly the case as mobile and wearable

[197] *Id.* ("Avoiding commercial biometric security could be an increasingly difficult feat in the future. Smartphone makers are sticking with the tech and say it is faster and safer to use than a passcode alone.").

[198] This also includes "personas." *See* Oliver Walker, *Analyzing Personas Using Advanced Segments*, ONLINE-BEHAVIOR (July 11, 2012), https://online-behavior.com/targeting/personas-analytics (explaining that web operators can obtain real insights from persona profiles) [https://perma.cc/CYG5-KLNM]; *see also Persona-Based Segmentation Using Web Analytics Data*, SMART INSIGHTS (July 16, 2012), https://www.smartinsights.com/persuasion-marketing/marketing-personas/persona-based-segmentation-using-web-analytics-data/ ("With persona-based segmentation, you get rich, powerful, data-driven segments that lend themselves to effective approaches to testing and suggest to marketers rich ways to use the data.") [https://perma.cc/B4UL-TP98].

[199] For example, researchers have demonstrated that companies have been able to infer the location of users who had turned off location services by collecting and analyzing information about nearby cell towers or WiFi nodes. *See* Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, QUARTZ, (Nov. 21, 2017), https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ [https://perma.cc/R7GG-J5X6]. In the FTC's own

devices proliferate, data available regarding children's activities on- and offline grows richer, and analytical capabilities become more powerful. The COPPA Rule should be revised to extend protections to inferred data.

F. The FTC should develop new COPPA Rule provisions implementing neglected sections of the statute

The FTC should develop new provisions of the COPPA Rule fully implementing neglected sections of the statute. COPPA has long been treated as a notice and comment framework by the FTC, but it is much more. COPPA also requires the FTC to promulgate regulations that 1) prohibit conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity and 2) require operators to protect the confidentiality, security, and integrity of personal information collected from children. To better protect children's privacy, the FTC should refocus its efforts under COPPA on these underutilized provisions of COPPA.

The relevant underutilized provisions of COPPA discussed here state:

> (1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate under section 553 of title 5, United States Code, regulations that—
>
> . . . .
>
> (C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
>
> (D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality,

---

case against InMobi, InMobi had circumvented users' location privacy elections by using WiFi networks to infer users' location. Nithan Sannappa & Lorrie Cranor, *A Deep Dive into Mobile App Location Privacy Following the Inmobi Settlement*, FED. TRADE COMM'N: TECH@FTC (Aug. 9, 2016), https:// www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy- following-inmobi-settlement [https://perma.cc/FSN8-RN3E].

security, and integrity of personal information collected from children.[200]

1. The FTC should adopt Rules prohibiting the collection of more children's information than is "reasonably necessary" to provide an online service

The current version of the COPPA Rule merely restates the provision of the statute that prohibits conditioning a child's participation on the disclosure of more information than is reasonably necessary. If the FTC is going to consider updating the COPPA Rule, it should expand and elaborate on this obligation.

Restricting information collection to that which is "reasonably necessary" to provide an online service is not only required by the statute, it is also consistent with the classic privacy principles of collection limitation, purpose specification, and use limitation. These principles hold, generally, that there should be limits to the collection of personal data, that the purposes for which personal data are collected should be specified at or before the time of data collection, and that personal data should not be used or disclosed for purposes other than those specified in advance.

The restatement of the statutory provision in the Rule does not go far enough. It provides no indication as to how one might determine whether information is "reasonably necessary" to provide an online service. It also does not articulate the process that an operator should undertake to ensure that it is not requiring children to disclose more information than is reasonably necessary.

The FTC has been tasked with promulgating regulations implementing this section of the statute and should do so. This would deliver greater clarity regarding operators' obligations under this section of COPPA, and would also empower law enforcement and parents to better challenge websites, apps, and services that appear to be collecting children's information in excess of what is necessary.

[200] Children's Online Privacy and Protection Act of 1998, 15 U.S.C. §§ 6501–05 (2012).

2. The FTC should adopt Rules requiring operators of child-directed sites and services to protect the confidentiality of children's information

The current version of the COPPA Rule restates the provision of the law regarding confidentiality, security, and integrity of personal information, and adds some small sections explaining that operators also must ensure third parties are capable of abiding by the requirement, and that operators must delete children's information once it is no longer necessary. But the current iteration of the Rule does not elaborate further on what constitutes "reasonable procedures to protect the confidentiality, security, and integrity" of children's information. If the FTC updates the Rule, it should expand on operators' obligations under this section of the statute.

In particular, it is unclear what operators must do to protect the "confidentiality" of children's information. The FTC brought an enforcement action against electronic toy maker VTech for inadequate security practices on its Kid Connect platform, but that action did not differentiate between "confidentiality, security, and integrity." Protection of confidentiality, however, is commonly understood to require strictly limiting the number of parties with whom sensitive information is shared. For example, according to the Computer Security Resource Center provided by NIST, the leading definition of confidentiality is "[p]reserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information," or alternatively, "[t]he property that sensitive information is not disclosed to unauthorized entities."[201] The FTC can and should adopt Rules explaining how operators can comply with this obligation. For example, it should be explicitly clear that the sharing of children's information with data aggregators and brokers, who are in the business of sharing information with additional third parties, is categorically prohibited.

[201] *Confidentiality*, COMPUT. SEC. RES. CTR., https://csrc.nist.gov/glossary/term/confidentiality [https://perma.cc/WV6D-6H88].

Conclusion

In light of the dramatic changes that have taken place in digital advertising and ed tech in the last several years, Commenters reiterate the call for the FTC to use its 6(b) authority to thoroughly study how information about children is collected and used before it adopts any privacy-related Rule or policy change.

But even in the absence of 6(b) studies, sufficient public information exists to know that children's privacy threats and related harms are on the rise and current enforcement of COPPA is insufficient to protect children online.

In light of this information:

- the FTC should not permit general audience platforms to rebut the presumption that the users of child-directed portions of their services are children;
- the FTC should retain its enforcement policy statement for voice recordings;
- the FTC should strengthen protections for student privacy;
- the FTC should rein in the definition of "support for the internal operations of the Web site or online service";
- the FTC should expand the definition of "personal information"; and
- the FTC should develop new COPPA Rule provisions implementing neglected sections of the statute.

In addition, the FTC must focus greater resources on enforcing the COPPA Rule. The greatest problem with COPPA is that the risk of enforcement is so low that many companies do not bother to comply. The easiest way to better protect children's privacy is thus to more fully enforce the existing COPPA Rule.

Commenters urge the FTC to conduct the necessary children's privacy studies and, ultimately, adopt only those COPPA Rule changes that will lead to better protection for children's privacy on- and offline, in homes, and in schools.

Respectfully submitted,

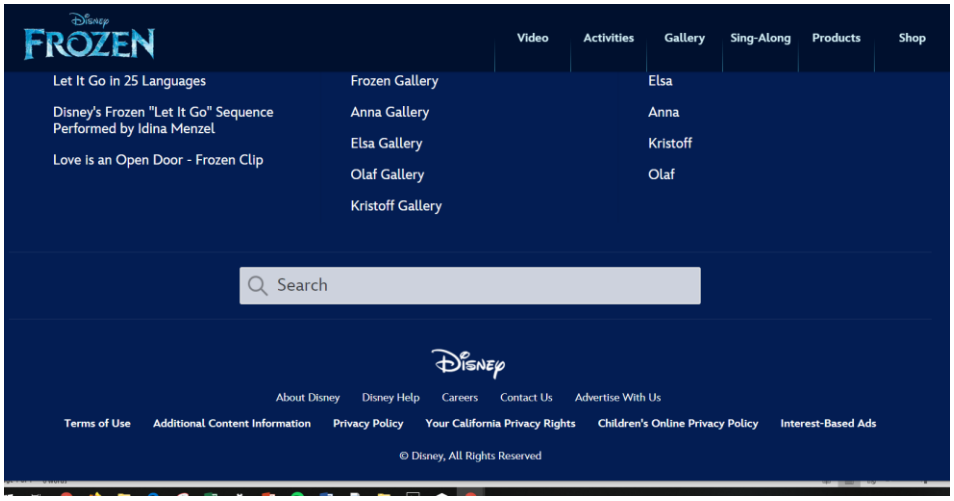
/s/_____

Laura Moy
Angela J. Campbell
Lindsey Barrett*
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue NW, Room 312
Washington, DC 20001
(202) 662-9535

Counsel for CDD and CCFC

* These comments were drafted with considerable and able assistance from Harsimar Dhanoa and Jonathan Greengarden, law students in the Institute for Public Representation Communications & Technology Clinic.

Exhibit A: Screen Shots Showing Steps to Find the Privo Seal on Disney's Frozen Website



Screen shot of the bottom of the home page of frozen.disney.com does not display a safe harbor seal.

CHILDREN'S PRIVACY POLICY

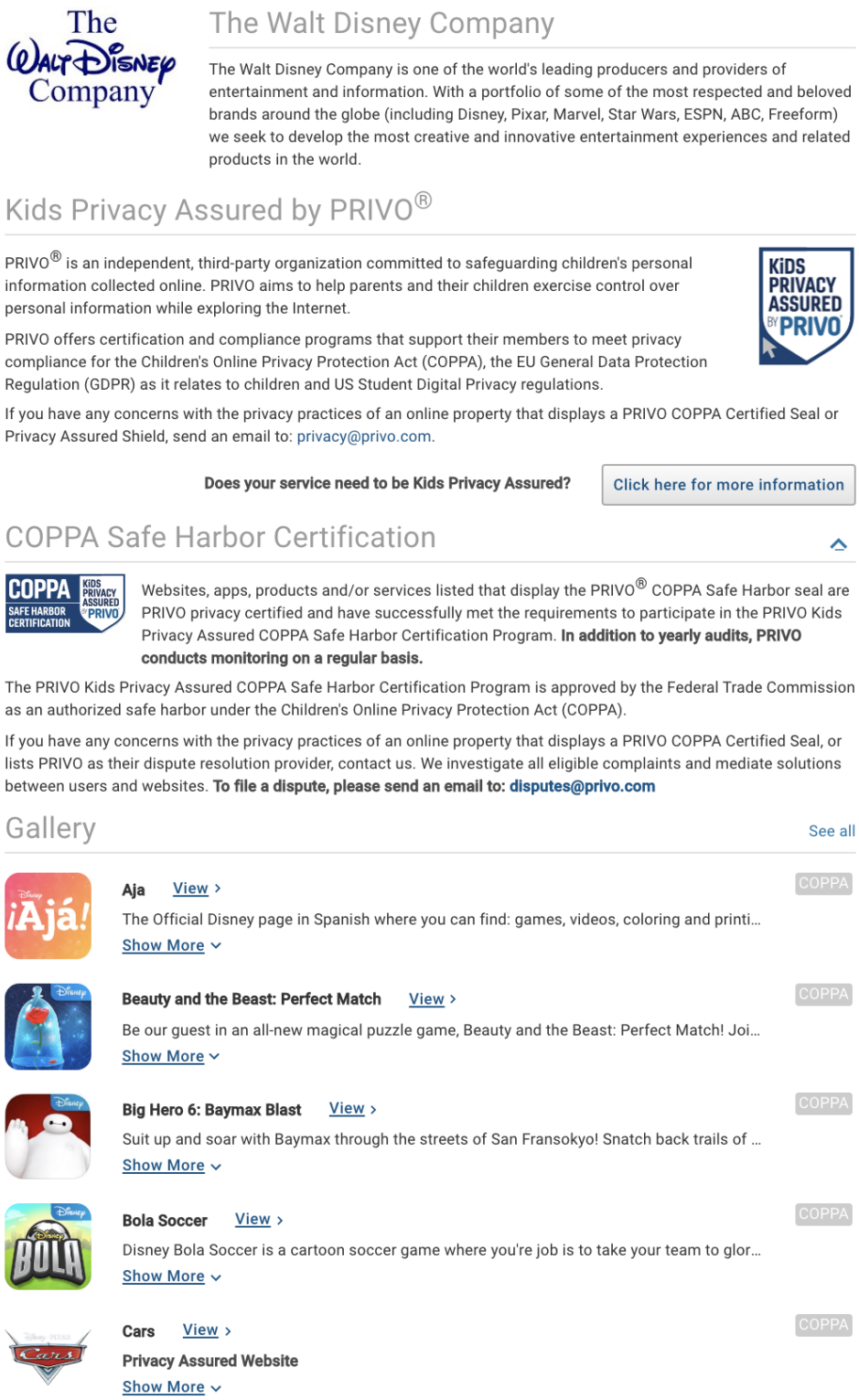
Updated: 05/13/2019

COPPA SAFE HARBOR CERTIFICATION — KIDS PRIVACY ASSURED BY PRIVO

The Walt Disney Family of Companies ("TWDC") is committed to protecting the privacy of children who use our sites and applications. This Children's Online Privacy Policy explains our information collection, disclosure, and parental consent practices with respect to information provided by children under the age of 13 ("child" or "children"), and uses terms that are defined in our general PRIVACY POLICY. This policy is in accordance with the U.S. Children's Online Privacy Protection Act ("COPPA"), and outlines our practices in the United States and Latin America regarding children's personal information. For more information about COPPA and general tips about protecting children's online privacy, please visit ONGUARD ONLINE.

The Walt Disney Company's Child Directed Websites and Mobile Apps are included in PRIVO's Kids Privacy Assured COPPA Safe Harbor Certification Program ("the Program"). The Program certification applies to the digital properties listed on the validation page that is viewable by clicking on the PRIVO seal. PRIVO is an independent, third-party organization committed to safeguarding children's personal information collected online. PRIVO aims to help parents and their children exercise control over personal information while exploring the Internet. The PRIVO COPPA certification seal posted on this page indicates The Walt Disney Company has established COPPA compliant privacy practices and has agreed to submit to PRIVO's oversight and consumer dispute resolution process. If you have questions or concerns about our privacy practices, please contact us at (877) 466-6669 or PRIVACYCONTACT@DISNEY.COM. If you have further concerns after you have contacted us, you can contact PRIVO directly at PRIVACY@PRIVO.COM.

Clicking on "Children's Online Privacy" goes to this page.



The Walt Disney Company

The Walt Disney Company is one of the world's leading producers and providers of entertainment and information. With a portfolio of some of the most respected and beloved brands around the globe (including Disney, Pixar, Marvel, Star Wars, ESPN, ABC, Freeform) we seek to develop the most creative and innovative entertainment experiences and related products in the world.

Kids Privacy Assured by PRIVO®

PRIVO® is an independent, third-party organization committed to safeguarding children's personal information collected online. PRIVO aims to help parents and their children exercise control over personal information while exploring the Internet.

PRIVO offers certification and compliance programs that support their members to meet privacy compliance for the Children's Online Privacy Protection Act (COPPA), the EU General Data Protection Regulation (GDPR) as it relates to children and US Student Digital Privacy regulations.

If you have any concerns with the privacy practices of an online property that displays a PRIVO COPPA Certified Seal or Privacy Assured Shield, send an email to: privacy@privo.com.

Does your service need to be Kids Privacy Assured? Click here for more information

COPPA Safe Harbor Certification

Websites, apps, products and/or services listed that display the PRIVO® COPPA Safe Harbor seal are PRIVO privacy certified and have successfully met the requirements to participate in the PRIVO Kids Privacy Assured COPPA Safe Harbor Certification Program. **In addition to yearly audits, PRIVO conducts monitoring on a regular basis.**

The PRIVO Kids Privacy Assured COPPA Safe Harbor Certification Program is approved by the Federal Trade Commission as an authorized safe harbor under the Children's Online Privacy Protection Act (COPPA).

If you have any concerns with the privacy practices of an online property that displays a PRIVO COPPA Certified Seal, or lists PRIVO as their dispute resolution provider, contact us. We investigate all eligible complaints and mediate solutions between users and websites. **To file a dispute, please send an email to: disputes@privo.com**

Gallery

See all

Aja View ›
The Official Disney page in Spanish where you can find: games, videos, coloring and printi...
Show More
COPPA

Beauty and the Beast: Perfect Match View ›
Be our guest in an all-new magical puzzle game, Beauty and the Beast: Perfect Match! Joi...
Show More
COPPA

Big Hero 6: Baymax Blast View ›
Suit up and soar with Baymax through the streets of San Fransokyo! Snatch back trails of ...
Show More
COPPA

Bola Soccer View ›
Disney Bola Soccer is a cartoon soccer game where you're job is to take your team to glor...
Show More
COPPA

Cars View ›
Privacy Assured Website
Show More
COPPA

Clicking on the PRIVO COPPA seal takes one to a list of over 75 covered properties.

One must scroll down the list to find the website of interest.

Exhibit B: Seals Displayed by COPPA Safe Harbors

Aristotle

Children's Advertising Review Unit (CARU)

Entertainment Software Rating Board (ESRB)

iKeepSafe

kidSAFE

Privacy Vaults Online, Inc. (PRIVO)

TRUSTe