December 11, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: COPPA Rule Review, 16 CFR part 312, Project No. P195404

Consumer Reports[1] writes in response to the Federal Trade Commission's (FTC) request for comment on potential updates to the COPPA Rule. Children's privacy continues to require protection by the FTC in light of well-documented evidence that compliance with the Children's Online Privacy Protection Act (COPPA) is uneven among apps, connected toys, and online services. While we suggest some improvements to the 2013 Rule, we also urge the Commission to use its authority[2] under 6(b) of the Federal Trade Commission Act[3] to fully understand how kids' personal information is treated before the 2013 Rule can be modified, in order to ensure that children and their data are protected. Regardless of any future changes to the Rule, the FTC must fully enforce the current requirements of COPPA *now* in order to ensure that companies are incentivized to comply with the law and that children's personal information is being treated correctly.

Furthermore, we urge the Commission to not roll back protections for children in response to urging from industry. Nationwide, states are considering passing strong protections for all consumers' digital information. At the federal level, Congress has held many hearings on the issue,

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For 83 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] *31 Advocacy Groups Call on FTC to Investigate Children's Digital Media Marketplace Before Proposing any Changes to Privacy Protections for Children*, CONSUMER REPORTS (Dec. 5, 2019), https://advocacy.consumerreports.org/research/coppa-6b-study-joint-letter/; *see also Leading child advocacy, health, and privacy groups call on FTC to investigate children's digital media marketplace before Proposing any changes to privacy protections for children*, CTR. FOR DIGITAL DEMOCRACY (Dec. 5, 2019), https://www.democraticmedia.org/article/leading-child-advocacy-health-and-privacy-groups-call-ftc-investigate-childrens-digital-0.

[3] 15 U.S.C. § 46 (b).

and lawmakers on both sides of the aisle have introduced federal privacy bills. At a time when the country is working towards stronger privacy protections for all, the Commission should not consider weakening protections for some of the most vulnerable: children.

A. General Questions for Comment

1. Is there a continuing need for the Rule as currently promulgated? Why or why not?

As our comments in response to question A(3)(c) below demonstrate, there is a clear need for the Rule as currently promulgated due to the lack of compliance for many products in the app, connected devices, and online services marketplaces. What is lacking is enforcement from the Commission on these issues. Without effective enforcement of the COPPA rules, manufacturers, designers, and app developers will continue to contravene the law. As Josh Golin of Campaign for a Commercial-Free Childhood notes: "The biggest problem with COPPA is not the rules—it is the lack of enforcement..."[4] Unfortunately, the public also cannot rely on gatekeepers like Apple or Google to police the digital marketplace. As Serge Egelman said in an article highlighting the issues he and his fellow researchers found when they analyzed over five thousand apps (detailed in response to question A(3)(c)), "The platforms have an incentive to not investigate...The violations are rampant."[5] The "crisis of enforcement"[6] is demonstrated by our response to question A(3)(c).

In addition, a lot of kids' content suffers from issues beyond privacy and the FTC should be focused on policies to address those important issues. For example, Professor Jenny Radesky and her fellow researchers reviewed 135 apps that were directed at children under five years old in the Google Play Store. Her research found that some of the children's apps had pop-ups with disturbing imagery and ads that "no child could reasonably be expected to close out of."[7] In addition, at times the researchers found that if the advertisement was triggered, the ad would send present the player with even more ads.

Characters in the games also pressured their young users to make purchases; sometimes the character even cries if the player clicks away from the in-app store as in the Doctor Kids game published by Bubadu.[8] In some cases, the researchers also found that an in-app purchase was

---

[4] Tony Romm & Craig Timberg, *Federal regulators eye update to rules governing children's privacy and the Internet*, WASH. POST (July 18, 2019), https://www.washingtonpost.com/technology/2019/07/18/federal-regulators-eye-update-rules-governing-kids-privacy-internet/.

[5] Craig Timberg, *Sex, drugs, and self-harm: Where 20 years of child online protection law went wrong*, WASH. POST (June 13, 2019), https://www.washingtonpost.com/technology/2019/06/13/sex-drugs-self-harm-where-years-child-online-protection-law-went-wrong/.

[6] *Id*.

[7] Nellie Bowles, *Your Kid's Apps are Crammed with Ads*, N.Y. TIMES (Oct. 30, 2018), https://www.nytimes.com/2018/10/30/style/kids-study-apps-advertising.html.

[8] *Id*.

required to play the game at all.[9] Radesky and her co-authors also found that 95 percent of the apps they examined (129 apps in total) contained at least one form of advertising. The advertisements commonly were presented in videos that interrupted play (like pop-ups (35 percent), or ads you had to interact with to unlock play items (16 percent), distracting ads like banners across the screen (17 percent), or hidden ads with misleading symbols or camouflaged as gameplay items (seven percent)) or used commercial characters (42 percent of the total 135 apps).[10] The study notes that advertising was "significantly more prevalent in free apps" (100 percent versus 88 percent of paid apps).[11] But advertisements occurred at similar rates in apps that were marked as "educational" to ones that did not include that designation.[12] Radesky and her colleagues concluded that many of the apps they encountered "seemed to violate FTC rules around unfair and deceptive advertising."[13] Due to these concerns, we urge the FTC to focus on methods to stem such deceptive advertising and related issues.

a. Since the Rule was issued, have changes in technology, industry, or economic conditions affected the need for or effectiveness of the Rule?

Since 2013, there has only been an increase in the number of connected products directed at children and in the amount of time children spend on these devices. In addition, more homes are connected and have access to a connected mobile device that the children can use.[14] For these

---

[9] For instance, in the app Strawberry Shortcake Bake Shop the researcher found that an in-app purchase was required to play one part of the game:

> In the app, players were presented with 2 options for tools: a free standard tool and a locked (in-app purchase) modern tool, and Strawberry Shortcake always states how much better the locked tool is. In this case, the researcher purchased locked tools in order to compare ease of gameplay between free and purchased items and found that purchased tools were notably faster. For example, while cutting a cake with the free wooden knife, the player needed to move the knife in and out across the cake and it was difficult to finish; however, with the purchased metal knife, the cake was cut in 1 quick swipe. Moreover, the storyline of the Strawberry Shortcake Bake Shop involves the player creating a dessert for 1 of Strawberry Shortcake's friends. When an order is successfully filled, the player receives a star; however, after a few levels, the player must make an in-app purchase in order to fulfill orders. If the player does not make a purchase and makes the wrong dessert, Strawberry Shortcake comments, "we didn't fill this order, so this dessert can be just for you."

Jenny Radesky, MD, Yung-Ju Chang, PhD, et al., *Advertising in Young Children's Apps: A Content Analysis*, 40(1) J. OF DEVELOPMENTAL & BEHAVIORAL PEDIATRICS, 32-39, 36 (2018), *available at* http://childrenstech.com/files/2018/11/Advertising_in_Young_Children_s_Apps___A_Content.99257.pdf [hereinafter *Advertising in Young Children's Apps*].

[10] *Id*; see also Jennifer Valentino-DeVries, et al., *How Game Apps That Captivate Children Have Been Collecting Their Data*, N.Y. Times (Sept. 12, 2018), https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html.

[11] *Advertising in Young Children's Apps supra* note 9.

[12] *Id*.

[13] Nellie Bowles, *Your Kid's Apps are Crammed with Ads*, N.Y.Times (Oct. 30, 2018), https://www.nytimes.com/2018/10/30/style/kids-study-apps-advertising.html.

[14] *The Common Sense Census: Media Use by Kids Age Zero to Eight*, COMMON SENSE MEDIA (2017),

reasons, there is more reason than ever for strong privacy protections for children and their personal information. And, as we note in response to A(3)(c), researchers and advocates have documented issues with connected products and services for children, highlighting the dangers that connected products pose to the security of children's information.[15]

Consumer spending on connected products (commonly also referred to as IoT for "internet of things") has only grown over the intervening years, with children's products also seeing a corresponding uptick. In 2013, there were 1.9 billion connected devices.[16] By contrast, there are over 26 billion connected devices in use today.[17] A report from Business Wire found that smart toys will represent an 18 billion market by 2023, with spending on kid's IoT devices at 6 billion in 2018. The report notes that the increase in the market will "primarily be driven by the growing popularity of smartphone-connected toys and related in-app purchases, which are projected to grow by 69% annually over the next 5 years."[18] As Credence Research notes, app-enabled mechanical toys and drones occupied the biggest market share of all connected kids products in 2017.[19] Although connected devices pose security problems for their users generally, the US Federal Bureau of Investigation issued a warning in 2017 to parents about the risks that IoT products pose to children.[20] Specifically, the FBI's statement warns:

> These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed...Personal information (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses/IPs. The exposure of such information could create opportunities for child identity fraud. Additionally, the potential misuse of sensitive data such as GPS

---

https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_zerotoeight_fullreport_release_2.pdf [hereinafter *2017 Common Sense Census*].

[15] *See* Bree Fowler, *Gifts That Snoop? The Internet of Things is Wrapped in Privacy Concerns*, CONSUMER REPORTS (Dec. 13, 2017), https://www.consumerreports.org/internet-of-things/gifts-that-snoop-internet-of-things-privacy-concerns/.

[16] Emily Adler, *Here's Why 'The Internet of Things' Will be Huge, and Drive Tremendous Value for People and Businesses*, BUS. INSIDER (Dec. 7, 2013), https://www.businessinsider.com/growth-in-the-internet-of-things-2013-10.

[17] Jaleesa Bustamante, *IoT Statistics*, IPROPERTY MGMT., https://ipropertymanagement.com/iot-statistics/ (last visited Dec. 9, 2019).

[18] Sam Smith, *Juniper Research: Smart Toy Revenues to Grow by Almost 200% from 2018 to $18 Billion by 2023*, BUS. WIRE (May 8, 2018), https://www.businesswire.com/news/home/20180508005050/en/Juniper-Research-Smart-Toy-Revenues-Grow-200.

[19] *Connected Toys Market 2018-2026 with Data by Product Types, Applications, and Regional Analysis*, REUTERS (Jan. 31, 2019), https://www.reuters.com/brandfeatures/venture-capital/article?id=79596.

[20] *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*, US FED. BUREAU OF INVESTIGATION (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx.

> location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks.
>
> Consumers should examine toy company user agreement disclosures and privacy practices, and should know where their family's personal data is sent and stored, including if it's sent to third-party services. Security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use.[21]

Due to the increase in connected products generally, and children's products specifically, there is only heightened need for the COPPA rules in the coming years. In addition, although the connected product marketplace demonstrates the need for the COPPA rules, the increase in child-directed apps also show that the COPPA rules, and robust enforcement of those rules, will be required in the coming years. In April 2013, there were an estimated 850,000 apps and as of June 2017 that number had increased to 2.7 million.[22] Many of these apps are also directed at children or are designed to work in conjunction with a connected-device for children.

Furthermore, the amount of time children spend on these devices has only gone up in the years since 2013. In 2013, children eight years old and younger spent 15 minutes a day, on average, on a mobile device.[23] By 2017, this time had more than doubled to about 48 minutes per day, on average.[24] In the last two years, it is likely that this number has only risen. Likewise, in 2013 only seven percent of children eight and younger had their own personal mobile device, but by 2017 this proportion had risen to 42 percent.[25] In addition, a report from Common Sense Media found that 98 percent of households with children eight and under, no matter their socioeconomic status, now have access to a mobile device, such as a tablet or smartphone.[26] By comparison, in 2013 only 52 percent of households with young children had access to a mobile device.[27]

As the Common Sense Media report also notes, while children still spend most of their screen time watching TV, mobile device viewership among young children (eight years and younger) has rapidly risen from five minutes a day in 2011 to 15 minutes in 2013 and to 48 minutes a day in 2017.[28] Meanwhile, time spent watching TV declined 11 minutes over the same period.[29] Finally,

---

[21] *Id*.

[22] *Number of Available Applications in the Google Play Store*, STATISTA (Sept. 2019), https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/.

[23] *2017 Common Sense Census supra* note 14.

[24] *Id*.

[25] *Id*.

[26] *Id*.

[27] *The Common Sense Census: Media Use by Kids Age Zero to Eight*, COMMON SENSE MEDIA (2013), https://www.commonsensemedia.org/file/zero-to-eight-2013pdf-0/download [hereinafter *2013 Common Sense Census*].

[28] *2017 Common Sense Census supra* note 14.

[29] *Id*.

home connectivity has grown over the same time period, with high speed internet access rising from 92 percent in 2011 to 96 percent in 2017 in high income homes. The increase was more dramatic for lower-income homes, from 42 percent in 2011 to 74 percent in 2017.[30]

Increased screen time for young children highlights not only the ongoing concerns about the content children are viewing (as we discussed in response to question A(1)) and the increased amount of data collection that is occurring while children are using these mobile devices (as we discuss in response to question A(3)(c)), but also harms that can come to children as a result of this time spent on devices. Three years ago, in 2016, the American Academy of Pediatrics (AAP) released guidelines recommending limiting screen time for children.[31] Specifically, the AAP recommended that children in the 18-24 month range should only be introduced to "high-quality programming" such as "content offered by Sesame Workshop and PBS" and the parents should watch alongside children to help them understand.[32] For children 2-5 years old, parents should limit screen time to about one hour per day and for children six and over, parents should place limits on screen time in order to avoid impacting other essential life areas like sleep and physical activity.[33]

Reinforcing these guidelines, Jean M. Twenge and W. Keith Campbell's 2018 study shows that increased screen time (including traditional TV viewing) is associated with well-being for kids ranging in age from 2-17.[34] High users of screens were shown to exhibit less curiosity, emotional stability, and self-control.[35] Although these effects were seen to be more pronounced in adolescent users than younger users (which suggests the AAP should create guidelines for adolescent users as well as young ones), caregivers of preschool children reported that high users were more likely to "lose their temper, less likely to calm down when excited, and less likely to switch tasks without anxiety or anger."[36] The researchers also found that even for moderate preschool users there was a lower sense of well-being than with low users: "moderate users (vs. low users) were 30% more likely to not bounce back and 33% more likely to lose their temper."[37]

Despite these findings, what effects immersive exposure to screens and other connected services like social media will have on young children is still unknown. Experts are worried about the

---

[30] *Id*.

[31] *American Academy of Pediatrics Announces New Recommendations for Children's Media Use*, AMERICAN ACAD. OF PEDIATRICS (Oct. 21, 2016), https://www.aap.org/en-us/about-the-aap/aap-press-room/Pages/American-Academy-of-Pediatrics-Announces-New-Recommendations-for-Childrens-Media-Use.aspx.

[32] *Id*.

[33] *Id*.

[34] Jean M. Twenge & W. Keith Campbell, *Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study*, 12 PREVENTIVE MEDICINE REPORTS 271-283 (Dec. 2018), https://doi.org/10.1016/j.pmedr.2018.10.003.

[35] *Id*.

[36] *Id*.

[37] *Id*.

effects of online videos or headphone use will have on children's hearing,[38] whether dry eyes or nearsightedness is being exacerbated or caused by increased screen time,[39] and how harmful blue lights are on the retina.[40] Beyond the physical effects, it is unknown how technology and connected services are impacting children's ability to develop normally with regard to cognitive functions and emotional development. As Twenge and Campbell's study shows, screens can have a negative impact on children's emotional well-being. In addition, although it is unclear if any of the uses described here actually rise to the clinical level of compulsive or addictive use in a diagnostic sense,[41] a report from Commercial Free Childhood found that one in four of all children surveyed described feeling "addicted" to video games.[42]

For this reason, Consumer Reports supports the Children and Media Research Advancement Act,[43] which would authorize a National Institutes of Health research program on the effects of technology and media on children's physical, cognitive, and socio-emotional development.[44] We also urge the Commission to use their 6(b) authority to study the effects of these issues on children.

---

[38] Lindsey Konkel, *Noise, Hearing Loss, and Young Ears*, CONSUMER REPORTS (Mar. 3, 2017), https://www.consumerreports.org/health/noise-hearing-loss-and-young-ears/.

[39] Ayedsha Malik, *How Too Much Screen Time Affects Kids' Eyes*, CHILDREN'S HOSPITAL OF PHILA. (Dec. 11, 2018), https://www.chop.edu/news/health-tip/how-too-much-screen-time-affects-kids-eyes; *and, see*,

> For instance, a study of nearly 2,000 school-age children in Taiwan, published in June in the journal Ophthalmology, found that those who reported two or more hours of "cram school" (after-school or weekend prep courses typically involving close reading and studying) were more likely to be nearsighted than those who didn't do the extra academic work. The Taiwan research findings can't directly be applied to American children, Epley says, but other studies have found similar rises in nearsightedness here: "Even in this country, it's approaching 45 percent. A few decades ago it was down in the 20s," he says.
>
> While we don't know how much of the upswing in nearsightedness may be attributable to technology, he says, "it's becoming more clear that increased use of devices, as well as just increased reading, potentially at close proximity, without some regular break intervals, could lead to that increase."

Julia Calderone, *Is Technology Harming Kids' Eyes and Ears?*, CONSUMER REPORTS (Aug. 20, 2018), https://www.consumerreports.org/children-s-health/is-technology-harming-kids-eyes-and-ears/.

[40] Kasun Ratnayake, et al., *Blue Light Excited Retinal Intercepts Cellular Signaling*, 8 SCI. REPORTS (2018), https://www.nature.com/articles/s41598-018-28254-8; *Noise, Hearing Loss, and Young Ears*, *supra* note 38.

[41] Daniel Kardeefelt-Winther, *How Does the Time Children Spend Using Digital Technology Impact Their Mental Well-Being, Social Relationships and Physical Activity?*, UNICEF (Dec. 2017), https://www.unicef-irc.org/publications/pdf/Children-digital-technology-wellbeing.pdf

[42] *Facing the Screen Dilemma: Young Children, Technology and Early Education*, CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD (2012), https://commercialfreechildhood.org/wp-content/uploads/archive/facingthescreendilemma.pdf.

[43] *Senators Markey, Sasse, Blunt, Schatz, Bennet, and Collins, and Reps. Delaney and Budd Introduce Bipartisan, Bicameral Legislation to Study Impact of Technology and Media on Children*, SENATOR ED MARKEY (July 26, 2018), https://www.markey.senate.gov/news/press-releases/senators-markey-sasse-blunt-schatz-bennet-and-collins-and-reps-delaney-and-budd-introduce-bipartisan-bicameral-legislation-to-study-impact-of-technology-and-media-on-children.

[44] *S. 948 – Children and Media Research Advancement Act*, CONGRESS.GOV https://www.congress.gov/bill/110th-congress/senate-bill/948 (last visited Dec. 9, 2019).

b. What are the aggregate costs and benefits of the Rule?

The aggregate value of protecting children's privacy under the Rule is extremely hard to estimate or evaluate. It would likewise be hard to estimate the value society gets from ensuring that kids have some degree of seclusion and limiting the ability of advertisers to leverage data to influence developing minds. We encourage the Commission to not tether children's privacy protections to subjective assessments of the costs involved in protecting kids' privacy. Rather, privacy protections, like the COPPA Rule, should recognize that children, and their parents, will always have a privacy *interest* in data collection, use, retention, or sharing of their data because once private information is in the hands of another there is *always* a chance of some misuse. For example, data collected in the past could be publicly breached, accessed through mandatory legal process, or used for other secondary purposes.[45] In addition, the transparency that the COPPA rules require is helpful not only for parents as they assess which products and services their children should be using, but also for other groups like Consumer Reports who depend on such disclosures to audit, assess, and rate products for consumers.

2. What effect, if any, has the Rule had on children, parents, or other consumers?

a. Has the Rule benefited children, parents, or other consumers? If so, how?

Please see our response to question A(1)(b).

c. What changes, if any, should be made to the Rule to increase its benefits, consistent with the Act's requirements? What costs would these changes impose?

The Commission should more broadly interpret the "actual knowledge" standard within the rules to better protect children and the privacy of their personal information.[46] A wider understanding of what constitutes actual knowledge would be more in line with the settlement between the Federal Trade Commission and Google's YouTube[47] and serve to better enforce the law with regard to general audience sites. In addition, we suggest the Commission look to the CCPA for some guidance. Under the CCPA, "actual knowledge" also encompasses businesses "who willfully disregard a consumer's age."[48] In interpreting COPPA's actual knowledge standard, the

---

[45] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[46] *See Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015) https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[47] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[48] CCPA Sec. 1798.120(c).

Commission should include companies that exercise a willful disregard for a user's age.

3. What impact, if any, has the Rule had on operators?

c. What changes, if any, should be made to the Rule to reduce the costs imposed on operators, consistent with the Act's requirements? How would these changes affect the Rule's benefits?

Unfortunately, there are not enough costs under the current COPPA enforcement regime to effectively incentivize companies to comply with the rules. Although one of our strongest privacy laws in the United States is the Children's Online Privacy Protection Act, the enforcement of this law has not been similarly robust. While children's products and services abound in the marketplace, many of the connected products and services directed at children are not in compliance with the COPPA rules. In order for manufacturers and designers to be incentivized to comply with COPPA, the Commission must more effectively police the marketplace. And, as a recent study shows, not only is the free children's app marketplace rife with potential violations, self-regulatory "Safe Harbor" programs do not increase the likelihood that an app will be COPPA-compliant. Finally, the study also demonstrates that platform-specific rules such as the Google Play Store's Designed for Families program requirements likewise fail to effectively police the apps in their marketplace and thus do not serve as sufficient incentivization for app developers to comply with COPPA. In addition, children's connected physical products have also been shown to be violative of the COPPA rules, putting children's digital privacy and security, as well as their physical safety at some points, at risk.

Children's Apps

Narseeo Vallina-Rodriguez, Serge Egelman, and their co-authors published a study in 2018 finding that the majority of the 5,855 popular free children's apps were potentially in violation of COPPA due to their use of third-party software development kits (SDKs). Although many SDKS offer the ability to comply with COPPA by disabling tracking and behavioral advertising, their study suggests that a majority of the apps tested either do not make use of these configurations or "incorrectly propagate them across mediation SDKs."[49] Of the majority of apps that likely violate COPPA rules, the study found that: "5% of apps collect location data or contact data without verifiable parental consent; 19% of apps use SDKs whose terms explicitly prohibit their use in child-directed apps (likely due to prohibited user profiling and behavioral advertising); and when SDKs do provide configuration options for COPPA compliance, those options seem to be often ignored."[50] Vallina-Rodriguez, Egelman, and their co-authors also found that 37 apps, all developed

[49] Narseo Vallina-Rodriguez, Serge Egelman, et al., *Won't Someone Think of the Children? Examining COPPA Compliance at Scale*, 3 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES (PoPETS) 63-83, 63 (2018), *available at* https://blues.cs.berkeley.edu/wp-content/uploads/2018/04/popets-2018-0021.pdf [hereinafter *Examining COPPA Compliance*].

[50] *Id*. at 66.

by a company called BabyBus, did not access to the location of the device through the Android permissions system. Instead, these apps collected data that could be used to locate the user (like WiFi hotspot locations and their MAC addresses, as well as currently connected WiFi access point) and transmitted them to Chinese analytics firm TalkingData.[51] As the authors note, this kind of practice is well known to the FTC as the Commission reached a four-million-dollar settlement with InMobi for deceptively collecting location data in a similar fashion.[52]

The study also examined the level of COPPA compliance for apps that were certified to be in COPPA compliance under various self-regulatory "Safe Harbor" programs. Unfortunately, apps designed under various industry-implemented self-regulatory guidelines did not necessarily perform better. For the 237 apps certified by one of seven designated Safe Harbor organizations, the study found that:

> In terms of transmitting personal information without consent, there is little (or no) difference between the certified apps and the [apps available on the Google Play Store's Designed for Families program]. For instance, eight apps (3.5% of 237 vs. 3.1% of 5,855 in the full corpus) transmit GPS coordinates, 4 transmit email addresses (1.7% of 237 vs. 1.8% of 5,855 in the full corpus,) however none transmitted phone numbers. We also observed 15 apps (6.3% of 237 vs. 3.0% of 5,855) gathering MAC addresses or SSID of the WiFi hotspot, which could be used to surreptitiously track location. Overall, these observations corresponded to the 24 unique apps (10.1% of the 237; double the rate of the [5,855 in the full corpus]) transmitting PII (i.e., location data or contact information) without consent.[53]

These violations of COPPA are especially concerning because they demonstrate the ineffectiveness of a self-regulatory regime to police the apps they certify. In addition, since certified apps under one of the seven recognized Safe Harbor organizations are entitled more lenient enforcement procedures, a self-regulatory program that fails to perform allows app providers to gain protection from enforcement actions by just participating, thus white-washing bad apps under toothless self-regulatory systems. The authors conclude that the "privacy behaviors of the certified apps are not appreciably better than those of children's apps that have not been certified under Safe Harbor programs (and may be worse)."[54] And indeed, despite these concerning practices, these apps will be entitled to more lenient enforcement.

While these app practices likely violate the COPPA rules, they also violate the Google Play Store's Designing for Families (DFF) program requirements. The DFF program is an optional review

---

[51] *Id*. at 64.

[52] *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*, FED. TRADE COMM'N (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

[53] *Examining COPPA Compliance at Scale*, *supra* note 49 at 76.

[54] *Id*. at 76.

process run by Google which enables developers to list their apps under special family-friendly categories and sections of content specifically for children under 13. In order to participate, developers must "ensure that your app, including any APIs or SDKs that your app calls or uses, is compliant with withe U.S. Children's Online Privacy and Protection Act (COPPA), E.U. General Data Protection Regulation (GDPR), and any other applicable laws or regulations.[55]" Despite that requirement, the study found several Google Play Store policy violations, such as the use of SDKs that were prohibited from being used in children's apps (18.8 percent of 5,855 used these verboten SDKs). In addition, although Google prohibits apps from transmitting the Android Advertising ID along with other persistent identifiers, 39 percent of the apps analyzed were transmitting such persistent ID information. Therefore, although the Google Play Store DFF program guidelines prohibit such problematic practices; it is clear that in practice "there appears to not be any (or only limited) enforcement"[56] of the Play Store policies.

Connected Children's Toys

In December 2018, Consumer Reports published our review of connected children's toys, including a smartwatch for kids made by Kurio and CogniToy's Dino, a child-oriented smart speaker in a dinosaur's body.[57] Our testing of these two toys shows that the manufacturers of the devices may not be employing adequate data security under COPPA. The Kurio Smart Watch 2.0+ lets kids play games, take pictures and video, message their friends through a Bluetooth connection to their parent's phone, tracks the child's activity, and pair their device with a friend's watch. Consumer Reports's testing revealed that the watch stores some information without encryption, uses personal information to establish a Bluetooth connection by creating an identifier based on the first names of both the parent and child, along with their favorite colors, and lacks any way for the firmware to be updated in order to patch vulnerabilities or otherwise improve security. Since there is no encryption for some information on the watch and it is not possible to update the firmware of the device, it is possible that Kurio could be violating the duty to "employ adequate data security" practices under COPPA.[58]

In addition, the use of the first names and favorite colors of the child and parent to create Bluetooth identifier does not necessarily violate COPPA, it does allow for important details about both individuals to be sniffed and therefore could be used to gain a child's confidence, even if that is a remote concern. Kurio could have instead randomized the identifier in order to avoid this issue. Another product that we tested, CogniToy's Dino smart speaker, also lacked the ability to receive software updates. The developer of the product, Elemental Path, shut down due to lack of funding

---

[55] Families, GOOGLE PLAY, https://play.google.com/about/families/#!?zippy_activeEl=families-policy#families-policy (last visited Nov. 24, 2019).

[56] *Examining COPPA Compliance at Scale*, *supra* note 49 at 77.

[57] Bree Fowler, *Parents Should be Cautious with Connected Toys, CR Testing Shows*, CONSUMER REPORTS (Dec. 19, 2018), https://www.consumerreports.org/privacy/test-of-connected-toys-shows-parents-should-be-cautious/.

[58] *Complying with COPPA*, *supra* note 46.

in 2018 and thus the many Dino speakers that remain on the market will lack crucial security updates.[59] This means that consumers who have either of these devices in their homes will be interacting with devices that cannot receive software updates to protect against emerging security threats. Finally, our testing indicated that these toys generally had overpowered machinery in them that could be manipulated to gather more data than they should or than they were designed to, making children and their toy vulnerable to bad actors.

However, this is not the first time a children's smart watch has been found to be vulnerable. In October 2017, the Norwegian Consumer Council (NCC) tested four smartwatches for children, Gator 2, Tinitell, Viksfjord, and Xplora.[60] All of these watches function as wearable mobile phones that let parents use an app on their phone to track the location of their child as well as contact them. Unfortunately, two of the devices had flaws that would allow someone access to a children's real-time and historical location, personal details, and contact the child directly, all without the parents' knowledge.[61] In addition, data was transmitted and stored without encryption. Other flaws also rendered the child vulnerable, such as unreliable geo-fencing feature meant to notify parents when a child leaves a specified area and a malfunctioning SOS function alerting parents when a child is in distress.[62] Finally, some of the watches had not privacy policies at all while others had policies that lacked basic consumer protections, such as notifying users of changes in terms, allowing users to delete stored data, or seeking consent for data collection.[63] Since two of these smartwatches were available for purchase in the US, a coalition of consumer and privacy organizations sent the FTC a letter asking the Commission to investigate the threat the watches pose to children.[64] The NCC also referred the smartwatch manufacturers to the Norwegian Data Protection Authority and the Consumer Ombudsman for Norwegian Personal Data Act and Marketing Control Act violations.[65]

Despite coordinated transatlantic action on this issue, one of the smartwatch manufacturers told NCC that the security issues were fixed and released a new version of their watch. However, a

---

[59] As of this writing, the CogniToys Dino is for sale on Walmart.com and Amazon.com. *Cognitoys, Dino*, WALMART.COM, https://www.walmart.com/ip/Cognitoys-Dino/55332130 (last visited Nov. 24, 2019); *Cognitoys Dino*, AMAZON.COM, https://www.amazon.com/s?k=cognitoys+dino&hvadid=78271535590407&hvbmt=be&hvdev=c&hvqmt=e&tag=mh0b-20&ref=pd_sl_738c8wuqb5_e (last visited Nov. 24, 2019).

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

[61] *Center for Digital Democracy Press Release on Letter to FTC about Smartwatches*, CONSUMER REPORTS (Oct. 18, 2017), https://advocacy.consumerreports.org/press_release/center-for-digital-democracy-press-release-on-letter-to-ftc-about-smartwatches/.

[62] *Id*.

[63] *#WatchOut*, *supra* note 60.

[64] *Smart Watch FTC Letter*, CTR. FOR DIGITAL DEMOCRACY (Oct. 18, 2017), https://www.democraticmedia.org/sites/default/files/field/public-files/2017/smart_watch_ftc_letter_10.18_final.pdf.

[65] *Significant Security Flaws in Smartwatches for Children*, FOBRUKERRÅDET (NORWEGIAN CONSUMER COUNCIL) (Oct. 18, 2017), https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/.

subsequent technical test by NCC demonstrated that not only were some of the issues still present, but some additional issues had appeared.[66] In response, a coalition of consumer privacy groups, including Consumer Reports, renewed their call for the FTC to investigate these watches.[67]

Other insecure connect toys have also been brought to the attention of the Commission due to work by the NCC. In 2016, a coalition of consumer privacy groups filed a complaint about the My Friend Cayla and the i-Que Intelligent robot, dolls marketed to both young girls and boys that collect and use personal information from children in violation of COPPA and FRTC rules prohibiting unfair and deceptive practices.[68] The manufacturer of the dolls failed to take reasonable security measures to prevent unauthorized Bluetooth connections with the toys, meaning that anyone within a 15-meter radius could connect to the toys and listen to the child play with and/or talk with their toy.[69]

Despite these coordinated advocacy efforts, children's connected toy market is still a minefield of security and privacy issues for children and parents. As Tod Beardsley, researcher director at Rapid7, notes, "internet toys tend to be replete with default user names and passwords"[70] which makes them easy to hack and exploit. In addition, to the harm an unsecured product poses, many children's products also contain sensitive sensors that increases a child's risk and makes the data collected even more sensitive. As we note response to A(1)(a), the Federal Bureau of Investigation even published a warning about connected toys, advising: "These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities—including speech recognition and GPS options. These features could put the privacy and safety of children at risk."[71] For all the foregoing reasons, the Commission needs to strongly enforce the current protections under COPPA and the 2013 Rule in order to make sure the children's toy, app, and connected services marketplace is safe for children and their personal information.

8. Has the Rule affected the availability of websites or online services directed to children? If so, how?

a. Has the number or type of websites or online services directed to children changed since the Rule became effective? If so, how? Did the Rule cause these changes?

---

[66] *Consumers Union Renews Call for FTC to Investigate Reports of Security, Privacy Concerns with Smartwatches for Kids*, CONSUMER REPORTS (Dec. 7, 2017), https://advocacy.consumerreports.org/press_release/consumers-union-renews-call-for-ftc-to-investigate-reports-of-security-privacy-concerns-with-smartwatches-for-kids/.

[67] *Id*.

[68] *Internet-Connected Toys are Spying on Kids, Threatening Their Privacy and Security*, CONSUMER REPORTS (Dec. 6, 2016), https://advocacy.consumerreports.org/press_release/internet-connected-toys-are-spying-on-kids-threatening-their-privacy-and-security/.

[69] *#Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys*, FOBRUKERRÅDET (NORWEGIAN CONSUMER COUNCIL) (Dec. 6, 2016), https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws.

[70] Brian Barrett, *Don't Get Your Kid an Internet-Connected Toy*, WIRED (Dec. 20, 2017), https://www.wired.com/story/dont-gift-internet-connected-toys/.

[71] *Consumer Notice*, *supra* note 20.

Please see our response to question A(1)(a).

B. Definitions

9. Do the definitions set forth in § 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety?

The definition of personal information should be expanded to include biometric information and hashed identifiers in order to more fully protect children's personal information.

13. Should the Commission consider further revision to the definition of "Personal information"? Are there additional categories of information that should be expressly included in this definition, such as genetic data, fingerprints, retinal patterns, or other biometric data? What about personal information that is inferred about, but not directly collected from, children? What about other data that serve as proxies for personal information covered under this definition? Does this type of information permit the physical or online contacting of a specific individual?

The Commission should add biometric identifiers such as gait, retinal patterns, etc. to the definition of personal information. Hashed identifiers should also be included.

14. Should the definition of "Support for the internal operations of the website or online service" be modified? Are there practices in addition to behavioral targeting and profiling that should be expressly excluded from the definition? Should additional activities be expressly permitted under the definition? For example, should the definition expressly include advertising attribution? Advertising attribution is the method used to determine whether a particular advertisement led the user to take a particular step, such as downloading an app.

The definition of "Support for internal operations of the website or online service" should be modified to explicitly exclude advertising attribution. Companies should not have the right to track kids across different apps and service just to see which ads are effective. In addition, as research from Veronica Marotta, Vibhanshu Abhishek, and Alessandra Acquisti shows, targeted advertising does not actually help increase revenues. In their study on the revenue gained from publishers as a result of targeted advertising, their findings indicate: "when a user's cookie is available publishers' revenue increases only about 4%. This corresponds to an average increase of $0.00008 per advertisement."[72] If we allow such advertising for children, we will be sacrificing

[72] Veronica Marotta, Vibhanshu Abhishek, & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, https://weis2019.econinfosec.org/wp-

privacy for a negligible return. In addition, as Serge Egelman's research (detailed in response to question A(3)(c)) demonstrates, it is unclear if companies are complying the constraints already outlined under COPPA. Research like Egelman's shows that apps are frequently sending identifiers to tons of third parties, and it is not really clear or testable whether all this data is really necessary for internal operations. The Commission may pursue requiring companies that offer support for internal operations for kids' directed sites to certify compliance in some way. But the enforcement for this certification program should be more rigorous than those used in the app marketplace (as Serge Egelman's research also demonstrates, detailed in response to question A(3)(c)). The Commission should also explore effective ways of incentivizing first-party data for these reasons.

C. Notice

18. Section 312.4 of the Rule sets out the requirements for the content and delivery of operators' notices of their information practices with regard to children.

a. Are the requirements in this Section clear and appropriate? If not, how can they be improved? Should the Rule, for example, more clearly state that an operator's direct notice should include not just the types of personal information collected, but also how the operator intends to use the personal information that is collected? Should the Rule require the notice to include information about the categories of third parties, such as advertisers, that may make use of the information collected? The Rule's direct notice requirement found in § 312.4(c) presupposes that the operator has collected the parent's online contact information. Should the Rule more clearly state the content of direct notices where the operator does not collect a parent's online contact information?

Privacy policies are an ineffective method of providing information directly to consumers. Unfortunately, privacy policies tend to be vague and expansive. But even if they were more precise, it would not be efficient for consumers to read them: a study by Aleecia McDonald and Lorrie Cranor estimated that reading every site's privacy policy would take users over 244 hours per year, at a collective societal cost in wasted opportunity of over $600 billion.[73] Even though this study was based on adult users and the privacy policies they are presented with, it is likely that the situation is substantially similar for children's products.

Despite these issues, privacy policies have a role to play. Companies should be required to provide more detailed information about their actual practices within their privacy policies—not so much for consumers, but for regulators, journalists, civil society, and ratings services such as Consumer Reports. As such, privacy policies would function more like financial filings, which are important accountability documents, and which are not necessarily read by ordinary investors, but which are

content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

[73] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, J. OF LAW & POLICY FOR THE INFO. SOCIETY (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

processed by intermediaries to convey meaningful information to the marketplace.

In light of the issues posed by privacy policies—and because consumers strongly desire the ability to control their data and protect their privacy, but lack the means to do so—consumers, parents and non-parents alike, need better information and tools to evaluate and compare privacy choices. To that end, Consumer Reports and its partners have developed The Digital Standard,[74] an open standard for testing products for privacy and security in order to help consumers make informed decisions in the marketplace. The testing includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies. This effort depends on the transparency that privacy policies and user interfaces provide consumers.

In addition, privacy policies for children's connected products and services should more clearly state that an operator's direct notice should include not just the types of personal information collected, but also how the operator intends to use the personal information that is collected. The Rule should also require the notice to include information about the categories of third parties, such as advertisers, that may make use of the information collected. Finally, the Rule more clearly state the content of direct notices where the operator does not collect a parent's online contact information.

E. Exceptions to Verifiable Parental Consent

23. In the Statement of Basis and Purpose to the 1999 COPPA Rule, the Commission noted that the Rule "does not preclude schools from acting as intermediaries between operators and schools in the notice and consent process, or from serving as the parents' agent in the process." [7] Since that time, there has been a significant expansion of education technology used in classrooms. Should the Commission consider a specific exception to parental consent for the use of education technology used in the schools? Should this exception have similar requirements to the "school official exception" found in the Family Educational Rights and Privacy Act ("FERPA"),[8] and as described in *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*? [9] If the Commission were to amend the COPPA Rule to include such an exception:

b. Should operators be able to use the personal information collected from children to improve the product? Should operators be able to use the personal information collected from children to improve other educational or non-educational products? Should de-identification of the personal information be required for such uses? Is de-identification of

[74] The Digital Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use every day.

such personal information effective at preventing re-identification? What kinds of specific technical, administrative, operational or other procedural safeguards have proved effective at preventing re-identification of de-identified data? Are there instances in which de-identified information has been sold or hacked and then re-identified?

We recommend that the Commission rely on the three-part test laid out in its 2012 report. Specifically, in order to ensure that data is not "reasonably linkable" the company or holder of the data must "(1) take[] reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try and re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[75] However, we would suggest that the Commission also look to the formulation in the CCPA, which expands on the first prong of the FTC test and makes the requirements more clear. For example, in order to be de-identified, the data "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular customer" by implementing: (1) technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (2) business processes that specifically prohibit reidentification of the information; and (3) business processes to prevent inadvertent release of deidentified information.[76] The CCPA also requires the company to "make[] no attempt to reidentify the information."[77]

c. *Should parents be able to request deletion of personal information collected by operators under such an exception?*

Yes. Just as parents should retain this right with respect to the commercial market, parents should be able to request deletion of personal information collected by operators. In addition, parents should be able to opt-out of secondary uses of that personal information in order to ensure that they retain some control over children's data.

d. *Should an operator require the school to notify the parent of the operator's information practices and, if so, how should the school provide such notice?*

Parents should be informed of the operator's information practices. But in order to minimize the burden on the parents, we recommend that they are notified of these practices via a bifurcated notification that includes a simple articulation of rights and highlights and more detailed on what exactly is going on in case the parent would like to know more.

---

[75] *Protecting Consumer Privacy in an Era of Rapid Change*, FED. TRADE COMM'N p. iv(Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[76] Cal. Civ. Code § 1798.140(h), *available at* https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140.

[77] *Id*.

f. Should the scope of the school's authority to consent be limited to defined educational purposes? Should such purposes be defined, and if so, how? Should operators seeking consent in the school setting be prohibited from using information for particular purposes, such as marketing to students or parents?

The scope of the school's authority should be limited to defined educational purposes and those purposes should be defined. In addition, operators seeking consent in the school setting should be prohibited from using the information for marketing.

25. In some circumstances, operators of general audience platforms do not have COPPA liability for their collection of personal information from users of child-directed content on their platform uploaded by third parties, absent the platforms' actual knowledge that the content is directed to children. Operators of such platforms therefore may have an incentive to avoid gaining actual knowledge of the presence of child-directed content on their platform. To encourage such platforms to take steps to identify and police child-directed content uploaded by others, should the Commission make modifications to the COPPA Rule? For example, should such platforms that identify and police child-directed content be able 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? [11] Given that most users of a general audience platform are adults, there may be a greater likelihood that adults are viewing or interacting with child-directed content than on traditional child-directed sites. In considering this issue, the Commission specifically requests comment on the following:

Currently, the Rule defines a web site or online service directed to children as a "commercial web site or online service, or portion thereof, that is targeted to children." To determine whether a web site or online service is directed towards children, the FTC considers a number of factors. Despite the factors that are considered when determining if an online service is directed to children,[78] online platforms continue to claim that their sites are not meant for children under the age of 13, and thus are not subject to COPPA. When addressing the weaknesses of the COPPA Rule protections, Josh Golin said, "right now we are incentivizing companies to not know that children are on their sites...they've literally been rewarded for pretending there are no children on their sites."[79]

Accordingly, as we stated in response to question 2(c), Consumer Reports recommends that the Commission interpret the "actual knowledge" standard to include instances where the company or service willfully disregards the presence of children on their platform. Platforms like general-audience sites and app stores should have a greater incentive to police the content that is uploaded

[78] 16 C.F.R. § 312.2.

[79] *Sex, drugs, and self-harm, supra* note 5.

by others, especially where the company has designated special kid-friendly or family-friendly sections of their sites or stores. Viewers and users of child-directed content should be treated as children under the COPPA rule because it will be true in the vast majority of cases. In addition, we do not wish for the Commission to incentivize companies to collect more data on consumers. As we have discussed earlier in this comment, platforms and app stores who claim to identify and police their third-party child-directed content clearly are not doing so now (see Dr. Jenny Radesky's study discussed in response to Question A(1) and Serge Egelman's work discussed in response to Question A(3)(c) in addition to the YouTube settlement[80]). However, it is not clear how general-audience sites seek to ascertain what population of users are children and what are not or how effective these methods are. It would be helpful to also know how sites plan to preserve children's privacy while also establishing that some users are children. Such methods should be transparently disclosed so third parties can evaluate their methods.

With regards to the rebuttable presumption issue posed in question E(25)(e) below, without such disclosures, we cannot be confident that allowing such a presumption will not result in more children being treated as adults on their sites, either inadvertently, or willfully as in the case of Google's YouTube.[81] In addition, if the Commission were to adopt such a presumption, the FTC would be prioritizing enabling ad targeting on children-directed content rather than ensuring that COPPA is followed by general-audience platforms. Therefore, absent better performance by general-audience sites or more transparent disclosures, we recommend that for the time being general-audience sites should continue to treat all visitors of child-directed content as children.

Furthermore, browsers and other connected services are increasingly using always-logged-in features in order to make the browsing experience more seamless across devices (in addition to helping the company consolidate data streams from multiple devices for the purposes of ad tracking). For example, recently Google's Chrome browser was modified to automatically log a user into Chrome if the user signed into any Google property on the device, without even notifying the user of this change.[82] Although this allows the company to easily sync data across devices, it means that if a child then uses that device to go to YouTube kids or another service it will appear that an adult is logged on and viewing the content. Since Chrome dominates 62 percent of the browser market,[83] this automatic sign-in feature will affect many children. If the rebuttable presumption was adopted with these features in use, a general-audience site could claim that they have an adult viewing their child-directed content when it is in fact a child using an adult's account.

---

[80] *Google and YouTube Will Pay Record $170*, *supra* note 47.

[81] *Complaint to the FTC Regarding YouTube's Treatment of Children's Data*, CONSUMER REPORTS (Apr. 4, 2018), https://advocacy.consumerreports.org/research/complaint-to-the-ftc-regarding-youtubes-treatment-of-childrens-data/; *Google and YouTube Will Pay Record $170*, *supra* note 47.

[82] Gordon Kelly, *Google Chrome Log-in Change Angers Users*, FORBES (Sept. 26, 2018), https://www.forbes.com/sites/gordonkelly/2018/09/26/google-chrome-problem-web-browser-upgrade-update-windows-mac-linux-chromeos/#14793e6c6996.

[83] *Id*.

The rules under COPPA are already under-inclusive; a rebuttable presumption would make the rules even more so. For these reasons, we urge the Commission to incentivize platforms to treat viewers of child-directed content as children by engaging in robust enforcement and beginning in a 6(b) study to fully understand the issues.

However, we urge the FTC to not be swayed by the thousands of comments submitted by YouTube content creators in response to the Commission's request for comment.[84] Many (if not most) of these comments depend on fundamental misunderstandings of the law, and simply express a desire to show personalized advertising to kids—in clear violation of COPPA's strictures and intent.[85] Congress made a decision to protect children's privacy even when it posed a threat to profit margins. Although the growth of streaming videos online has grown since 2013, the need to protect children's privacy is as necessary as ever. Furthermore, it is telling that Google's YouTube pushed their creators to act on this issue,[86] despite the fact that their CEO has publicly stated that she does not allow her children to view YouTube proper, but only the YouTube Kids site.[87] For all the reasons we have included in this comment, we respectfully urge the Commission to keep children's privacy, and not profits, paramount in mind when considering changes to the 2013 Rule.

e. What, if any, risk is presented by permitting general audience sites to rebut the presumption that all users of child-directed content are children? Would it prove challenging to reliably distinguish between a parent and a child who accesses content while logged in to a parent's account? In considering whether to permit general audience sites to rebut the presumption, should the Commission consider costs and benefits unrelated to privacy, such as whether children may be exposed to age-inappropriate content if they are treated as an adult?

Please see our response to question E(25).

F. Right of a Parent to Review or Have Personal Information Deleted

---

[84] Harsimar Dhanoa & Jonathan Greengarden, *Misinformed YouTubers Are Undermining the Fight for Children's Privacy Online*, SLATE (Nov. 27, 2019), https://slate.com/technology/2019/11/youtube-coppa-google-ftc-settlement-children-privacy.html.

[85] *Petition: SAVE Family-Friendly Content on YouTube,* CHANGE.ORG, https://www.change.org/p/the-federal-trade-commission-youtubers-and-viewers-unite-9045ee7f-f6f0-460e-b088-3429209dd7c6?recruiter=1015502725 (last visited Dec. 10, 2019).

[86] "YouTube has said it will comply with the new rules, but it has also encouraged creators to express their views. The company sent a notice to creators over the summer informing them of a workshop with the FTC. "It is important they hear from creators and small businesses that could be deeply impacted by potential changes," a YouTube representative wrote, according to an email viewed by Bloomberg News." Mark Bergen, Lucas Shaw, & Ben Brody, *YouTubers Are Lobbying FTC to Fight Child Privacy Law Expansion*, BLOOMBERG (Nov. 5, 2019), https://www.bloomberg.com/news/articles/2019-11-05/youtubers-are-lobbying-ftc-to-fight-child-privacy-law-expansion.

[87] E.J. Dickson, *YouTube CEO Susan Wojcicki Apparently Doesn't Let Her Young Kids Watch YouTube*, ROLLING STONE (Dec. 2, 2019), https://www.rollingstone.com/culture/culture-news/susan-wojcicki-ceo-youtube-kids-920168/.

26. Section 312.6(a) of the Rule requires operators to give parents, upon their request: (1) A description of the specific types of personal information collected from children; (2) the opportunity to refuse to permit the further use or collection of personal information from the child and to direct the deletion of the information; and (3) a means of reviewing any personal information collected from the child. In the case of a parent who wishes to review the personal information collected from the child, § 312.6(a)(3) of the Rule requires operators to provide a means of review that ensures that the requestor is a parent of that child (taking into account available technology) and is not unduly burdensome to the parent.

Most consumers do not make use of the settings they are provided with;[88] therefore, it is likely that parents are generally underutilizing the right to access their children's information under COPPA. Despite this, parents should still retain their rights to (1) obtain a description of the specific types of personal information that are being collected from children, (2) refuse to permit the further use or collection of personal information from the child and to direct the deletion of that information; and (3) review what personal information was collected from the child. As we detail below, although the US still lacks strong federal privacy laws, the passage of the California Consumer Privacy Act (CCPA) and the discussion of similar measures in other states will likely lead to greater utilization of the rights under COPPA. This expectation is based on the EU's experience following the passage of the General Data Protection Regulation. In addition, the ability to know what kinds of data are being collected about children generally and the information that has been collected about one's own child specifically is essential to parents not only understanding how their child's data is being collected and handled but also is necessary for consumer advocacy groups and product rating organizations to be able to audit these companies' practices with regard to children's products and services.

Finally, states across the country are considering implementing laws like the CCPA in their own jurisdictions and bills preserving the same rights are being discussed in the US Congress. Therefore, it would be concerning if a previously more-protective law (COPPA) is made weaker with regard to these rights at the same time that states and the US Congress have, or are considering, extending these rights to *all* consumers. COPPA was passed in 1998 in order to respond to concerns about a vulnerable population of consumers, children. It would undermine the spirit and purpose of the law if the protections for children's data are rolled back while adult

[88] Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PROPUBLICA (July 27, 2016), https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world; Charles Arthur, *Why the Default Settings on Your Device Should be Right the First Time*, THE GUARDIAN (Dec. 1, 2013) https://www.theguardian.com/technology/2013/dec/01/default-settings-change-phones-computers; The study conducted by Jared Pool and his colleagues showed that less than 5% of users changed any default setting: "Less than 5% of the users we surveyed had changed any settings at all. More than 95% had kept the settings in the exact configuration that the program installed in." Jared Pool, *Do Users Change Their Settings?*, UIE (Sept. 14, 2011), https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/.

consumers are granted similar protections.

a. To what extent are parents exercising their rights under § 312.6(a)(1) to obtain from operators a description of the specific types of personal information collected from children?

Parents should still retain the ability to obtain a description of the specific types of personal information collected from children. Parents need to know what kinds of data will be collected just as adult consumers should know what kinds of data is being collected about them. We expand on this issue in response to question F(26)(c).

b. To what extent are parents exercising their rights under § 312.6(a)(2) to refuse to permit the further use or collection of personal information from the child and to direct the deletion of the information?

As we note in response to question F(26), all consumers in California now have the right to refuse to permit the further use or collection of personal information and direct the deletion of this information. Although the use of this right may be underutilized currently, the experience of the GDPR in the EU leads to the expectation that consumers in the US will likewise be more inclined to make use of these rights once they are more aware of their ability to do so. And this increase in use will likely extend to children's information, especially since they are considered more vulnerable. As a report from Deloitte notes, 79 percent of all EU respondents were aware of their right to delete and 12 percent had already exercised their right in the six months following the implementation of the GDPR. In addition, the publicization of the GDPR implementation seems to have some effect on residents even outside the EU, with 17 percent of respondents saying that they plan to request deletion in the future.[89] Similarly, we can expect US residents to make more use of their ability to stop the use of or delete the information collected about their children after the implementation of the CCPA since there will be increased awareness about the right to do so (at least if you are a resident of CA) and heightened cognizance of the general need and utility of this exercising such a right. We expand more on the effect the GDPR has had on EU residents' awareness of their rights, even rights they had held previously, in response to question F(26)(c).

c. To what extent are parents exercising their rights under § 312.6(a)(3) to review any personal information collected from the child?

Parents should retain the right to access and review their children's information. Not only do data access requests provide parents with helpful information, this kind of data can also be used by

[89] *A New Era for Privacy: GDPR Six Months On*, DELOITTE (2018), https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf.

advocacy and product rating groups in order to audit children's connected products and services. The implementation of the California Consumer Privacy Act (CCPA),[90] which accords all consumers with the right to access their data, may increase parent's interest in obtaining such information about their children's data due to the increased awareness of the ability to submit such requests. This expectation is predicted by the European Union's experience with the General Data Protection Regulation (GDPR).

Before the GDPR went into effect in May 2018, individuals in the EU could request their data under a subject access request. However, the news around the implementation of the GDPR led to many more data subject access requests following May 2018. As one article notes: "this is one of the major benefits of the Regulation's much-publicised powers. It raised the stakes for effective cyber security and data privacy, leading to widespread discussions of the GDPR's requirements and the rights it enshrined."[91] A report from Deloitte documenting the effects of the GDPR six months after it was implemented found: "79% of respondents are aware of their right of access...10% of respondents have already submitted access requests to organisations that hold their personal data."[92] The section on data access requests concludes: "However, there is a strong likelihood that individuals' awareness of their rights and their propensity to exercise those rights will increase over time as further scenarios that take advantage of these rights emerge and are used to enforce consumer rights."[93]Accordingly, we can expect parents in the US to make greater use of their ability to access and review their children's in the wake of the CCPA's implementation. Likewise, since adult consumers are being granted similar rights in California and residents of other states may also gain these rights in the upcoming legislative sessions (not to mention the possibility that all US consumers could gain similar rights under a federal privacy law), it would be odd for such protections for a more vulnerable population, children, to lose those rights under any alterations to the COPPA Rules that the FTC contemplates.

G. Prohibition Against Conditioning a Child's Participation on Collection of Personal Information

27. COPPA and § 312.7 of the Rule prohibit operators from conditioning a child's participation in an activity on disclosing more personal information than is reasonably necessary to participate in such activity.

Privacy is an inalienable human right and participation in an activity should not be conditioned on

---

[90] Deepak Gupta, *California, here we come: How companies need to prepare for new digital privacy laws*, FAST CO. (Nov. 22, 2019), https://www.fastcompany.com/90434818/california-here-we-come-how-companies-need-to-prepare-for-new-digital-privacy-laws?partner=feedburner.

[91] Luke Irwin, *The GDPR has led to a spike in DSARs (data subject access requests)*, IT GOVERNANCE (Oct. 9, 2019), https://www.itgovernance.eu/blog/en/the-gdpr-has-led-to-a-spike-in-dsars-data-subject-access-requests.

[92] *GDPR Six Months On*, *supra* note 89.

[93] *Id*.

disclosing more personal information that is reasonable. This right to privacy applies to children as well as adults. Just as the GDPR does not allow a company to require the processing of additional information that is unrelated to the activity,[94] COPPA should not allow such additional processing for children, who are a more vulnerable population. Organizations like Consumer Reports[95] have and are advocating for similar safeguards to be put in place for adults. The Commission should not roll back such protections for children, especially in light of similar elements being considered for adults in Congress and the GDPR protecting those rights for adults and children alike. A safeguard against secondary processing unconnected to the purpose the data was collected is essential for any strong privacy law. Children should retain this protection.

H. Confidentiality, Security, and Integrity of Personal Information

28. Section 312.8 of the Rule requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child, and to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the personal information, and who provide assurances that they will do so.

a. Have operators implemented sufficient safeguards to protect the confidentiality, security, and integrity of personal information collected from a child?

As our responses to questions A(1) and A(3)(c) demonstrate, companies have not implemented sufficient safeguards to protect the confidentiality, security, and integrity of the personal information collected from children. Also, if the adult population is any measure, companies are not adequately protecting the data that they obtain, store, process, and use no matter the kind of data they have. For example, the Equifax data breach of 2017 led to the disclosure of the personal information, including Social Security numbers, of over 145 million Americans—about half of the United States population—leaving them susceptible to identity thieves seeking to open credit in their names for years to come.[96] This breach also affected children, leading lawmakers to make credit freezes for adults, and their children, free[97] in the wake of this massive breach.[98] Companies have dramatically expanded their data collection practices as they have found new ways to monetize consumer data, but incentives to protect consumer data from unauthorized disclosure remain inadequate. Without sufficient enforcement by the Commission on the security of

---

[94] Art. 5 of the GDPR, *available at* https://gdpr-info.eu/art-5-gdpr/.

[95] Katie McInnis, *Comments on Consumer Privacy for the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century on February 12-13, 2019*, CONSUMER REPORTS (Dec. 21, 2018), https://advocacy.consumerreports.org/research/consumer-privacy-feb-2019/.

[96] Jeremy C. Owens, *The Equifax Data Breach, In One Chart*, MARKETWATCH (Sept. 10, 2018), https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07.

[97] *S.2155 - Economic Growth, Regulatory Relief and Consumer Protection Act*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/senate-bill/2155 (last visited Dec. 9, 2019).

[98] Ron Lieber, *You Should Freeze Your Child's Credit. It's Not Hard. Here's How*, N.Y. TIMES (Dec. 28, 2018), https://www.nytimes.com/2018/12/28/your-money/credit-freeze-children.html.

children's personal information, companies have insufficient incentives to be better stewards of children's personal data.

I. Safe Harbors

29. Section 312.11(g) of the Rule provides that an operator will be deemed in compliance with the Rule's requirements if the operator complies with Commission-approved self-regulatory guidelines (the "safe harbor" process).

a. Has the safe harbor process been effective in enhancing compliance with the Rule?

No. Please see our response to question A(3)(c).

Thank you for the opportunity to respond to the Commission's request for comments on potential updates to the COPPA Rule. If you have any questions, please feel free to contact us at 202.462.6262.

Respectfully submitted,

Katie McInnis
Policy Counsel
Consumer Reports
1101 17th Street NW, Suite 500
Washington, DC 20036