Testimony of Professor Angela J. Campbell
Hearing before the Senate Committee on the Judiciary
Protecting Innocence in a Digital World
July 9, 2019

Thank you for inviting me to testify about protecting children in the digital age. So many of the problems that families are struggling with today – such as how to protect children's privacy, how to prevent exposure to inappropriate content, and how to limit the amount of time children spend on digital devices – are a direct result of two things. First, the business models of the dominant tech companies are designed to attract large number of users, including children, and to keep them online as long as possible, so they can maximize revenue by collecting valuable data about the users and delivering targeted marketing to them. Second, the government has failed to adopt sufficient safeguards for children and has not effectively enforced existing safeguards. In particular, the Federal Trade Commission's (FTC) failure to vigorously the enforce the Children's Online Privacy Act (COPPA) creates an atmosphere in which the big tech companies – such as Google, YouTube, Facebook, and Amazon – feel empowered to ignore existing safeguards.

COPPA was adopted in 1998 to protect the privacy of children under age 13. At that time, there was no YouTube, no social media, no smartphones, no smart speakers in children's bedrooms, and no toys connected to the internet. Moreover, the Children's Television Act of 1990 and FCC rules limited the amount and types of advertising on children's television programs, on both broadcast and cable. These safeguards, however, have not been applied to children's content on the internet. Thus, the laws are out of sync with the current media marketplace and fail to provide the protections children need for healthy development.

My testimony today largely summarizes the points made in the attached comments I filed with the FTC on behalf of the Campaign for a Commercial Free Childhood and Center for Digital Democracy. These comments explain why COPPA is no longer sufficient to protect children in the current environment and call for new legislation. Passing the Do Not Track Kids Act of 2019 introduced by Senators Markey and Hawley would be a good first step.

Even in the absence of new legislation, however, the FTC can and should act to better protect children's privacy. First, the FTC must enforce COPPA more effectively. Since COPPA took effect in 2000, the FTC has brought only 29 actions to enforce COPPA, and all have been settled by consent decree. Consent decrees provide only limited relief; they are binding only on the parties to the decree and provide less guidance for interpreting COPPA than litigated cases or rules. Moreover, the civil penalties imposed have generally been too low to deter future violations.

In addition, the self-regulatory safe harbors, which Congress intended to augment the FTC's enforcement efforts, have not been effective. While the FTC has approved seven safe harbors, these programs seem more interested in protecting companies that pay for the right to display a seal than protecting children. The FCC has failed to hold the safe harbors accountable, or to even make public the annual reports that safe harbors are required to submit to the FTC.

This lack of transparency extends to the FTC operations as well. It will not discuss any investigation or even say whether an investigation is taking place. The FTC provides no formal process for parents to file complaints or obtain relief for COPPA violations.

Nonetheless, on behalf of my clients, I have filed since 2012, filed 14 requests asking the FTC to investigate COPPA violations. The FTC has not acted – at least publicly – in response to any of these requests.

I would like to tell you about two recent requests that may be of particular interest to the Committee. In December 2018, we asked the FTC to investigate whether the Google Play Store was engaging in unfair and deceptive practices in marketing apps for children. After several academic studies found that many apps in the "Family" section of the Play Store identified as intended for children, were not actually appropriate for children, we conducted our own investigation.

Apps included in the Family section display a small green star to indicate they are "family-friendly." Often, the star is accompanied by the age range that the app was designed for, such as under age 8. Google requires app developers to apply and to meet certain criteria to be included in the Family section and display the green star. To meet the criteria, apps must comply with children's privacy laws, not engage in deceptive or unfair advertising practices, and not show content inappropriate for children. While these are reasonable criteria, we discovered that Google was not enforcing them.

We found many examples of children's apps that violate COPPA by collecting personal information from children without giving notice to parents and obtaining verifiable parental consent. We also found many instances of unfair or deceptive practices – such as manipulating kids to watch ads or make in-app purchases. We also found apps with content inappropriate for children such as advertisements for beer and gambling. We argued that by misrepresenting that these apps were appropriate for children, Google was engaging in deceptive practices in violation of Section 5 of the FTC Act.

Earlier, in April 2018, we asked the FTC to investigate whether YouTube was violating COPPA. YouTube is the most popular online platform among children. It hosts channels of nursery rhymes, unboxing videos, popular cartoons, and other content specifically designed for

children on the main YouTube platform. Some, such as ChuChuTV Nursery Rhymes & Kids Songs and Ryan ToysReview, are among the most popular of all YouTube channels.

Google asserts that it need not give notice or obtain parental consent for collecting personal information as required by COPPA, because children are not on YouTube. The absurdity of this claim is belied by the company's recent decision to disable comments on tens of millions of videos featuring children under 13 due to concerns that pedophiles have used comments on videos of children to guide other predators.[1]

Recent press reports have indicated that the FTC is considering taking action against YouTube for violating COPPA. Consequently, my clients and I wrote the FTC outlining what we believe would be appropriate remedies. Among other things, we asked the FTC to ensure that Google lives up to its Terms of Service – which stipulate YouTube is only for persons thirteen and older – by removing all kids' content from the main YouTube platform. All child-directed content should be placed on a separate platform where targeted advertising, commercial data collection, links to other sites or content, comments, and autoplay are prohibited. These changes would help advance a healthy media environment for children, while sending a clear message to all online and mobile operators that no one is above the law.

I appreciate the opportunity to appear before the Committee and am happy to answer any questions.

[1] Daisuke Wakabayashi, YouTube Bans Comments on Videos of Young Children in Bid to Block Predators, NY Times, (Feb. 28, 2019), https://www.nytimes.com/2019/02/28/technology/youtube-pedophile-comments.html?module=inline.

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

Competition and Consumer Protection in the 21st Century, Hearing #12: The FTC's Approach to Consumer Privacy	**)** **)** **)**	No. P181201

Comments of the Center for Digital Democracy and the Campaign for a Commercial Free Childhood

The Center for Digital Democracy (CCD) and Campaign for a Commerical Free Childhood (CCFC), by their attorneys, the Institute for Public Representation (IPR) at Georgetown Law, [2] submit comments regarding the FTC's Approach to Consumer Privacy. Our comments focus on privacy of children and teens. We show how prevalent data collection and tracking have become in the lives of children and teens.

While the Children's Online Privacy Protection Act (COPPA) is intended to protect the privacy of children under age 13, it is no longer up to the task. COPPA's underlying assumption is that parents will be able to protect their children's privacy if companies give notice of their privacy practices and do not collect personal information until unless the parent gives consent. But this no longer works. Most parents do not read privacy policies, and even if they do, many not provide the information needed for informed consent. Given the unprecedent amount of data being collected, the sophistication of data mining techniques, and the lack of transparency, most people lack a sufficient understanding of scope of the data collected and how it could be used. Moreover, because the FTC has not effectively enforced COPPA, many companies feel free to ignore COPPA's requirements.

[2] Georgetown law student Tracey Klees assisted in the preparation of these comments.

New legislation, such as the bi-partisan Markey-Hawley bill, is needed to address COPPA's short comings. Any legislation must include developmentally-appropriate protections for teens, because COPPA only covers children under age 13. The legislation should also prohibit practices that may be harmful to children, rather than requiring parents to read and try to understand the impact of multiple privacy policies.

Until such legislation is passed, however, the FTC can and should do more to better protect children's privacy. Specifically, we urge the FTC to undertake more enforcement actions, to enforce COPPA's notice requirements, and to fix problems with the COPPA safe harbor program.

Table of Contents

I. Introduction

Both CCD and CCFC have had many years of experience with COPPA. CDD's predecessor organization, Center for Media Education (CME), and counsel IPR, filed the first complaint alleging that a children's website, Kidscom, was engaging in unfair and deceptive practices in 1996.[3] After Congress passed COPPA in 1998, a coalition of groups led by CME commented on the FTC proposed rules for implementing COPPA.

[3] FTC Staff Sets Forth Principles For Online Information Collection From Children, July 16, 1997, https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection.

When the FTC opened a proceeding to revise COPPA in 2010, CDD, CCFC, and others urged the FTC to update the COPPA Rule to take account of changes in technology and marketing. The FTC adopted many of our suggestions and cited our comments multiple times in the Statement of Basis and Purpose accompanying the revised rule.[4] We also filed comments on every proposal for a COPPA safe harbor as well as and proposals for verifiable parental consent mechanisms.

CDD and CCFC have also filed numerous complaints alleging COPPA violations and asking the FTC to investigate.[5] Most recently, in April 2019, we alleged that Amazon's Echo Dot Kids Edition violated COPPA by failing to give adequate notice, failing to obtain verifiable parental consent, and retaining children's voice recordings and transcription for far longer than necessary. In December 2018, we alleged that Google Play's family section included a large number of apps rated for children under age 13 that were not in compliance with COPPA. In October, 2018, CCFC and others alleged that Facebook's Messenger Kids violated COPPA by collecting personal information from children without obtaining verifiable parental consent or providing parents with clear and complete disclosures of Facebook's data practices.

In April 2018, CDD and CCFC alleged that YouTube failed to provide notice or get parental consent before collecting personal information from children watching children's program channels on YouTube. Other complaints alleging COPPA violations concerned interactive toys, online promotions of candy, a child-directed website, mobile apps, and "refer-a-friend" features on children's websites.

[4] *Children's Online Privacy Protection Rule, Statement of Basis and Purpose*, 78 Fed. Reg. 3972 (2013).

[5] A list of all of our COPPA filings is attached.

Our experience informs these comments. While historically COPPA has protected children's privacy, it is no longer sufficient today. Due to the pervasiveness of data collection, tracking and surveillance and the FTC's failure to adequately enforce the law, children may be tracked in virtually all aspects of life. Unless a website is considered "directed to children" and parents decline to consent, a child will likely be tracked whenever she browses the internet, watches a video online, uses a search engine, plays an online game, visits a website, or makes an online purchase. Simply having a cell phone, allows a child's location to be tracked. Smart speakers in the home, as well as toys connected to the internet, record children's voices and answer their questions. Children's television viewing may be tracked by smart television sets or streaming services.

As explained below, the collection of so much data, combined with sophisticated means of analyzing data poses substantial risks to children and teens. Personal information collected from children and teens may combined with other data from a variety of sources. It can be mined using powerful computing processing including AI, to allow marketers to gain insights on how they can influence consumer attitudes and values, test how to make advertising even more manipulative, test what products will be successful, and expand or limit opportunities that children and teens are exposed to through marketing. Thus, new legislation. along with more effective enforcement of existing laws, are needed to ensure adequate protection of children and teens.

II. Changes since COPPA was adopted in 1998 require new legislation

In the more than 20 years since COPPA's passage, the development of new platforms, the rise of the internet of things, and the ubiquity of data collection have allowed digital risks to outpace the law. COPPA was intended to mitigate these privacy risks to children, but experience

has shown that it is no longer provides sufficient protection. For this reason, we urge the FTC to support bi-partisan legislation such as S. 748, introduced by Senators Markey and Hawley.

A. Digital technologies have become a pervasive presence in the life of children and teens

In 1999, children ages 2-18 spent on average 5:29 minutes a day using media. Of this total, 2:46 hours were spent watching television, 21 minutes using the computer for fun, 20 minutes playing video games, and 8 minutes using the internet.[6] When COPPA was passed in 1998, YouTube, Instagram, Facebook, Twitter and other social networks did not exist. Nor did smart phone and mobile apps.

At that time, broadcast and cable television were the dominant means for advertisers to market to children and teens. But today, television is just one of many ways that advertisers can reach children. An entire industry has developed to track consumers (including children) across difference digital devices, to profile them based on their online activities and other data, and to target marketing messages to them on a one-to-one basis. New forms of advertising such as "influencer" videos, has proven very effective with children because children do not recognize them as ads. Advertisers use artificial intelligence and other sophisticated techniques for analyzing and acting upon data. Advertisers have very strong incentives to keep children and teen on screens – as it both allows them to deliver more advertising and to collect more data that it can use to target ads with greater precision.

Studies show that new technologies such as smart phones and tablets play a large role in the lives of children and teens. As of 2017, 98% of homes with children aged 8 and under had a

[6] Kaiser Family Foundation*, Kids and Media at the New Millennium* at 7-8, (Nov. 1999), https://files.eric.ed.gov/fulltext/ED445369.pdf,

smartphone or tablet, up from 53% in 2011.[7] On average, children 8 and under spent 2 hours and nineteen minutes on a screen, of which only 42% was watching television, while 35% was on mobile devices. [8]

A 2015 study found that 53% of tweens (aged 8-12) had their own tablets and 67% of teens had their own smartphones.[9] On average, tweens spent almost 4 hours, 36 minutes on screen media and teens spent 6 hours, 40 minutes.[10] A Pew Survey of teens in 2018 found that 85% of teens reported using YouTube, 72% using Instagram, 69% using Snapchat, 51% using Facebook and 32% using Twitter.[11] In addition to being an essential part of children's and teen's social lives, students are often required to use digital technologies in school, for homework, and to participate in extracurricular activities. Technology is no longer an optional part of childhood or adolescence.

B. Teens as well as children need privacy protections

One reason that new legislation is needed is that COPPA applies only to children ages 13 and under. Consequently, once a child turns thirteen, she is treated the same as an adult in terms

---

[7] Common Sense Media*, Common Sense Census: Media Use By Kids Age Zero To Eight,* at 23 (Oct. 2017), https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_zerotoeight_fullreport_release_2.pdf. Moreover, 42% of children aged 8 and under had their own tablet. *Id.* at 3.

[8] *Id.* at 3.

[9] Common Sense Media, *Common Sense Media Census: Media Use By Teens and Tweens* at 20 (Nov. 2015), https://www.commonsensemedia.org/sites/default/files/uploads/research/cs_mediacensusinfographic_d4.pdf.

[10] *Id.* at 20, Table 7. Total time spend with media is even higher, as it includes print and media. *Id.* at 19, Table 4.

[11] Monica Anderson and Jinjing Jiang, Pew Research Center, *Teens, Social Media & Technology 2018* at 2 (May 2018), https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/ (Pew Teens Report).

of data collection and use. US laws generally do not require that adults be given notice of privacy practices or choices about whether and how their data is collected and used.

We support legislation that would give privacy protections to people of all ages because that would represent an improvement over the status quo for teens and children (when they are using an online service that is not directed at children). But teens also need their own special protections. Teens are particularly at risk because their cognitive control systems necessary to regulate risky behavior are relatively immature.[12] As panelist Ariel Fox Johnson explained at the April 9 hearing, adolescents are more reward-sensitive than adults are, which means they're more likely to take short term risks online.[13] Not only do adolescents tend to take more risks, but they are more vulnerable to peer pressure. This means they are more likely to join (and less likely to leave) online communities where their friends are.[14]

These development characteristics of teens means that they have more difficulty evaluating privacy risks than adults are and less likely to abandon technologies that violate their privacy because of network effects. The Pew Report found that few adolescents regularly deleted or restricted access to their posts due to concerns that they could negatively impact them in the

[12] Ethan McCormick, Yang Qu, Eva H. Telzer, *Adolescent Neurodevelopment of Cognitive Control and Risk-Taking in Negative Family Contexts*, Neuroimage (Oct. 3, 2015) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4651739/ (describing how cognitive development in adolescence engenders risk-taking).

[13] *Transcript: Competition and Consumer Protection In the 21st Century* at 162 (April 9, 2019), https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_1_4-9-19.pdf.

[14] Taylor Lorenz, *Teens Are Being Bullied 'Constantly' on Instagram*, The Atlantic (Oct. 10, 2018), https://www.theatlantic.com/technology/archive/2018/10/teens-face-relentless-bullying-instagram/572164/ (describing how teens fail to leave Instagram despite massive bullying because "quitting wasn't an option"); Pew Report, at 13 (reporting that teens are more likely to spend time with their friends online on a daily basis than to do so in person).

future.[15] Research have shown that teens care about and make efforts to protect their privacy, but but they find it challenging to control how their information is distributed.[16]

C. Affording parents notice and consent is no longer sufficient to protect children's privacy

COPPA properly recognizes that children are not capable of assessing privacy risks on their own. Children often do not understand the implications of the technology they use, and they are more vulnerable to manipulation than teens or adults. As Ariel Fox Johnson explained at the April 9 hearing, children don't understand the privacy implications of the technology they're using, and they're even less capable than adults are of correctly assessing the risks.[17]

Studies back up this claim. A recent study found that children under age 11 "could identify and articulate certain privacy risks well, such as information oversharing or revealing real identities online; however, they had less awareness with respect to other risks, such as online tracking or game promotions." [18] This study found that familiarity could give children a false sense of safety.[19] Another study found that children rarely understand the invasive potential of

---

[15] Pew Teen Report, at 12.

[16] *E.g.* Alice Marwick & danah boyd, *Networked privacy: How teenagers negotiate context in social media*, 16 new media & society 1051 (2014). These researchers cite examples of harms such as a high school student who did not realize his crass and juvenile humor that he share with his friends could be viewed by college representatives who were friends with one of his friends. Id. at 1058. In another case, a college student was outed to his parents because they could see he joined a facebook group for his univeristy's queer chorus. *Id.* at 1062.

[17] Ariel Fox Johnson, Federal Trade Commission, *Transcript: Competition and Consumer Protection In the 21st Century* at 153 (April 9, 2019) https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_1_4-9-19.pdf.

[18] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke Childs, Max Van Kleek, & Nigel Shadbolt, *"I make up a silly name": Understanding Children's Perception of Privacy Risks Online,* at 1, CHI Conference on Human Factors in Computing Systems Proceedings 2019 (May 2019), https://arxiv.org/pdf/1901.10245.pdf..

[19] *Id.* at 9. For example, in one focus group, a ten year old girl remarked "I don't think YouTube and stuff like that could collect much," while other children described using the fact that their friends played a certain app or game as a reason to trust it.

the interconnected toys.[20] When asked whether a smart toy could remember what the child told it, most children either didn't understand the toy was recording them, or thought that the toy would only record them when a parent was nearby.[21]

Because children cannot protect their own privacy, COPPA places the responsibility on parents. COPPA is premised on the assumption that parents will be able to protect their children's privacy by reading privacy notices and deciding whether to give consent. COPPA requires direct notice to parents and post privacy policies contain the information needed for parents to make an informed decision. COPPA further requires verifiable parental consent before an operator may collect personal information from a child. It also gives parents the right to find out what information has been collected, to delete than information, and to prohibit further collection.

In the 1990s, when there were fewer child-directed websites and online services and no YouTube, no social networks such as Facebook and Instagram did, and no smart phones collecting geolocation and other information, it was reasonable to expect that parents could protect their children's privacy if they had adequate notice of an operator's. privacy practices and children's information could not be collected in the absence of verified parent consent. Notice and consent, however, are no longer sufficient today. The proliferation of networked technology has made that paradigm obsolete. There are too many privacy notices to read them all, and parents are ill-equipped to evaluate the information provided in privacy policies that they do read.

---

[20] Emily McReynolds, Sarah Hubard, Timothy Lau, Aditya Saraf, Maya Cakmak, & Franziska Roesner, *Toys that Listen: A Study of Parents, Children and Internet-Connected Toys*, 2, CHI 2017 (May 6, 2017), http://techpolicylab.uw.edu/wp-content/uploads/2017/10/Toys-That-Listen_CHI-2017.pdf.

[21] *Id.* at 6.

It is common knowledge that most people do not read privacy policies. A recent poll found that 56% of consumers usually or always click to accept a company's privacy policy without reading it, while only 13% say they never do so.[22] This is hardly surprising. People do not have time to read privacy policies. A well-known study published in 2008 estimated that it would take 76 work days for an internet user to read every privacy policy on every website they visited. The study further calculated the national opportunity cost of reading privacy policies at $781 billion, or greater than the GDP of Florida. [23] Given the increase in the number of websites and other online services (such as mobile apps) and the increasing amount of data collection by third parties, it would undoubtedly take much longer today. And as the *New York Times* recently opined, "Why would anyone read the terms of service when they don't feel as though they have a choice in the first place? It's not as though a user can call up Mark Zuckerberg and negotiate his or her own privacy policy."[24]

Privacy law scholars have documented many reasons why notice and consent is not effective at protecting consumer privacy.[25] For example, Alessandro Acquisti & Jens Grossklags have shown how hyperbolic discounting, i.e., the idea that people tend to opt for quick rewards

---

[22] Kim Hart, Privacy policies are read by an aging few, Axios, Feb. 28, 2019, https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html.

[23] Aleecia M. McDondald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[24] How Silicon Valley Puts the 'Con' in Consents, Feb. 2, 2019, https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html?searchResultPosition=3.

[25] Neil Richards & Woodrow Hartzog*, Pathologies of Digital Consent*, Wash. U. Law Rev at 1-5 (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433 (surveying various critiques of digital consent). *See also* Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. Law Rev.1880 (2013); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 Yale L.J. 1180 (2017); Scott Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent, 93 Tex. L. Rev. 85 (2014).

in the short term over more protracted rewards in a longer timeframe, skews privacy decision-making. [26]

Other research shows that many parents lack the understanding necessary to assess privacy risks. For example, a Pew Research Center survey found that 52% of internet users believe — incorrectly — that "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."[27] Another survey found that while many parents use privacy settings on social media, "privacy settings are not well understood by all users." As a result of this lack of understanding, many children under 13 "have a lengthy "digital profile" based on their parents' social media use." [28] Another study showed it was possible to deduce the names, birthdates, addresses and faces of children from their parents' publicly-available Facebook profiles combined with the parents' voter registration information.[29]

Privacy policies are often long.[30] And they can be difficult to understand. Research by Professor Turow at the Annenberg School of Communications suggests that "ordinary users don't fully understand the scope of the data that is being collected on them — or how small amounts of data can be used to create a much more detailed portrait when matched with information from third-party sites that collect and share various types of customer information

---

[26] Alessandro Acquisti & Jens Grossklags, Privacy and Rationality in Individual Decision Making, 3 INST. ELECTRIC & ELECTRONICS ENGINEERS SECURITY & PRIVACY 31 (2005).

[27] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, Pew Research Center (Dec. 4, 2014) https://perma.cc/9GBKH4HM.

[28] Mott Poll Report, *Parents on social media: Likes and dislikes of sharenting,* (March 2015), https://mottpoll.org/reports-surveys/parents-social-media-likes-and-dislikes-sharenting.

[29] Tehila Minkus, Kelvin Liu, Keith W. Ross, *Children Seen But Not Heard: When Parents Compromise Children's Online Privacy*, International World Wide Web Conference Committee, 5, 7-8, (May 2015).

[30] For example, a printed version of the privacy policy for the popular children's app Roblox is 17 pages long. Roblox Privacy and Cookie Policy, https://en.help.roblox.com/hc/en-us/articles/115004630823-Roblox-Privacy-and-Cookie-Policy-.

with each other."[31] Turow explains that the "general sense among marketers is that people understand that their data is being used, but we've found in our research that people don't truly understand how data mining works. They may realize that one or two pieces of their information are being given out; what they don't realize is that those one or two data points can be linked with other sources to uncover information they would have never given out in the first place."[32]

Finally, COPPA requires that websites and online services directed to children, directed to a general audience, or that operate an ad network, plug-in or other third-party service used by child-directed sites, to have a children's privacy policy.[33] Moreover, privacy policies must contain certain information specified in Rule 312.4(d) such as a "description of what information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how the operator uses such information; and, the operator's disclosure practices for such information."

In our experience, privacy policies often do not contain all required information. For example, the privacy policy for Facebook's Messenger Kids states that Facebook may transfer information to third parties to "support [its] business." That phrase might be interpreted to cover almost anything, including transfers to advertising networks, data brokers, and analytics firms, and Facebook lists only a few, non-exclusive examples of service providers that would support Facebook's business. This privacy policy also states that data may be disclosed "to improve the services provided by the Facebook family of companies." While this sounds benign, most

---

[31] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, Pew Research Center (Dec. 4, 2014) https://perma.cc/9GBKH4HM.

[32] *Id. See also* Joseph Turow, *Let's Retire the Phrase 'Privacy Policy*,' NY Times, Aug. 20, 2018,

https://www.nytimes.com/2018/08/20/opinion/20Turow.html?searchResultPosition=1.

[33] *Children's Online Privacy Protection Rule: Not Just for Kids' Sites,* https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites.

parents are unlikely to know that Facebook has acquired or merged with 66 different companies, including Instagram, WhatsApp, and Masquerade (which sells face-tracking technologies), and Facebook does not name any of these companies. Facebook also fails to list all third party operators collecting or maintaining personal information from children as required by §312.4(d)(1) and that that parents have the right to direct the operator to delete their child's personal information as required by §312.10. [34] Similarly, we found that the we found the privacy policies for the Amazon Echo Dot Kids Edition did not identify the actual types of personal information collected, and improperly disavowed any responsibility for third party collection of data through this service.[35] Insufficient notice preventing parents from making informed decisions about whether to grant consent.

D. Manipulative designs exacerbate the problems with inadequate notice

Many digital services employ what are known as "dark patterns," or surreptitious design cues that prey on users' vulnerabilities to induce conduct that benefits the service, typically to the detriment of the user.[36] Such practices make it difficult for teens to protect their privacy and for adults to protect the privacy of children under age 13.

Some examples of dark patterns include default settings that require users to opt out of having their information shared, defaults that are difficult to change, ads disguised as organic content, and misleading, loaded descriptions of user choices.[37] A report by the UK's Information

[34] *Letter to Donald S. Clark from James T. Graves regarding Facebook Messenger Kids*, Oct. 3, 2018, at 4-6, https://www.commercialfreechildhood.org/sites/default/files/devel-generate/wab/FTC%20FB%20Messenger%20Kids%20Letter.pdf.

[35] Echo Dot Request for Investigation, at 17-22.

[36] Thomas Germain, *How To Sport Manipulative 'Dark Patterns' Online*, Consumer Reports (Jan. 30, 2019), https://www.consumerreports.org/privacy/how-to-spot-manipulative-dark-patterns-online/.

[37] *Id.*

Commissioner's Office on "age-appropriate design" describes "sticky" features like "reward loops, continuous scrolling, notifications and auto-play features, which encourage users to continue playing a game, watching video content or otherwise staying online." It found that these types of intentionally persuasive design techniques may be overly coercive for children.[38]

Examples of manipulative design intended to coax more data, money, or time spent on kids' platforms abound. Our investigation of children's apps on the Google Play Store, as well as a study by researchers at the University of Michigan,[39] found that children's apps in the family section of the Google Play Store were filled with disruptive and manipulative advertising. For example, we saw ads disguised as game content so that children would mistakenly click on them.[40] We also found content that was highly manipulative, such as an app in which Strawberry Shortcake told the child that the puppy will be sad unless she makes an in-app purchase of a "treat" For it.[41] These games prey on children's vulnerabilities—difficulty closing ads, frustration with frequent interruption, a desire to please to wring data and revenue from them. And of course, the more time that a child or teen spends using these apps, the more information companies can collect and use to manipulate them.

We agree with Professor Ohm's comments at the April 9 hearing rejecting the concept that when strong privacy preferences contrast with non-privacy-protective behavior, the behavior "reveals" consumers' true preference. The inability of teens and parents to navigate a broken system doesn't indicate privacy apathy; it indicates that the system is broken. Or, as Professor

---

[38] Information Commissioner's Office, *Age-Appropriate Design* Code, 37-8 (April 2019), https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf.

[39] Marisa Meyer, et al., *Advertising in Young Children's Apps: A Content Study*, J. of Developmental & Behavioral Pediatrics (Oct. 29. 2018).

[40] Google Play Complaint at 35-36.

[41] *Id.* at 43-43, Meyer at 4-5.

Ohm put it, "it's crazy think that any of the preferences that we're measuring in any of these "studies" are revealed. They're manipulated, they're bought, they're controlled. We're talking about companies that have made their great wealth by being the greatest purveyors of information that the globe has ever seen. And so the fact that they can trick people to act against their preferences is not surprising."[42]

E. Pervasive Tracking of Children and Teens is Harmful

The pervasive tracking the online behaviors of children and teens puts young people at significant risk of harm. Here are just a few examples;

- Data brokers have compiled lists of students based on criteria such as "fourteen and fifteen year old girls for family planning services."[43]

- Student data brokers have catalogued children on the basis of descriptors like "affected by September 11th attacks," "refugee/immigrant," "down syndrome" or "clinically depressed." Some of these categories include children as young as two years old.[44]

- Wearable devices, growth monitors, and fitness trackers collect extremely sensitive information about children, particularly their health data and location, which could be used to sort and filter students in unexpected and detrimental ways.[45]

- Facebook has the ability to monitor posts and photos in real time to determine the emotional state of young people, for example, when they feel stressed, overwhelmed, or anxious, and to make this information available to advertisers.[46]

---

[42] Federal Trade Commission, *Transcript: Competition and Consumer Protection In the 21st Century*, 34-5 (April 9, 2019) https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_1_4-9-19.pdf.

[43] N. Russell et al, *Transparency and the Marketplace for Student Data*, 22 Virginia Journal of Law & Technology 3, 115 (Spring 2019), http://vjolt.org/wp-content/uploads/2019/04/Russell_Transparency_22_1_3.pdf;

[44] *Id.* at 135; 115.

[45] Deborah Lupton & Ben Williamson, *The datafied child: The dataveillance of children and implications for their rights,* 19 new media and society 5, 783-784; *Id.* at 785 (2017).

[46] Sam Levin, *Facebook told advertisers it can identify teens feeling 'insecure' and worthless*, The Guardian, May 1, 2017, https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-

As shown by the Georgetown Center on Privacy and Technology, opaque and unreliable automated decision-making can have a very real and dangerous impact on the lives and opportunities of children and teens, especially those from economically disadvantaged families.[47] We also agree with the Georgetown Center on Privacy and Technology that when it comes to teens, the FTC should recognize privacy violations themselves as harms.[48]

We urge the FTC to support new legislation to extend appropriate privacy protection to teens. New legislation should also replace the unrealistic expectation that parents can safeguard their children's privacy by choosing whether or not to give consent after reading privacy policies, and instead, prohibit practices that are harmful and unfair to children.

III. Even without new legislation, the FTC can take steps to better protect children's privacy

Even in the absence of new legislation, however, the FTC can and should take actions to better protect children's privacy. Specifically, we urge that the FCC bring more COPPA enforcements action, ensure that companies comply with COPPA's notice requirements, and to make sure that COPPA safe harbors are in fact ensuring that their members comply with COPPA.

---

teens. Facebook also conducted a secret experiment in which it manipulated information posted on users' home pages and found that it could change their emotional state. Id.

[47] *Competition and Consumer Protection in the 21st Century: Algorithms, Artificial Intelligence, and Predictive Analytics*, Docket No. FTC-2018-0101-0001 (Feb. 15. 2019), https://drive.google.com/file/u/1/d/1th6wNCY6QfC1oKtshed8yArnkWXttei0/view?usp=sharing

[48] Georgetown Law Center on Privacy & Technology, *Comments on FTC Hearing on Competition and Consumer Protection in the 21st Century* 9-10 (Dec. 31, 2019), https://drive.google.com/file/d/1OZvjBpBWrmlbLSr0OdeJAccZ-9MmBDVB/view. No separate showing of harm is required under COPPA.

A. The FTC should enforce the existing COPPA Rules more effectively

The small number of enforcement actions brought by the FTC, as well as the generally low civil penalties imposed, have created a climate in which companies have little incentive to comply with COPPA. Given the large number of providers that have child-directed websites or online services, or have actual knowledge that children are using their services, the chance that the FTC will take an enforcement action against an particular company is miniscule. Second, even when the FTC has acted, it has often imposed civil penalties so low that companies may view them as simply the cost of doing business. Consequently, it is not surprising that many companies seem to be ignoring the COPPA requirements.

1. The FTC rarely brings enforcement actions under COPPA

Since COPPA took effect in 2000, the FTC has brought only 29 actions to enforce COPPA, or an average of 1.5 per year.[49] None of these cases were litigated. Instead, they were settled by entering into a consent decree prohibiting further COPPA violations. Consent decrees provide only limited relief, as they are binding only on the parties to the decree. Consent decrees also provide much less guidance for interpreting COPPA rules than litigated cases.

All but one consent decree have included civil penalties ranging from a low of $10,000 to a high of $5.7 million. The largest civil penalty was imposed earlier this year when the FTC

[49] Neither the states nor COPPA self-regulatory bodies have stepped in to fill the gap caused by the FTC's lack of enforcement. In rare instances, the FTC has sent letters warning companies that were not in compliance with COPPA. For example, in April 2018, the FTC sent letters to Gator Group and Tinitell warning that their apps, connected to "smartwatches," were not in compliance with COPPA because they collected children's geolocation without notice and consent. *FTC letter to Gator Group Cp., Ltd., on potential violation of COPPA*, (Apr. 26, 2018), https://www.ftc.gov/system/files/attachments/press-releases/ftc-warns-gator-group-tinitell-online-services-might-violate-coppa/coppa_gator_group_co_ltd_letter_4-26-18.pdf; *FTC letter to Tinitell, Inc. on potential violation of COPPA*, (Apr. 26, 2018), https://www.ftc.gov/system/files/attachments/press-releases/ftc-warns-gator-group-tinitell-online-services-might-violate-coppa/coppa_tinitell_inc_letter_4-26-18.pdf.

settled with Musical.ly.[50] But even the civil penalty assessed against Musical.ly's, is extremely small compared to the financial resources of its parent company Bytedance, which was recently valued at $75 billion.[51]

The FTC has no formal process for members of the public to file complaints and to get relief. Nor does it make public when it undertakes an investigation or report on the outcome. The FTC has not acted – at least publicly – in response to any of the many COPPA complaints filed by CCD, CCFC, and IPR. It is particularly concerning that the FTC has not taken any enforcement action against Google for the ongoing COPPA violations on YouTube. As we documented in our April 2018 complaint, YouTube is the most popular online destination for children and is rife with content designed for young kids. The FTC's failure to act more than a year after the complaint was filed sends the message to website operators and app developers that they can evade COPPA's requirements if they pretend their service is not child-directed.

2. Many companies fail to comply with COPPA requirements

When the FTC is seen as ineffectual and unlikely to do anything, and companies are rewarded in the market for collecting and using large amounts of data, it is not surprising that COPPA violations are rampant. Many 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

[50] *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.

[51] Bytedance Is Said to Secure Funding at Record $75 Billion Value, Bloomberg News (October 26, 2018), https://www.bloomberg.com/news/articles/2018-10-26/bytedance-is-said-to-secure-funding-at-record-75-billion-value. The $5.7 million civil penalty thus amounted to 0.0076% of its estimated valuation.

the most third-party trackers of any category (tied with news).[52] Another study by computer scientists at UC Berkeley found that examined 5,855 of the most popular free children's apps in the Google Play store. It found that a majority were potentially in violation of COPPA, mainly due to their use of third-party SDKs. It noted that while many of these SDKs offer configuration options to respect COPPA by disabling tracking and behavioral advertising, the majority of apps either do not make use of these options or incorrectly propagate them across mediation SDKs. [53] It also found that 19% of children's apps collect identifiers or other personally identifiable information via SDKs whose terms of service outright prohibit their use in child-directed apps.

Other studies have found widespread security weaknesses in internet connected toys and gadgets used by children. 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.[54] They discovered several publicly undisclosed vulnerabilities such as a lack

---

[52] Reuben Binns, et al., *Third Party Tracking in the Mobile Ecosystem* at 6, Association for Computing Machinery, (May 2018), https://arxiv.org/pdf/1804.03603.pdf.

[53] Irwin Reyes, et al. *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, 63-83, Proceedings on Privacy Enhancing Technologies: 2018 (April 2018), https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf.

[54] Gordon Chu, Noah Apthorpe & Nick Feamster, *Security and Privacy Analyses of Internet of Things Children's Toys*, 6 IEEE Internet of Things Journal, 979-83 (Feb. 2019), 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 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/teksta-toucan-can-listen-to-kids-researchers-security/; Lorenzo Franceschi-Bicchierai, *Internet of Things Teddy Bear Leaked 2 Million Parent and Kids*

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." [55]

These examples illustrate the need for the FTC to bring more COPPA enforcement actions. In so doing, it is particularly important that the FTC act quickly, so that developers will feel the need to pay attention to privacy rules, and security weaknesses will be minimized. Unfortunately, it took the FTC more than two years after reports came out that digital toy company Vtech experienced a massive breach of children's data before the FTC reached a settlement with Vtech.[56]

B. The FCC should enforce COPPA's requirements regarding parental notice

Not only should the FTC bring more enforcement actions on a timely basis, but it should enforce all COPPA provisions. Our experience reviewing online services directed at children suggests that the FTC has been exceptionally lax in enforcing COPPA's requirement that

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; Samuel Gibbs, *Hackers can hijack Wi-Fi Hello Barbie to spy on your children*, The Guardian (Nov. 26, 2016), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children.

[55] Chu et al. at 978-79.

[56] *Compare* Daniel Victor, *Security Breach at Toy Maker Vtech Includes Data on Children*, NY Times, Nov. 30, 2015, with FTC Press Release, *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act,* Jan. 8, 2018, https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

parental notice "must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory material regarding adequate notice."[57]

Even though, as discussed above, parental notice and choice is no longer a realistic way to protect children's privacy, there is still tremendous value in the FTC enforcing the COPPA notice requirements. A well-written privacy policy remains the best way to determine what data is collected, how it is used, and whether it is shared with third parties. Even if privacy policies are not very helpful to parents to make informed decisions on an individual basis, they provide valuable information for regulators, researchers, and advocates.

We have reviewed numerous privacy policies and found that many do not comply with the notice requirements set out in Rule 312.4. See supra at 13-14. Often, they fail to list exactly what kind of information is collected or how it is used. Similarly, privacy policies are often confusing, contradictory or simply unclear. Furthermore, even though the FTC's guidance that the COPPA rule is "not just for kids' sites,"[58] many websites and online services aimed at general audience that include children, such as YouTube, do not have even have a children's privacy policy.

While the COPPA rule explicitly requires companies to provide the name, address, phone number, and email address of any third party collecting information about child users, companies frequently fail to do so. For example, Amazon's children's privacy policy does not list the third parties that collect or receive children's personal information and improperly tells parents that it

[57] 16 CFR 312.4(a).

[58] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy.

has no responsibility for third party collection.[59] Thus, the FTC should strictly enforce COPPA's notice requirements.

C. The FTC should hold COPPA safe harbors accountable for enforcing COPPA

The FTC should also do more to ensure that COPPA safe harbors are functioning effectively. COPPA allows entities subject to COPPA to satisfy the law by following a set of self-regulatory guidelines issued by an approved COPPA Safe Harbor.[60] COPPA Safe Harbors must apply to the FTC for approval. The FTC rules require that a safe harbor provide at least as much protection as the FTC's COPPA rules. The FTC has stated that the purpose of the safe harbor program is to

> to encourage industry members and other groups to develop their own COPPA oversight programs, thereby promoting efficiency and flexibility in complying with COPPA's substantive provisions.306 COPPA's safe harbor provision also was intended to reward operators' good faith efforts to comply with COPPA. The Rule therefore provides that operators fully complying with an approved safe harbor program will be ''deemed to be in compliance'' with the Rule for purposes of enforcement. In lieu of formal enforcement actions, such operators instead are subject first to the safe harbor program's own review and disciplinary procedures.[61]

The Children's Advertising Review Unit (CARU) filed the first application for approval of a safe harbor program in April 2000, the same month that the COPPA rules took effect. CARU subsequently revised the guidelines to respond to public comments, and the FTC approved the application in January 2001. Also in 2001, the FCC approved two more COPPA safe harbors— Entertainment Software Rating Board (ESRB) and TRUSTe. It has since approved four more -- Privacy Vaults Online, Inc. (PRIVO), Aristotle International, Inc.,

[59] Echo Dot Kids Complaint at 24-5.

[60] 15 USC §6053.

[61] Statement of Basis and Purpose, 78 Fed. Reg. at 3995-96.

iKeepSafe, and kidSAFE. Two of the seven safe harbors – CARU and ESRB – are operated by industry-supported non-profit organizations, while the others are for-profit entities.

When the FTC launched its review of the COPPA Rule in 2010, CDD, CCFC, and other organizations represented by IPR, asked the FTC to take action to assure the effectiveness of the safe harbor program.

> First, [the FTC] should determine what proportion of child-directed websites and online service operators participate in a safe harbor program. Second, it should assess the effectiveness of the safe harbor programs by requiring annual reports about their enforcement efforts. Third, to ensure that the safe harbor programs are keeping up to date on new threats to children's privacy, it should require them to apply for recertification every five years.[62]

While the FTC did not adopt all of these proposals, it did take steps to strengthen the COPPA Safe Harbor program.[63] Specifically, it "mandate[d] that (at a minimum) safe harbor programs conduct annual, comprehensive reviews of each of their members' information practices."[64] It also required applicants" to explain in detail their business model and their technological capabilities and mechanisms for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program." Finally, it required approved safe harbors to submit an annual report to the FTC containing an aggregated summary of the result of its independent assessments.[65]

---

[62] Comments of CDD et al., No. P104503, at iv & 37, June 30, 2010.

[63] Statement of Basis and Purpose, 78 Fed. Reg. at 3996.

[64] *Id.*

[65] *Id.* Initially, the FTC proposed that the annual reports list names of members that were not in compliance, but it changed this proposal, finding that "While commenters generally supported stronger Commission oversight of safe harbor activities post-approval, they were concerned that a requirement forcing safe harbors to 'name names' of violative member operators would chill the programs' abilities to recruit and retain members, and generally would be counter to notions of self-regulation."

1. The FTC should make public all information in the safe harbor annual reports

CDD and CCFC expected the FTC to make these annual reports available for public comment, just as it does for the applications.[66] But it did not, and so CDD and IPR filed FOIA requests for both the 2014 and 2015 annual reports. Eventually, the FTC released the reports, but virtually all information that could permit an analysis of their effectiveness was redacted.[67]

A more recent review conducted by the Technologist in Commissioner Chopra's office, found that many safe harbor programs "received very few, often zero, complaints." It also found that few safe harbor programs disciplined or suspended operators for noncompliance.[68] These findings are very troubling. Thus, it is important that the FTC make the full reports available to the public so that there can be a rigorous assessment of the effectiveness of the safe harbor program.

2. The small number of complaints does not mean that safe harbor members are complying with COPPA

It would be incorrect to infer from the small number of complaints that the COPPA safe harbors are working well. That might be a plausible claim only if parents recognized the privacy

---

[66] This belief was supported by the FTC's decision to only require reporting in the aggregate. The FTC expressed concern that "a requirement forcing safe harbors to ''name names'' of violative member operators would chill the programs' abilities to recruit and retain members, and generally would be counter to notions of self-regulation." SPB at 3996.

[67] For example, every report filed in 2014 had some information redacted, and in some cases, entire pages, sections and exhibits were redacted in their entirety. Quantitative data, such as the number of companies participating in the safe harbor, the number of properties, websites or mobile apps participating, the number of new members, the number of members that dropped out, and the number approved were redacted. as were the categories of enforcement/complaints and other information.

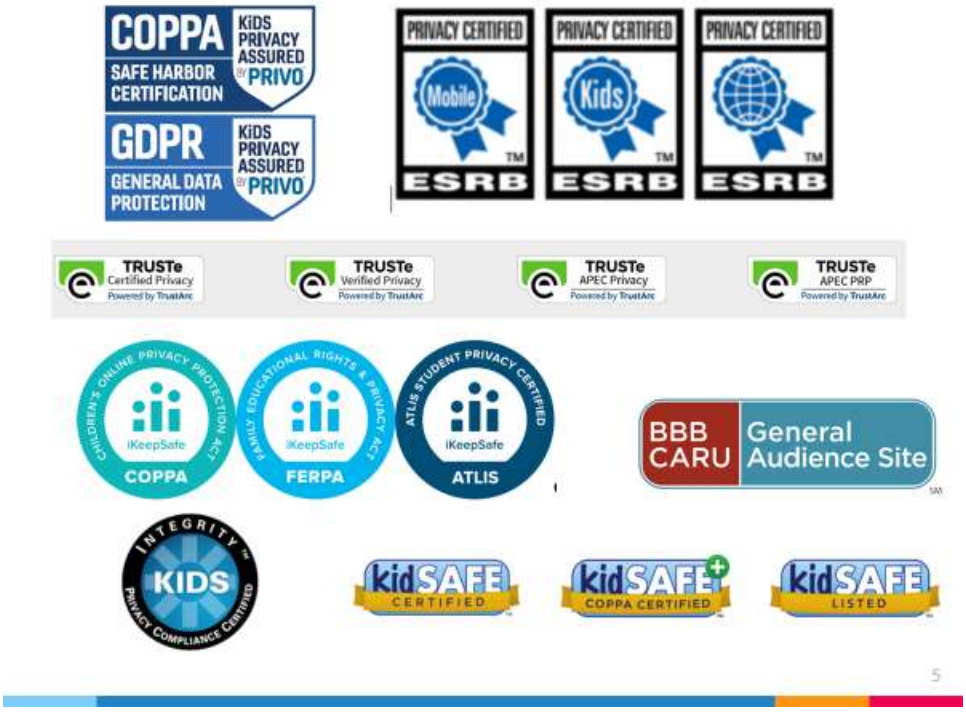
[68] Prepared Remarks of Federal Trade Commissioner Rohit Chopra at Truth About Tech Conference, at 3-4 (April 4, 2019, https://www.ftc.gov/system/files/documents/public_statements/1512078/chopra_-_truth_about_tech_4-4-19.pdf.

seals, correctly understood their meaning, knew that they had a right to file a complaint, and had an incentive to file a complaint. Yet, these conditions do not exist.

FCC rules require that the COPPA safe harbors review their members' privacy practices at least annually. If the members are found in in compliance, they may display a seal signifying that they comply with COPPA. The seal is intended to assist parents in deciding whether to allow their child to use a particular website or online service.

Since most COPPA safe harbors refuse to publicly disclose their members, parents have no easy way of finding websites and online services that participate in a safe harbor; they only find out that a website or on-line service is part of a safe harbor program if they see the seal or they read the privacy policy. Oftentimes, seals are not easy to find.

Even if parents see a seal, they are likely to be confused about what it means. Not only are there seven different seal programs, but several have multiple types of seals, as shown below.



Parents are unlikely to understand, for example, that of the three nearly identical kidSafe seals, only the one that includes "kidsSafe COPPA certificate" have been reviewed for COPPA compliance.

Even if parents recognize a COPPA safe harbor seal, they may not realize its significance. Safe harbor seals may mislead parents into a false sense of security. Parents may see an official-looking seal and assume that it means that the website or online service will protect their child's privacy. But in fact, it only means that the website or online service complies with the safe harbor guidelines. It does not mean, as some might believe, that no personal information is collected. Nor does it relieve parents from the burden of reading and trying to understand privacy policies.

Finally, even if a parent understands what COPPA requires and determines that a website or online service displaying a seal is not in compliance, it is unclear what incentives busy parents would have to file a complaint with the safe harbor. The costs of filing such a complaint would surely outweigh any benefit. At best, the member might be required to change its practices, but the parent filing the complaint would not be able to obtain any monetary or other relief.

3. COPPA Safe harbors lack the incentive to rigorously enforce their guidelines

Companies that comply with an FTC-approve safe harbor program are exempt from agency COPPA enforcement. While as discussed above, the FTC rarely enforces COPPA, when it does, it can result in substantial civil penalties, such as those assessed against Musical.ly. In these circumstances, as Commissioner Chopra has observed, it is "hard for anyone to bite the hand that feeds them. Whenever regulated entities pay fees and shop for a regulator, are there the

right incentives for the regulators to be tough? Or might the incentives lead to competition on who can be the most lax and forgiving?"[69]

Commissioner Chopra cites as an example the for-profit company TRUSTe, which failed to carry out the required annual recertifications of its members.[70] But this problem is not limited to for-profit safe harbors. Non-profit CARU receives its funding from the advertising industry, while the ESRB receives funding from the video game industry. It is in the interests of both industry groups that the guidelines should not be rigorously enforced, and they would be unlikely to continue these programs if it hurt their members' bottom line. Moreover, the nonprofit safe harbors see themselves a competing with the for-profit companies. At an event last fall, the head of CARU's safe harbor program stated that CARU no longer publishes a list of its members because when they did, other safe harbor programs "poached them."[71] While such competition may lower the costs for safe harbor members, this "race to the bottom" is harmful to consumers.

To ensure that COPPA safe harbors protect children's privacy rather than protect their members from FTC enforcement, the FTC needs to make its oversight process more transparent. The FTC should require the safe harbors, as organizations delegated to perform a government regulatory function, to make their annual reports public. If safe harbors are not willing to make public information necessary for to assess their performance, or otherwise perform their responsibilities, the FTC should decertify them.

---

[69] Prepared Remarks of Federal Trade Commissioner Rohit Chopra at Truth About Tech Conference, at 3 (April 4, 2019) https://www.ftc.gov/system/files/documents/public_statements/1512078/chopra_-_truth_about_tech_4-4-19.pdf; *id.*, at 4

[70] *Id.*

[71] Dona Fraser from CARU, Panel 3 - Enforcing COPPA: Successes, Challenges & Opportunities, October 24, 2018 3:15-4:30 PM, COPPA at 20: Protecting Children's Privacy in the New Digital Era, available at https://www.georgetowntech.org/coppa.

IV. Conclusion

Because notice and consent no longer provide an effective means to protect the privacy of children, the FTC should call for new legislation that prohibits practices that may be harmful to children, rather than requiring parents to read and try to understand the impact of multiple privacy policies. Legislation should also include developmentally-appropriate protections for teens, because COPPA only covers children under age 13. Until such legislation is passed, however, the FTC can and should do more to better protect children's privacy. Specifically, we urge the FTC to undertake more enforcement actions, to enforce COPPA's notice requirements, and to fix problems with the COPPA safe harbor program.

Respectfully submitted,

/s/ Angela J. Campbell
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

Attachment

Requests to Investigate COPPA violations filed by CDD and/or CCFC

Amazon, Inc.'s Echo Dot Kids Edition for Violating the Children's Online Privacy Protection Act, May 9, 2019, https://commercialfreechildhood.org/sites/default/files/devel-generate/ciw/echo_dot_complaint.pdf.

Google's Unfair and Deceptive Practices in Marketing Apps for Children, Dec. 18, 2018, https://www.democraticmedia.org/sites/default/files/field/public-files/2018/12-19_google_play_store_complaint_with_exhibits.pdf.

Letter to Donald S. Clark from James T. Graves regarding Facebook Messenger Kids, Oct. 3, 2018, https://www.commercialfreechildhood.org/sites/default/files/devel-generate/wab/FTC%20FB%20Messenger%20Kids%20Letter.pdf

Google's YouTube Online Services and Advertising Practices for Violating the Children's Online Privacy Protection Act, Apr. 9, 2018, https://www.law.georgetown.edu/wp-content/uploads/2018/08/Filed-Request-to-Investigate-Google%E2%80%99s-YouTube-Online-Service-and-Advertising-Practices-for-Violating-COPPA.pdf.

Genesis Toys and Nuance Communications (My Friend Cayla doll), Dec. 6, 2016, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

The Topps Company, Inc., Operator of Candymania.com, for Violation of the Children's Online Privacy Protection Act, Dec. 9, 2014.

Sanrio's Violation of the Children's Online Privacy Protection Act in Connection with Hello Kitty Carnival Mobile Application, Dec. 18, 2013

Disney and Marvel's Violation of the Children's Online Privacy Protection Act Rule in Connection with Marvelkids.com, Dec. 18, 2013.

Requests to Investigate "Mobbles" and "SpongeBob Diner Dash," Two Child-Directed Mobile Applications, Dec. 17, 2012

General Mills, Inc.'s Violation of the Children's Online Privacy Protection Act in Connection with TrixWorld.com and ReesesPuffs.com, Aug. 22, 2012

McDonald's Corporation's Violation of the Children's Online Privacy Protection Act in Connection with HappyMeal.com, Aug. 22, 2012

Viacom, Inc.'s Violation of the Children's Online Privacy Protection Act in Connection with Nick.com, Aug. 22, 2012

Doctor's Associates, Inc.'s Violation of the Children's Online Privacy Protection Act in Connection with SubwayKids.com, Aug. 22, 2012

Turner Broadcasting Systems, Inc.'s Violation of the Children's Online Privacy Protection Act in Connection with CartoonNetwork.com, Aug. 22, 2012.