UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Alvaro M. Bedoya

Statement of Commissioner Alvaro M. Bedoya
On the Issuance of the Notice of Proposed Rulemaking to
Update the Children's Online Privacy Protection Rule (COPPA Rule)

December 20, 2023

I. What harms was COPPA intended to prevent?

Today, for the third time in a quarter century, the Commission is issuing a Notice of Proposed Rulemaking to issue or update regulations implementing the Children's Online Protection Act, 15 U.S.C. § 6501, *et. seq.* Attention to this notice may rightly focus on the important ways in which—as directed by Congress—the Commission proposes to update the COPPA Rule to keep up with advancing technology. On this front, I am most proud of how the proposed rule (1) expressly protects a range of biometric identifiers as personal information; (2) ensures that companies do not abuse the exceptions to the consent rules to nudge children to engage with online platforms for longer than they want; and (3) expressly tells companies that they cannot keep children's information forever—a critical protection when new, machine learning-fueled systems require ever larger amounts of training data.[1]

In this Statement, I would like to take a step back to address a critique that has quietly proliferated around children's privacy: the idea that many privacy invasions do not actually hurt children. We've heard it from my friend and former colleague Commissioner Noah Phillips, who wrote in 2020 that "[m]any violations of data privacy statutes on the books today—including COPPA—regulate conduct that does not involve a great deal of harm, at least as harm is traditionally considered."[2] We've heard it from former staff presenting at COPPA workshops.[3] Most recently, we've heard it from a federal judge in California who preliminarily enjoined California's Age-Appropriate Design Code, and in doing so, implicitly raised a much broader set of questions about the potential harms to children from privacy invasions.[4] Arguments like these are most commonly raised in discussions about surveillance related to online behavioral tracking.

---

[1] *See* Statement of Commissioner Alvaro M. Bedoya, joined by Chair Lina M. Khan & Comm'r Rebecca Kelly Slaughter, In the Matter of Amazon Alexa (*United States v. Amazon.com, Inc.*) (May 31, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya-Statement-on-Alexa-Joined-by-LK-and-RKS-Final-1233pm.pdf.

[2] Statement of Commissioner Noah Joshua Phillips, *FTC v. HyperBeard, Inc., et al.*, at 3, https://www.ftc.gov/system/files/documents/public_statements/1576434/192_3109_hyperbeard_-_dissenting_statement_of_commissioner_noah_j_phillips.pdf. In fairness, Commissioner Phillips followed this with a recognition that "COPPA violations also do reach conduct that is more obviously harmful." *Id.* at 4.

[3] Remarks of Dr. James C. Cooper, *The Future of the COPPA Rule: An FTC Workshop*, Transcript of COPPA Workshop, Part 2 (Oct. 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_2_1.pdf ("And what is the harm we're talking about? What is the injury?").

[4] *Netchoice, LLC v. Bonta*, No. 22-cv-08861-BLF, 2023 WL 6135551, at *17 (N.D. Cal. Sept. 18, 2023) ("the State provides no evidence of a harm to children's well-being from the use of personal information for multiple

Given these challenges, I think it is useful to look through the 25-year history of COPPA's origins, enactment, implementation, and enforcement and ask: What harms is COPPA intended to prevent? Who does the collection, use, retention, and disclosure of children's information really hurt, and how much?

I think a review of that record shows a broad consensus across Congress, the Commission, civil society, and industry that the unauthorized or unnecessary collection, use, retention, and disclosure of children's information (1) endangers children's safety; (2) exposes children and their families to hacks and data breaches; and (3) allows third-party companies to develop commercial relationships with children that prey on their trust and vulnerability. I think each of these harms, particularly the latter, undermines the idea that the pervasive tracking of children online is "victimless crime."

II. Privacy invasions endanger children.

COPPA was passed in 1998 in response to FTC research revealing that websites directed to children were collecting a barrage of personal information from them—often without notifying or getting permission from their parents. In a survey of 212 sites directed to children, 89% collected personal information from children, including their names, emails, physical address, phone numbers, dates of birth, gender, as well as, in some cases, information about their parents' incomes, occupations, education levels, and Social Security numbers.[5] Senator Richard Bryan of Nevada, the lead sponsor of COPPA, was "surprised" and "startled" by these findings, and the resultant COPPA legislation was crafted in direct response to that study.[6]

Child safety was a core concern of the FTC's and of Senator Bryan. In 1997, the FTC issued its first advisory opinion on a matter touching upon children's privacy. The opinion concerned a pen-pal website called "KidsCom," which collected children's contact information and released it to other "key pals" without notifying or getting permission from parents. In a letter to the Center for Media Education (now known as the Center for Digital Democracy), the director of the FTC's Bureau of Consumer Protection went out of her way to recognize that "the release of children's personally identifiable information to third parties creates a risk of injury or exploitation of the children so identified," specifically citing testimony from the Federal Bureau of Investigation expressing a particular concern about the release of information that "create[s] a possibility of access by child predators."[7]

---

purposes"); *id.* ("the State has not shown a harm resulting from the provision of more personal information 'beyond what is reasonably expected' for the covered business to provide its online service, product, or feature"); *id.* ("the State has not shown that dark patterns causing children to forego privacy protections constitutes a real harm"); and *id.* at *18. ("the State does not show how this law indicates a harm to minors caused by the sale of personal information").

[5] *See* Federal Trade Commission, *Privacy Online: A Report to Congress* at 31-42 (June 1998) (hereinafter "1998 FTC Report").

[6] *See* 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan); *S. 2326: Children's Online Privacy Protection Act of 1998*, Hearing before Senate Subcomm. on Communications, Comm, on Commerce, Science, and Transportation, 105th Cong. 3, (1998) (Statement of Sen. Burns) (COPPA "drew heavily" from the FTC report).

[7] *See* Letter from Jodi Bernstein, Fed. Trade Comm'n, Dir. of Consumer Prot., to Kathryn C. Montgomery, President, Center of Media Educ. at 5 n. 12 (July 15, 1997).

The FTC's subsequent investigation into children's privacy in 1998 revealed instances in which websites requested highly personal information from children which were very difficult to justify from a business perspective.[8] When Senator Bryan went to the Senate floor to introduce COPPA, he highlighted some of the most unnerving requests: "Some [websites] were asking where the child went to school, what sports he or she liked, what siblings they had, their pet's name, *what kind of time they had after school alone without the supervision of parents*."[9] Indeed, Senator Bryan expressly invoked the threats to children's safety posed by data collection and dissemination at least three times in his short introduction speech.[10]

Safety was also a focus for the Federal Trade Commission when it initially promulgated the first rule to implement COPPA in 1999. In promulgating what is now current rule § 312.5(a)(2)—allowing parents to separately consent to any *disclosures* of a child's personal information to third parties—the Commission explained that the comment record "show[ed] that disclosures to third parties are among the most sensitive and potentially risky uses of children's personal information."[11] Similar reasoning can be found in the Commission's 2011 proposal to add geolocation information to the list of personal information protected by COPPA.[12]

The FTC's COPPA enforcement record since the issuance of the most recent rule update in 2013 reveals that potential threats to child safety from the unauthorized and unnecessary collection, use, retention, and disclosure of children's data remain widespread.

- In 2013, the FTC filed and settled COPPA charges against Path, Inc., the owner of a social networking online service that allegedly knowingly collected precise location and other personal information from children and enabled children to post it to up to 150 of the child's contacts on the service—without first obtaining their parents' permission.[13]

- In 2018, the FTC filed and settled COPPA charges against a website ostensibly directed to new actors that allegedly (1) requested—from over 100,000 users under 13—information on home address, "body type"; measurements of their "waist," "hips" and "bust"; and (2) allowed adult users to "friend" and exchange direct private messages with those users, all without parental notification and consent.[14]

- In 2019, the FTC filed and settled COPPA charges against the Musical.ly app (now known as TikTok) for allegedly (1) making public the profile photos and videos of their users (including a significant number of children); (2) allowing adults to identify other

[8] *See* 1998 FTC Report at 31–34, 39–40.
[9] *See* 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan) (emphasis added).
[10] *See e.g., id.* (advances in technology "leav[e] [children] unwittingly vulnerable to exploitation and harm by… criminals").
[11] *See* 64 Fed. Reg. 59899 (Nov. 3, 1999).
[12] *See* 76 Fed. Reg. 59804, 59813 (Sept. 27, 2011) ("Numerous commenters raised with the Commission the issue of the potential risks associated with operators' collection of geolocation information from children.").
[13] *See* Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 3, 6-10, *United States v. Path, Inc.,* No 3:13-cv-00448-RS (N.D. Cal. Feb. 8, 2013).
[14] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 7–9, *United States v. Prime Sites*, No. 2:18-cv-00199 (D. Nev. Feb. 5, 2018).

> users within a 50-mile radius; and (3) allowing adults to freely send those users direct messages. According to public reports, this configuration resulted in adults messaging and sexually harassing children. [15]

Perhaps the most compelling COPPA case illustrating the dangers of certain design choices and unauthorized data collection, use, and disclosure is the *Epic Games* case, which the FTC brought and settled against the maker of the popular video game Fortnite. There, in addition to alleging that the company violated COPPA by failing to obtain consent from parents before collecting personal information from children, the FTC alleged that Epic Games configured Fortnite's default privacy settings to allow adults to directly speak, via live audio feed, to other players, including children 12 and under, and obscured the option to disable the voice chat by failing to inform users that the company created and rolled out a "toggle switch" for that purpose. [16]

Unfortunately, the company also allegedly used design techniques that obscured this "toggle switch", burying the switch "on a hard-to-find settings page," where it was "in the middle of a detailed" series of settings. [17] The FTC complaint alleged that these actions helped create an environment where "kids have been bullied, threatened, and harassed, including sexually, through Fortnite," and that news stories and player support tickets document "predators blackmailing, extorting, or coercing children and teens they met through Fortnite into sharing explicit images or meeting offline for sexual activity." [18]

III. Privacy invasions expose children and their families to hacks and data breaches.

While data breaches and identity theft were far less common in the late 1990s than they are today, the record of COPPA's passage shows that the FTC and the legislators who enacted COPPA were presciently aware of the security dangers of unnecessarily collecting excessive personal information from children.

In its 1998 report, the FTC uncovered instances in which websites asked children extremely detailed information about their family's finances. The report described one such site:

> A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The Web site also asks a child extensive personal finance questions, such as whether a child has received gifts in the form of stocks, cash, savings bonds, mutual funds, or certificates of deposit; who has given a child these gifts; whether a child puts monetary gifts into mutual funds, stocks or bonds; and whether a child's parents own mutual funds.

---

[15] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 4–7, *United States v. Musical.ly*, No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019); *see also Dad warns of potential privacy dangers for children in Musical.ly app*, ABC News, (Aug. 24, 2017, 8:43 AM), https://abcnews.go.com/Lifestyle/dad-warns-potential-privacy-dangers-children-musically-app/story?id=49387669 (Illinois father reporting "a stranger asked his 7-year-old daughter to send shirtless pictures of herself through the app's messaging feature").

[16] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 17–22, *United States v. Epic Games, Inc.* No. 5:22-cv-00518-BO (E.D.N.C. Dec. 12, 2022).

[17] *Id.* at 20–21.

[18] *Id.* at 18.

> Elsewhere on the Web site, contest winners' full names, age, city, state, and zip code are posted. [19]

Senator Bryan discussed this very website when he introduced COPPA on the floor of the Senate. He went on to identify data security as one of five key goals for the bill. [20] As a result, the COPPA statute and implementing regulations include a range of data security requirements, including the above-cited prohibition against the unnecessary retention of children's data. [21]

Congress and the FTC understood that collecting unnecessary data from kids—and retaining it for longer than needed—imposed obvious data security risks to children and their families. FTC's recent COPPA's enforcement cases show that too often, those risks become reality.

In 2018, for example, the FTC brought and settled COPPA charges against toymaker VTech Electronics Limited and its U.S. subsidiary (collectively "VTech") relating to "Kid Connect," an online service directed to, and primarily intended to be used by, children. Kid Connect allegedly allowed children to communicate with other children and their own parents, and to play online games. Kid Connect included accounts for almost 638,000 children. When children used Kid Connect, VTech allegedly collected and retained a detailed range of information from children and their parents, including children's photos, home addresses, and dates of birth. The FTC complaint alleged that a hacker broke into VTech's computer network in 2015 and gained access to much of that data. The complaint further alleged that if "a child had submitted a photo through Kid Connect, the hacker could have found that photo, along with their physical address." [22]

Just this year—at a time when the sound of one's voice can function as a form of identification or can be cloned by bad actors and used to commit fraud—the FTC encountered an instance where a highly sophisticated technology company allegedly opted to retain the voice recordings of tens of thousands of children forever, "in perpetuity," in violation of COPPA's prohibition against unreasonably long data retention. [23]

We are only at the beginning of an era of biometric fraud. The corporate practices I have encountered as a commissioner make me highly concerned about how companies are protecting children's biometric data against breaches, fraud, and abuse.

---

[19] 1998 FTC Report at 39.
[20] *See* 144 Cong. Rec. S8483 (July 17, 1998) ("Establish and maintain reasonable procedures to ensure the confidentiality, security… and integrity of personal information on children.").
[21] *See* 15 U.S.C. § 6502(b)(1)(D); 16 C.F.R. §§ 312.8, 312.10.
[22] *See* Complaint, *United States v. Vtech Electronics Ltd.* at 3–9, No. 1:18-cv-00114 (N.D. Ill. Jan 8, 2018); *see also United States v. Unixiz, Inc*., No. 5:19- cv-02222 (N.D. Cal. Apr. 24, 2019) (hack involving the usernames, email addresses, gender, and dates of birth of 245,000 users under 13).
[23] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 6–7, 14–15, *United States v. Amazon.com, Inc*., No. 2:23-cv-00811 (W.D Wash. May 31, 2023); *see also The FTC Voice Cloning Challenge*, Fed. Trade Comm'n, https://www ftc.gov/news-events/contests/ftc-voice-cloning-challenge (last visited Dec. 18, 2023) (discussing risks of voice cloning for fraud and impersonation).

IV. Privacy invasions let companies create commercial relationships with children that prey on their trust and vulnerability.

When we consider the harms of online behavioral advertising to children, we cannot forget one of the original reasons COPPA was envisioned and enacted: A desire to ensure that companies cannot build a commercial relationship with children that preys on their immaturity, honesty, and trust. When Senator Bryan wrote and introduced COPPA, this is what he focused on: how companies can use personal data to take advantage of children's trusting instincts and lack of judgment—deliberately outside of the protection of their parents:

> [C]ompanies are attempting to build a wealth of information about you and your family without an adult's approval – a profile that will enable them to target and to entice your children to purchase a range of products. The Internet gives marketers the capability of interacting with your children and developing a relationship without your knowledge. Where can this interactive relationship go? Will your child be receiving birthday cards and communications with online cartoon characters or particular products? […] If a child answers a phone and starts answering questions, a parent automatically becomes suspicious and asks who they are talking to. When a child is on the Internet, parents often have no knowledge of whom their child is interacting.[24]

Again, these concerns were grounded in the FTC's 1998 report, which raised specific concerns about children's vulnerability, "lack of developmental capacity[,] and judgment."[25]

These concerns were expounded upon at length in the Senate hearing held to consider the COPPA legislation. There, Senator Bryan again warned his colleagues that kids "are by their very nature honest and trusting, and when approached on the Internet by their favorite cartoon character… children will freely provide very personal and private information."[26]

One of the witnesses that day, Dr. Kathryn Montgomery, president of the Center for Media Education, memorably warned senators that "children are not little adults"—and that "many marketers have been willing to design their Web sites… in ways that tap into these vulnerabilities."[27] She gave as an example a Batman-related website that asked kids to fill out a form and told them: "Be a good citizen of Gotham and fill out this census." "The idea," she explained, "is to have the spokescharacter develop a personal relationship with the child and to ask the child for personal information."[28]

In perhaps her most prescient prediction, Dr. Montgomery warned about the dangers of "psychographic profiling":

---

[24] *See* 144 Cong. Rec. S8482–3.
[25] *See* 1998 FTC Report at 5-6.
[26] *See* Senate COPPA Hearing at 3.
[27] *See* Senate COPPA Hearing at 34 (statement of Dr. Montgomery).
[28] *Id.* at 34–-35.

> [E]ven now, marketers are able to collect, through this very sophisticated medium, not only the information that is volunteered, but tracking information which shows how a child responds to various messages. They are able to then track certain kinds of emotional responses of that child. There are a number of companies in the marketplace that are involved in the business of creating detailed psychographic profiles of people who use the online medium. So the capability there is to develop very, very sophisticated kinds of profiles that would potentially be a very harmful form of data collection.[29]

Sadly, the FTC's recent COPPA enforcement cases show that companies continue to take advantage of children's vulnerabilities to collect information to build increasingly sophisticated profiles on them, and to build commercial relationships with children, all outside of their parents' view.

The FTC has encountered this most frequently in the context of free online apps that attract children with cute animals or other activities to harvest their data through direct requests or through the otherwise invisible collection and sale of personal information, including persistent identifiers that can be used to track children across the web.

- In 2014, the FTC brought and settled COPPA charges against TinyCo, Inc., which offered a range of free online apps targeted at kids. "Raise dinosaurs, build valuable shops and complete amazing quests in your own prehistoric village!" promised one app that was downloaded 13 million times. "Build the BEST zoo and raise ADORABLE animals in Tiny Zoo Friends!" said another that was downloaded on 7 million occasions. The apps allegedly then asked kids to provide their email address, without their parents' permission, and even after parents complained about the practice.[30]

- In 2015, the FTC brought and settled COPPA charges against a company that let its app users make virtual cakes and pizzas, style hair, play with a talking dog, and hear animals sounds. The latter app was expressly targeted to parents who would be unable to consistently supervise their children; "keep your child entertained at a restaurant, during a long drive or while shopping," was how the company described the app in an online store. Yet, unbeknownst to the parents, the company allegedly allowed third-party advertising networks to collect persistent identifiers from the children that would allow targeted ads to be served to the children based on their activity across time and over *other* online sites.[31]

- That same year, the FTC brought and settled COPPA charges against a separate company that also offered children's apps, including games involving ice cream, pudding, cats, dogs, and cartoon characters afflicted with "Sneezies." "Meet a Happy Ice Cream Scoop who dreams of soaring through the skies," was how the company described one of the

---

[29] *Id.* at 35.
[30] *See* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4-6, *United States v. TinyCo, Inc*., No. 3:14-cv-04164 (N.D. Cal. Sept. 16, 2014).
[31] *See* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 6-8, *United States v. Lai Systems, LLC*, No. 2:15-cv-09691 (C.D. Cal. Dec. 17, 2015).

apps in an online app store. Again, unbeknownst to parents, the company allegedly allowed third-party advertising networks to collect information from those children, including persistent identifiers that would allow those advertising networks to track the children's activities across the Internet. [32]

The FTC also has encountered the problem of companies taking advantage of children's lack of sophistication to gather personal information from them in the school context, especially in the last few years when children often have had to engage with online education tools ("ed tech") to participate in a variety of school-related activities. In 2023, the FTC brought and settled COPPA charges against a company that offered virtual class spaces for teachers to host class discussions and share materials with students under age 13 and their parents. Without first obtaining parental permission, the company allowed third-party advertisers to collect personal information from those children, including persistent identifiers, to serve them with ads. [33]

Indeed, what is most concerning is that what appeared to be the most hyperbolic predictions at COPPA's passage have largely proven to be accurate. In 2016, for example, the FTC brought and settled COPPA charges against InMobi Pte Ltd., an online advertising company that tracked users' locations in thousands of child-directed apps with hundreds of millions of users without getting parents' consent. Not only did InMobi Pte Ltd. let third-party companies target those users with ads based on their present or future locations, but it also offered companies the ability to place "Psychographic" ads based on a two-month history of a particular user's movements. [34]

In the most recent workshop to consider the future of the COPPA Rule, Dr. Jenny Radesky, a pediatrician who has surveyed a range of children's apps and services online, summarized her concerns about this kind of targeting: "[A]pps can even capture our psychological profile. [They] can tell how impulsive we are, how hard workers [or] critical thinkers we are. I don't want my patients who have impulse control issues[,] who have immature frontal cortexes to be up against a really powerful ad network that has been able to collect data about them." [35]

---

[32] *See* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 7-10, *United States v. Retro Dreamer*, No. 5:15-cv-02569 (C.D. Cal. Dec. 17, 2015).
[33] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 4–6, *United States v. Edmodo, LLC*, No. 3:23-cv-02495 (N.D. Cal. May 22, 2023); *see* also Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act (May 19, 2022) (making clear that the FTC will crack down on companies that illegally surveilled children using ed tech tools).
[34] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 12–13, *United States v. InMobi Pte Ltd*., No. 3-15-cv-03474 (N.D. Cal. June 22, 2016).
[35] *See* Remarks of Dr. Jenny Radesky, *The Future of the COPPA Rule: An FTC Workshop*, Transcript of COPPA Workshop, Part 1 (Oct. 7, 2019), https://www.ftc.gov/news-events/events/2019/10/future-coppa-rule-ftc-workshop.

V. The harms that COPPA sought to prevent remain real, and COPPA remains relevant and profoundly important.

Thanks to the hard work of FTC staff in the Division of Privacy and Identity Protection and the government, civil society, and industry commenters who ensured they benefited from a rich comment record, the Children's Online Privacy Protection Rule will enter its second quarter century stronger and better prepared to protect children online. As we do that, we must remember why COPPA exists in the first place, and the very real harms to children's safety, data security, and trust that it was intended to prevent.