



Office of Commissioner  
Melissa Holyoak

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

HOW CAN WE USE EXISTING LAW TO PROTECT CHILDREN ONLINE?

**MELISSA HOLYOAK\***  
COMMISSIONER, U.S. FEDERAL TRADE COMMISSION

SEPTEMBER 25, 2024

REMARKS AT THE INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK  
(ICPEN) CONFERENCE 2024

\* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

Good morning. I am honored to meet and speak with you all, representatives of the approximately 80 countries and seven observer organizations that comprise the ICPEN. I am grateful for the work you do to protect consumers both within your own countries and to promote cross-border information sharing and enforcement cooperation. As Chair Khan has noted, the FTC is honored to serve as the ICPEN president. This week is a wonderful opportunity for us to learn from each other as we advance our individual and collective missions.

One of the topics for this week's discussion is online gaming, a topic near and dear to several of my teenage children. I am a mother of four. Like most parents, I am trying to teach my children how to use the Internet responsibly—how to seek information without being misled by manipulative web design. How to engage in discourse without targeting or becoming a target. And how to find the good, the interesting, the entertaining, and the instructive, without stumbling upon, or being lured into, what is instead harmful. Parental engagement and oversight are the first—and perhaps the best—defense against misuse of the Internet.

As consumer protection enforcers, we play a critical role in protecting kids online from deception, fraud, and other harms the law prohibits. The Commission has two primary tools for protecting children online: Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices,<sup>1</sup> and the Children's Online Privacy Protection Act (COPPA),<sup>2</sup> as implemented by the COPPA Rule,<sup>3</sup> which imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13. Many stakeholders have concerns that these tools are not enough to protect kids, tweens, or teens online. Indeed, legislatures around the world, including the U.S. Congress, are having important conversations about whether and how existing law should change to further protect our children.<sup>4</sup>

While those conversations happen, however, we can and should protect the youngest among us with existing tools. Today, I'd like to highlight three of those ways: *First*, ensuring that parental controls deliver as promised. *Second*, promoting greater understanding of whether AI can be used to determine age with greater accuracy relative to legacy technologies, in ways that may help protect children and involve parents. And, *third*, requiring, where appropriate, child-protective default settings to forestall unfair or deceptive practices. I highlight these three ways to protect children not because they are an exhaustive list, but because they are not. Instead, I hope to contribute some answers to the critical question we must explore this week and beyond, which is: What are the concrete ways that we, as enforcers of existing law, can better protect children online?

Let's begin with parental controls. Parental controls are ubiquitous—available on the operating systems for smart phones, tablets, smart watches, televisions, gaming consoles, etc. and

---

<sup>1</sup> 15 U.S.C. § 45.

<sup>2</sup> 15 U.S.C. § 6501 *et seq.*

<sup>3</sup> 16 C.F.R. Part 312. The Commission is currently reviewing the COPPA Rule.

<sup>4</sup> *See, e.g.*, U.S. Sen. Comm. on Commerce, Science, & Transp., Press Release, *Senate Overwhelmingly Passes Children's Online Privacy Legislation* (July 30, 2024), <https://www.commerce.senate.gov/2024/7/senate-overwhelmingly-passes-children-s-online-privacy-legislation>.

in individual apps, games, and online services. They offer parents a vision of control and safety. But do screen limits, content-filtering mechanisms, and other parental controls work as promised? Do parental controls work as effectively as they should to protect children from over-exposure to screens and harmful content, such as self-harm challenges and pornography? Are parental controls designed to anticipate children and teens' likely attempts to circumvent their limits? And are parental controls updated with sufficient frequency to fix the inevitable bugs that could compromise their efficacy?<sup>5</sup>

These are important questions that we, as enforcers, should be asking both the research community and—where our legal authorities permit—the manufacturers and distributors of software with parental controls. And we should be examining consumer complaints, including through the FTC's own complaint aggregation system, the Consumer Sentinel Network, to understand how these issues are affecting parents and children.

A second means of protecting children online turns on more accurately gauging age. The FTC's COPPA Rule requires operators of online services directed to children under 13 to obtain "verifiable parental consent"—or VPC—prior to the collection, use, and disclosure of personal information from children.<sup>6</sup> VPC methods seek to determine whether the person giving consent is in fact the child's parent, by, for example, requiring the person providing consent to engage in a credit card transaction that provides notice to the account holder.<sup>7</sup> Operators of online services that are directed to children but that do not target children as their primary audience (called "mixed audience" services) may use an age screen so that they can treat their children and non-children users differently.<sup>8</sup> Every method for assessing age has its flaws. For example, children can be adept at circumventing age screening measures like age gates.

AI may be able to help in better determining age. AI is properly the topic of much discussion this week, as AI, like any existing or emerging technology, can be used for good or for ill. The FTC is a bulwark against harmful uses, as demonstrated by the Commission's announcement today of "Operation AI Comply," a law enforcement sweep aimed at stopping unfair and deceptive uses of AI.<sup>9</sup>

---

<sup>5</sup> Cf. Joanna Stern, *How Broken Are Apple's Parental Controls? It Took 3 Years to Fix an X-Rated Loophole*, WALL ST. J. (June 5, 2024), <https://www.wsj.com/tech/personal-tech/a-bug-allowed-kids-to-visit-x-rated-sites-apple-took-three-years-to-fix-it-17e5f65d>.

<sup>6</sup> 16 C.F.R. § 312.3(b).

<sup>7</sup> *Id.* § 312.5(b)(1) (requiring a method of verifiable parental consent that is "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent"); Fed. Trade Comm'n, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4> (last visited Sept. 18, 2024).

<sup>8</sup> For users who indicate that they are children, the service must either refrain from collecting personal information or obtain VPC.

<sup>9</sup> Fed. Trade Comm'n, Press Release, FTC Announces Crackdown on Deceptive AI Claims and Schemes (Sept. 25, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>.

While law enforcers should not hesitate to stop the harmful uses of AI, we should also consider how we can promote its beneficial uses.<sup>10</sup> For example, could AI-enabled facial age estimation technology be used to establish that an individual is an adult who can provide parental consent or to prevent children from accessing prohibited sites? Some critics of such technology have raised concerns about harmful downstream or ancillary use of images collected for these purposes or stifling of speech on age-assured sites.<sup>11</sup> Certainly, like every new technology, there may be concerns associated with AI, such as if it is used in a manner inconsistent with consumers' reasonable expectations. At the same time, we must balance potential risk with the potential benefit of more effectively protecting children from harmful content online.<sup>12</sup>

The last means of protecting children online I'd like to raise are child-protective default settings. Our enforcement action against Epic Games, the maker of the video game Fortnite, is a great example. The Commission's complaint alleged that Epic enabled real-time voice and text chat communications for children and teens by default, while matching children and teens with strangers to play Fortnite. Children and teens who played Fortnite were allegedly bullied, threatened, harassed, and exposed to dangerous and psychologically traumatizing issues such as suicide. According to the complaint, Epic employees urged the company to change the default settings to require users to opt in for voice chat, but the company's leadership resisted. The FTC's order required Epic to adopt strong privacy default settings for children and teens, ensuring that voice and text communications are turned off by default.<sup>13</sup>

As enforcers, our role is to take a careful look at the online services children are using to understand whether the default settings are set to protect their most vulnerable users in a manner that prevents unfair or deceptive practices.<sup>14</sup> We should also engage with the research community

---

<sup>10</sup> Cf. Concurring Statement of Comm'r Melissa Holyoak, Joined by Chair Lina M. Khan, *In re DoNotPay, Inc.*, FTC Matter No. 2323042 (Sept. 25, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/Holyoak-Khan-Statement-re-DoNotPay-09-25-2024.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Holyoak-Khan-Statement-re-DoNotPay-09-25-2024.pdf) ("Today's settlement [with an AI lawyer service] shows the Commission's important role in eliminating deception from the market so that honest firms can compete to offer consumers innovative, trustworthy products."); Dissenting Statement of Comm'r Melissa Holyoak, Joined by Comm'r Andrew N. Ferguson, *In re Rytr, LLC*; Matter No. 2323052, at 5 (Sept. 25, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/holyoak-rytr-statement.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-rytr-statement.pdf) ("We must protect consumers through robust enforcement. Indeed, the Commission is at its best when it does so. But we must also think carefully about the potential harms to consumers and innovation that attend misguided enforcement.").

<sup>11</sup> See, e.g., *Free Speech Coalition, Inc. v. Paxton*, 95 F.4th 263 (5th Cir. 2024), cert. granted, 144 S. Ct. 2174 (2024) (challenging a lower court judgment allowing Texas to enforce a state statute's age verification requirements on commercial websites that contain sexual content).

<sup>12</sup> Protecting *children* from clearly harmful online content, such as self-harm challenges and pornography, should not be a means of introducing broader restrictions on online speech directed to adults, as we are not (and should not be) arbiters of acceptable speech for adults. Cf. Concurring and Dissenting Statement of Comm'r Melissa Holyoak, *Social Media and Video Streaming Services Staff Report*; FTC Matter No. P205402 (Sept. 19, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/commissioner-holyoak-statement-social-media-6b.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/commissioner-holyoak-statement-social-media-6b.pdf).

<sup>13</sup> Fed. Trade Comm'n, Press Release, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges* (Dec. 19, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/12/fornite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>.

<sup>14</sup> Fed. Trade Comm'n, Press Release, *FTC Order Will Ban NGL Labs and its Founders from Offering Anonymous Messaging Apps to Kids Under 18 and Halt Deceptive Claims Around AI Content Moderation* (July, 9, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-order-will-ban-n-gl-labs-its-founders-offering-anonymous-messaging-apps-kids-under-18-halt>.

and other stakeholders to promote innovative controls that will provide greater protections for children.

I have mentioned just three mechanisms to protect children online, but, as enforcers, I strongly believe that we should be looking at every possible avenue to use existing law to accomplish this important goal, while also offering our expertise to legislatures that can effect more systemic change. Sometimes, a blunt fix may be warranted—for example, knocking out of the market companies that are offering purely harmful products. That’s why I supported the Commission’s action against the makers of the NGL app, which allegedly lured children and teens into paying for their service with fake, bullying messages like “i know what you did” and “are you straight?”.<sup>15</sup> Oftentimes, however, it will be a finer point.

I will close by adding an exhortation—a call to arms—to my original question. As this group of global consumer protection enforcers convenes this week, and after our week together concludes, let us continue to ask ourselves and each other: How can we work together, using our current legal authorities, to protect children online?

---

<sup>15</sup> Concurring Statement of Commissioner Melissa Holyoak, *In re NGL Labs, LLC*, FTC Matter No. 2223144 (July 9, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/2024.7.8-holyoak-statement-re-ngl.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2024.7.8-holyoak-statement-re-ngl.pdf).