No. 23-2969

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NETCHOICE, LLC, d/b/a NetChoice,
Plaintiff-Appellee,

v.

ROB BONTA, in his official capacity as
Attorney General of the State of California,
Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California,
No. 5:22-cv-08861 (Hon. Beth Labson Freeman)

BRIEF FOR AMICUS CURIAE FEDERAL TRADE COMMISSIONER ALVARO M. BEDOYA IN SUPPORT OF DEFENDANT-APPELLANT

ALVARO M. BEDOYA
Commissioner

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

abedoya@ftc.gov
(202) 326-2630

TABLE OF CONTENTS

Introduction And Interest Of Federal Trade Commissioner Bedoya 1

Background 4

I. The California Age-Appropriate Design Code Act (CAADCA) 4

II. This Case 6

III. COPPA's Relevance to This Case 7

Argument 10

I. COPPA's History Shows How Unauthorized and Unnecessary Data Collection, Use, Retention, and Sale Can Endanger Child Safety. 10

II. COPPA's History Shows How Unnecessary Data Collection, Use, Retention, and Sale Can Undermine Data Security for Children and Families. ..16

III. COPPA's History Shows How Unnecessary Data Collection, Use, Retention, and Sale Allow Companies to Create Commercial Relationships With Children That Exploit Their Trust and Vulnerability. 19

Conclusion 26

TABLE OF AUTHORITIES

Cases

Central Hudson Gas & Electric Corp. v. Public Service Commission of New York,
447 U.S. 557 (1980) 6

Jones v. Google, LLC,
73 F.4th 636 (9th Cir. 2023) 1

Metro Lights, L.L.C. v. City of Los Angeles,
551 F.3d 898 (9th Cir. 2009) 6

United States v. Amazon.com, Inc.,
No. 2:23-cv-00811 (W.D Wash. May 31, 2023) 18

United States v. Edmodo, LLC,
No. 3:23-cv-02495 (N.D. Cal. May 22, 2023) 24

United States v. Epic Games, Inc.
No. 5:22-cv-00518-BO (E.D.N.C. Dec. 12, 2022) 15

United States v. InMobi Pte Ltd.,
No. 3-15-cv-03474 (N.D. Cal. June 22, 2016) 25

United States v. Lai Systems, LLC,
No. 2:15-cv-09691 (C.D. Cal. Dec. 17, 2015) 23

United States v. Musical.ly,
No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019 14

United States v. Path, Inc.,
No 3:13-cv-00448-RS (N.D. Cal. Feb. 8, 2013) 13

United States v. Prime Sites,
No. 2:18-cv-00199 (D. Nev. Feb. 5, 2018) 13

United States v. Retro Dreamer,
No. 5:15-cv-02569 (C.D. Cal. Dec. 17, 2015) 24

United States v. TinyCo, Inc.,
No. 3:14-cv-04164 (N.D. Cal. Sept. 16, 2014).....22

United States v. Unixiz, Inc.,
No. 5:19-cv-02222 (N.D. Cal. Apr. 24, 2019).....18

United States v. Vtech Electronics Ltd.,
No. 1:18-cv-00114 (N.D. Ill. Jan 8, 2018).....18

Statutes, Rules, & Regulations

144 Cong. Rec. S8482..... 1, 8, 12, 20

15 U.S.C. § 6501 .....1, 3

15 U.S.C. § 6502 ..... 1, 8, 17

15 U.S.C. § 6504 1

16 C.F.R. § 312 ..... 9, 12, 17

64 Fed. Reg. 22750 (Apr. 27, 1999) 9

64 Fed. Reg. 59888 (Nov. 3, 1999).....9

64 Fed. Reg. 59899 (Nov. 3, 1999).....12

76 Fed. Reg. 59804, 59813 (Sept. 27, 2011) 12

78 Fed. Reg. 3972 (Jan. 17, 2013) 9

Assem. Bill 2273, 2021-2022 Reg. Sess. (Cal. 2022) 4

Cal. Civ. Code § 1798.99.30.....3

Cal. Civ. Code § 1798.99.31.....3, 6

Other Authorities

144 Cong. Rec. S8483 (July 17, 1998) 17

Alvaro Bedoya, Commissioner, Fed. Trade. Comm'n, Prepared Remarks at the National Academies of Sciences, Engineering & Medicine Meeting of the Committee on the Impact of Social Media on the Health and Wellbeing of Children & Adolescents (Feb. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/national-academies-speech-bedoya.pdf.....26

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 ...14

Dr. Jenny Radesky, Remarks at The Future of the COPPA Rule: An FTC Workshop (Oct. 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf 26

Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998)..... passim

Letter from Jodi Bernstein, Fed. Trade Comm'n, Dir. of Consumer Prot., to Kathryn C. Montgomery, President, Center of Media Educ. (July 15, 1997) 11

Not Ready for Take-Off: Face Scans at Airport Departure Gates (Georgetown Law Center on Privacy & Technology, Dec. 21, 2017) 3

Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act (May 19, 2022).....24

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) 18, 19

The Perpetual Line-Up: Unregulated Police Face Recognition in America (Georgetown Law Center on Privacy & Technology, Oct. 18, 2016).....3

What Facial Recognition Technology Means for Privacy and Civil Liberties, Hearing before Senate Subcomm. on Priv., Tech. and the Law of the Senate Judiciary Comm., 112th Cong., 2d Sess. (2012) 2

INTRODUCTION AND INTEREST OF FEDERAL TRADE COMMISSIONER BEDOYA

For 25 years, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, *et. seq.*, has protected children twelve and under by prohibiting the unauthorized or unnecessary collection, use, retention, or sharing of their data. COPPA was passed in 1998 in response to a Federal Trade Commission ("FTC") study that found that a majority of websites directed at children collected their personal information without obtaining permission from their parents. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* at 31-37 (June 1998) (hereinafter "1998 FTC Report"); 144 Cong. Rec. S8482 (July 17, 1998) (statement of Sen. Bryan) (citing FTC study).

The FTC is the primary enforcer of COPPA and wrote its implementing rule.[1] Notably, as this Court recently held in *Jones v. Google, LLC*, 73 F.4th 636, 643-44 (9th Cir. 2023), COPPA allows the states to write and enforce their own kids' privacy laws—separate and apart from COPPA—so long as those laws are not "inconsistent" with it. *See* 15 U.S.C. § 6502(d). Indeed, this case involves the State of California's own efforts to enact a privacy law to protect minors in California.

[1] States can also enforce COPPA after providing notice to the FTC. *See* 15 U.S.C. § 6504.

The Federal Trade Commission is an independent agency of the United States Government that protects consumer interests by, among other things, enforcing consumer protection laws and conducting studies of industry-wide consumer protection issues. As one of the three Senate-confirmed appointees who currently lead the FTC, I have a keen interest in promoting children's privacy. I also want to make sure that courts give full weight to the many ways in which privacy invasions hurt children.[2]

Prior to serving as a Federal Trade Commissioner, I spent over a dozen years working to identify, investigate, and prevent privacy violations, with a particular focus on biometric technology and surveillance affecting vulnerable individuals and communities. I did this initially as the first chief counsel of the U.S. Senate Subcommittee on Privacy, Technology, and the Law upon its founding in 2011, and subsequently as a law professor at the Georgetown University Law Center, where I founded and led the Center on Privacy & Technology at Georgetown Law from 2014 to 2022. *See generally What Facial Recognition Technology Means for Privacy and Civil Liberties*, Hearing before Senate Subcomm. on Priv., Tech. and the Law of the Senate Judiciary Comm., 112th Cong., 2d Sess. (2012); Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-Up: Unregulated*

[2] I understand that, under the Federal Rules of Appellate Procedure, I may file a brief as *amicus curiae* without the consent of parties or leave of court. *See* Fed. R. App. P. 29. Nonetheless, I have informed the parties that I am filing this brief.

Police Face Recognition in America (Georgetown Law Center on Privacy & Technology, Oct. 18, 2016) (discussing bias against women and African-Americans); Harrison Rudolph, Laura Moy, & Alvaro Bedoya, Not Ready for Take-Off: Face Scans at Airport Departure Gates (Georgetown Law Center on Privacy & Technology, Dec. 21, 2017) (same).

The district court below preliminarily enjoined enforcement of the California Age-Appropriate Design Code Act ("the CAADCA" or "the Act"), Cal. Civ. Code § 1798.99.28, *et seq.*,[3] on First Amendment grounds. *See* 1-ER-46 at 1-2. In analyzing three provisions of the CAADCA protecting against the unnecessary collection, use, retention, and sale of minors' data, *id.* at 30-33 (discussing CAADCA §§ 31 (b)(3), (b)(4), (b)(7)), the district court did not adequately consider the full range of harms to children that are created by those practices.[4] The 25-year record of COPPA's passage, implementation, and enforcement illustrates a broad consensus across government, civil society, and industry that the

[3] Like the district court, when subsequently citing to the Act, this brief will cite to the statute's abbreviated title and last two digits. So, the brief will cite to Cal. Civil Code § 1798.99.29 as "CAADCA § 29."

[4] In this brief, "children," "child" or "kids" will refer to those under 13, the population protected under COPPA. *See* 15 U.S.C. § 6501(1). "Minors" refers to those under 18, the population protected under the CAADCA—although the CAADCA defines those individuals as "children." *See* Cal. Civ. Code § 1798.99.30(b)(1). To clarify this difference, when quoting the CAADCA, this brief will substitute the bracketed words "[minor]" or "[minors]" for any appearance of the words "child" or "children."

unauthorized or unnecessary collection, use, retention, and sale 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.

By limiting its discussion of harms to (1) profiling that leads to minors being shown harmful content, (2) deceptive design techniques used to keep minors online for longer periods of time (also known as "dark patterns"), and (3) financial losses to minors, the district court only considered a fraction of the ways in which the privacy violations that would be prevented by the CAADCA actually hurt kids 12 and under. This brief seeks to ensure that this Court benefits from a more complete record, drawn from the FTC's experience with COPPA, of how privacy invasions hurt children.

BACKGROUND

I. The California Age-Appropriate Design Code Act (CAADCA)

In passing the CAADCA in 2022, California lawmakers sought to "create a safer online space for [minors] to learn, explore, and play." Assem. Bill 2273 § 1(a)(3), 2021-2022 Reg. Sess. (Cal. 2022). The California legislature recognized that greater privacy protections would help achieve that goal, observing that "greater privacy necessarily means greater security and well-being." *Id.* § 1(a)(4).

To these ends, the CAADCA enacts a series of mandates and prohibitions, including a requirement that certain online businesses conduct internal privacy audits, and various prohibitions against the unnecessary collection, use, retention, and sale of the data of minors younger than 18. *See* CAADCA §§ 31(a), (b). This brief will focus on three of those prohibitions challenged by the plaintiffs:

> (b) A business that provides an online service, product, or feature likely to be accessed by [minors] shall not take any of the following actions: […]
>
> (3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a [minor] is actively and knowingly engaged, […] unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of [minors] likely to access the online service, product, or feature.
>
> (4) If the end user is a [minor], use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of [minors]. […]
>
> (7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature[,] to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.

CAADCA §§ 31(b)(3), (b)(4), (b)(7). Taken together, these three provisions generally prevent the unnecessary collection, retention, disclosure, or sale of minors' personal information, the use of that data for a secondary purpose separate

from the purpose for which it was collected, or the use of design techniques to trick minors into allowing any of these practices, or any practice that might otherwise harm them.

II. This Case

In the decision below, the district court applied an intermediate standard of review for commercial speech to analyze the challenged provisions. 1-ER-46 at 18. Analyzing each provision, the Court focused on the "means-ends" fit: "whether the 'restriction… directly advance[s] the state interest involved' and whether it is not 'more extensive than is necessary to serve that interest.'" 1-ER-46 at 19 (citing *Metro Lights, L.L.C. v. City of Los Angeles*, 551 F.3d 898, 903 (9th Cir. 2009); quoting *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564–66) (1980)).

In analyzing the provisions cited above, the district court focused *solely* on three examples of harms: (1) profiling leading to minors being shown harmful content, (2) deceptive design techniques used to keep minors online for longer periods of time, and (3) financial losses to minors. The district court found none of these harms to be sufficient to justify the breadth of the challenged provisions. *See* 1-ER-46 at 31 (finding that CAADCA § 31 (b)(3) is an overbroad remedy to the problem of harmful content); *id.* (same with regard to CAADCA § 31(b)(4)); *id.* at 32-33 (same for CAADCA § 31(b)(7)); *id.* at 33 (use of dark patterns to collect

information used to extend engagement on a platform "is not causally connected to an identified harm" that can justify CAADCA § 31(b)(7)); *id.* (use of dark patterns to manipulate users into making purchases cannot justify CAADCA § 31(b)(7), as defendant did not assert that CAADCA was "an attempt to address monetary harms to [minors]").

Critically, the district court did not consider any other harms that could justify these protections. This is a significant mistake that overlooks numerous other ways in which the conduct targeted by the CAADCA harms children.

III. COPPA's Relevance to This Case

In effect, the district court's decision asks: How does unnecessary data collection, use, retention, and disclosure hurt kids? The 25-year-old history of COPPA's passage, implementation, and enforcement provides an unparalleled insight into how Congress, law enforcement, civil society, and industry have answered that question.

As discussed above, 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. *See* 1998 FTC Report at 31–42. 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. *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) at 3 (hereinafter "Senate COPPA Hearing") (Statement of Sen. Burns) (COPPA "drew heavily" from the FTC report).

COPPA charged the FTC with issuing a rule to protect children's privacy and safety online. 15 U.S.C. § 6502(b). That rule, as it currently stands, contains four prohibitions for operators of websites directed at children that protect against the unauthorized and unnecessary collection, use, retention, and disclosure of children's data:

> An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented. […]
>
> An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties. […]

> An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.
>
> An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. […]

Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. §§ 312.5(a)(1), 312.5(a)(2), 312.7, and 312.10. The first of those two provisions use a verifiable parental consent requirement, while the latter two provisions rely on an assessment of reasonable necessity, that is, of whether and for how long a child's personal information is needed for the underlying service requesting that data.

COPPA's implementing rules were not written at random. Rather, they reflect the culmination of a years-long process during which (1) Congress debated the harms stemming from the collection, use, and disclosure of children's data, and crafted a statute to protect against those harms; (2) the FTC conducted a public notice and comment rulemaking where it drafted a rule based on feedback from law enforcement, civil society, and industry; and (3) FTC experts refined those rules in light of advances in technology and another round of public comments. *See generally* Senate COPPA Hearing; 64 Fed. Reg. 22750 (Apr. 27, 1999) (Notice of Proposed Rulemaking); 64 Fed. Reg. 59888 (Nov. 3, 1999) (Notice of Final Rule addressing public comments); 78 Fed. Reg. 3972 (Jan. 17, 2013) (Notice of Final

Rule updating the COPPA Rule in light of technological advances and public feedback).

Indeed, a review of that record reveals a broad consensus that the unauthorized and unnecessary collection, use, retention, and sale of children's data hurts children and their families by (1) endangering children's safety, (2) exposing kids and their families to hacks and data breaches, and (3) allowing third-party companies to develop commercial relationships with children that prey on their trust and vulnerability. Because the district court did not consider these harms, the remainder of this brief will explain them and will urge this Court to weigh these harms in its own analysis of the constitutionality of CAADCA §§ 31(b)(3), (b)(4), and (b)(7).

ARGUMENT

I. COPPA's History Shows How Unauthorized and Unnecessary Data Collection, Use, Retention, and Sale Can Endanger Child Safety.

It is particularly surprising that the district court did not consider how the unauthorized and unnecessary collection, use, retention, and sale of children's information—practices that would be curbed by CAADCA §§ 31(b)(3), (b)(4), and (b)(7)—could endanger the safety of those children. Indeed, the threat of privacy invasions to child safety was front of mind for the legislators who enacted COPPA and the FTC researchers who wrote the 1998 report to which COPPA responded.

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." *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. *See* 1998 FTC Report at 31–34, 39–40. 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." *See* 144 Cong. Rec. S8482 (July 17, 1998) (statement of Sen. Bryan) (emphasis added). 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. *See, e.g.*, *id.* (advances in technology "leav[e] [children] unwittingly vulnerable to exploitation and harm by … criminals").

Safety was also a focus for the Federal Trade Commission when it initially promulgated the 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." *See* 64 Fed. Reg. 59899 (Nov. 3, 1999). Similar reasoning can be found in the Commission's 2011 proposal to add geolocation information to the list of personal information protected by COPPA. *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.").

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. *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).
- 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. *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).
- 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 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. *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").

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. *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).

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. *Id* at 20–21. 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." *Id.* at 18. The allegations in Fortnite exemplify the kinds of harms these design techniques can impose on children and their families.

In the decision below, the district court concluded that "the State has not shown that dark patterns causing children to forego privacy protections constitutes a real harm." 1-ER-46 at 33. That analysis overlooks ample evidence that these design techniques—and other strategies that maximize the unauthorized and

unnecessary collection, use, retention, or disclosure of children's information—can clearly endanger children, as the Fortnite allegations illustrate.[5]

II. COPPA's History Shows How Unnecessary Data Collection, Use, Retention, and Sale Can Undermine Data Security for Children and Families.

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

---

[5] The plaintiffs did not challenge the constitutionality of CAADCA §§ 31(b)(5) and (6), which address the collection, sale, or disclosure of precise geolocation information, 1-ER-46 at 20, and the district court *did* find the defendant was "likely to establish a real harm" from the failure of online services to provide high default privacy settings, *id.* at 24. Thus, defendants could conceivably argue that some of the above cases are not relevant to the instant appeal. The same cannot be said of the *Epic Games* case, which involved the use of deceptive design to obscure a new privacy option to remedy an already-low default setting.

1998 FTC Report, *supra*, at 39. 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. *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."). 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. *See* 15 U.S.C. § 6502(b)(1)(D); 16 C.F.R. §§ 312.8, 312.10.

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." *See* Complaint, *United States v. Vtech Electronics Ltd.* at 3-9, No. 1:18-cv-00114 (N.D. Ill. Jan 8, 2018); *see also* Complaint for Civil Penalties, Permanent Injunction, and other Equitable Relief at 9, *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).

The Court should also be aware that, in an era where 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 recently 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. *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).

Based on over a decade of policy work and research in biometrics, I believe 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.

III. COPPA's History Shows How Unnecessary Data Collection, Use, Retention, and Sale Allow Companies to Create Commercial Relationships With Children That Exploit Their Trust and Vulnerability.

A substantial portion of data collection, use, retention, and sale practices are intended to serve the data requirements of online advertising. Yet the district court only considered one of the harms created by these practices. What's more, it entirely ignored a core harm that drove COPPA's passage, implementation, and enforcement: companies' use of children's data to create commercial relationships with them that take advantage of their trust and vulnerability.

The district court considered the possibility that data collected from minors could allow them to be targeted with harmful behavioral advertising and other content, such as "extreme weight loss content and gambling and sports betting ads." *See* 1-ER-46 at 30–31. The district court did not dispute the harms that may flow from this content but rejected them as insufficient to justify the breadth of the

challenged CAADCA provisions. *Id.*at 30–34. The district court also rejected as irrelevant the possibility that the practices prohibited by the CAADCA could cause minors "monetary harm." *Id.* at 33.

Both of these harms are real and cognizable. What the district court's analysis entirely ignores, however, is a core concern at the heart of COPPA related to online marketing. When Senator Bryan introduced COPPA, he was concerned about companies using 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.

See 144 Cong. Rec. S8482-3. 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." *See* 1998 FTC Report at 5-6.

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." *See* Senate COPPA Hearing at 3.

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." *See* Senate COPPA Hearing at 34 (statement of Dr. Montgomery). 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." *Id.* at 34-35.

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

> [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.

Id. at 35.

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 the otherwise invisible collection and sale of their 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. *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).

- 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. *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).
- 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 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. *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).

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 technology ("ed tech") tools 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 advertising networks to collect personal information from those children, including persistent identifiers, to serve them with ads. *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 take action against companies that illegally surveilled children using ed tech tools).

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. *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).

In the most recent workshop to consider the future of the COPPA Rule, Dr. Jenny Radesky, a pediatrician who offered her expert testimony on behalf of the defendant in the district court proceedings—and 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." *See* Dr. Jenny Radesky, Remarks at The Future of the COPPA Rule: An

FTC Workshop (Oct. 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf (Transcript of COPPA Workshop, Part 1).

CONCLUSION

The Internet can be a lifeline to young people, particularly those who live in remote areas or who struggle to find acceptance and community in their immediate family and surroundings. Any effort to regulate the Internet must not cut off that lifeline. *See* Alvaro Bedoya, Commissioner, Fed. Trade. Comm'n, Prepared Remarks at the National Academies of Sciences, Engineering & Medicine Meeting of the Committee on the Impact of Social Media on the Health and Wellbeing of Children & Adolescents 5 (Feb. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/national-academies-speech-bedoya.pdf (discussing the particular importance of social media for transgender teens).

Based on the congressional record and the FTC's decades-long experience protecting the privacy of pre-teens, the district court engaged in too narrow of an analysis of how the data practices prohibited by the CAADCA can hurt children 12 and under. This Court should consider how the CAADCA protects children from that full range of harms.

December 20, 2023

Respectfully submitted,
/s/ Alvaro Bedoya

ALVARO M. BEDOYA
Commissioner
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
WASHINGTON, D.C. 20580
abedoya@ftc.gov
(202) 326-2630

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 23-2969

I am the attorney or self-represented party.

This brief contains 6,040 **words,** including _____ words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Alvaro Bedoya **Date** 12/20/2023

(use "s/[typed name]" to sign electronically-filed documents)

CERTIFICATE OF SERVICE

I certify that on December 20, 2023, I served the foregoing Brief as *Amici Curiae* in Support of Defendant-Appellant via the Court's ECF system upon all counsel.

Dated: December 20, 2023

/s/ Alvaro Bedoya

Alvaro M. Bedoya
Commissioner
Federal Trade Commission