

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

NETCHOICE, LLC, d/b/a NetChoice

Plaintiff,

v.

ROB BONTA, Attorney General of the State
of California, in his official capacity,

Defendant.

Case No. 22-cv-08861-BLF

**ORDER GRANTING MOTION FOR
PRELIMINARY INJUNCTION**

[Re: ECF 29]

This suit challenges the enforceability of the California Age-Appropriate Design Code Act (“the CAADCA” or “the Act”), which was recently enacted for the stated purpose of affording protections to children when they access the internet. *See* Cal. Civ. Code § 1798.99.29.¹ The Act applies to for-profit businesses that collect consumers’ personal information and satisfy other criteria relating to business size and revenue. *See* CAADCA § 30; Cal. Civ. Code § 1798.140. Effective July 1, 2024, the Act imposes a number of requirements on any covered business that “provides an online service, product, or feature likely to be accessed by children.” CAADCA § 31.

Plaintiff NetChoice, LLC (“NetChoice”) “is a national trade association of online businesses that share the goal of promoting free speech and free enterprise on the Internet.” Compl. ¶ 5, ECF 1. NetChoice’s members include Google, Amazon, Meta, TikTok and many other companies with strong online presences. NetChoice sues Defendant Rob Bonta, Attorney

¹ The CAADCA is codified at California Civil Code §§ 1798.99.28–1798.99.40. When citing to the Act, the Court will cite to the statute’s abbreviated title and last two digits. For example, the Court will cite to Cal. Civil Code § 1798.99.31 as “CAADCA § 31.”

1 General of the State of California (“the State”), for declaratory and injunctive relief related to the
2 CAADCA, which it asserts is both facially unconstitutional and preempted by federal statute.

3 NetChoice moves for preliminary injunction based on its claims that the CAADCA
4 violates the First Amendment and the dormant Commerce Clause of the United States
5 Constitution, and is preempted by both the Children’s Online Privacy Protection Act (“COPPA”),
6 15 U.S.C. §§ 6501–6506, and Section 230 of the Communications Decency Act, 47 U.S.C. § 230.
7 *See Mot.*, ECF 29. The State opposes the motion, arguing that the CAADCA regulates conduct—
8 the collection and use of children’s personal information—that does not implicate the First
9 Amendment. *See Opp’n*, ECF 51. The State also contends that the CAADCA does not violate the
10 dormant Commerce Clause and is not preempted by either COPPA or Section 230. *See id.*

11 Mindful that the CAADCA was enacted with the unanimous support of California’s
12 Legislature and Governor, the Court has given careful consideration to the motion, the State’s
13 opposition, NetChoice’s reply, the supplemental briefs filed by both parties, the briefs filed by
14 seven sets of amici curiae, and the oral arguments presented at the hearing on July 27, 2023. The
15 Court finds that although the stated purpose of the Act—protecting children when they are
16 online—clearly is important, NetChoice has shown that it is likely to succeed on the merits of its
17 argument that the provisions of the CAADCA intended to achieve that purpose do not pass
18 constitutional muster. Specifically, the Court finds that the CAADCA likely violates the First
19 Amendment. The motion for preliminary injunction is GRANTED on that basis.

20 **I. BACKGROUND**

21 The internet has become indispensable to the exchange of information. Many online
22 providers allow users to view content and access services without creating an account, while
23 others require the creation of a free account to access services, and still others require users to pay
24 fees. *See Cairella Decl.* ¶¶ 4–8, ECF 22; *Masnack Decl.* ¶¶ 5–6, ECF 29; *Roin Decl.* ¶¶ 7–9, ECF
25 25; *Paolucci Decl.* ¶ 2, ECF 28. Online providers generally rely on advertising to earn revenue
26 that supports the content and services they offer. *See Cairella Decl.* ¶¶ 4, 21; *Roin Decl.* ¶ 10.
27 Advertisements are targeted to users based on their interests, which are gleaned from data
28 collected from the users while they are online. *See Egelman Decl.* ¶¶ 13–14, ECF 51-1. Such data

1 also is used by online providers to tailor content to individual users. *See* Cairella Decl. ¶ 8; Roin
2 Decl. ¶¶ 2–6. In addition, online providers may sell user data to third parties. *See* Egelman Decl.
3 ¶ 11.

4 Users can manage their online privacy by reading privacy policies before engaging with
5 the provider’s services. *See* Egelman Decl. ¶ 24. Users also may change their privacy settings to
6 block or delete “cookies,” which are data that websites store in consumers’ web browsers, which
7 are then transmitted back to websites when visited again. *See id.* ¶ 29. However, privacy policies
8 can be difficult to understand and privacy settings are not always user friendly. *See id.* ¶¶ 24–30.

9 These privacy concerns have become increasingly relevant to children, because their
10 internet use has grown dramatically in recent years. *See* Radesky Decl. ¶¶ 21–25, ECF 51-5.
11 During the COVID-19 pandemic, children’s access to digital technology and time online went up
12 significantly. *See id.* ¶ 26. Children’s time online increased approximately 52% during the
13 pandemic, and heavier technology use habits have persisted. *See id.* Children depend on the
14 internet for both educational and entertainment purposes. *See id.* ¶¶ 26-29. Unplugging is not a
15 viable option. *See id.* ¶ 29.

16 A federal child privacy law, COPPA, limits the ability of online providers to collect
17 personal information from children. *See* 15 U.S.C.A. §§ 6501–06. COPPA makes it “unlawful
18 for an operator of a website or online service directed to children, or any operator that has actual
19 knowledge that it is collecting personal information from a child, to collect personal information
20 from a child in a manner that violates the regulations prescribed” under the statute. 15 U.S.C. §
21 6502(a)(1). “Child” is defined as an individual under the age of 13. 15 U.S.C. § 6501(1). The
22 applicable regulations require the operator to obtain parental consent prior to any collection, use,
23 or disclosure of personal information from children. *See* 16 C.F.R. § 312.3(b).

24 The California Consumer Privacy Act (“CCPA”) imposes limits on the collection of
25 personal information from users generally, requiring among other things that online providers
26 inform users of the categories of personal information to be collected and the purposes of such
27 collection. *See* Cal. Civ. Code § 1798.100(a)(1). The CCPA defines “personal information” to
28 include any information that “relates to, describes, is reasonably capable of being associated with,

1 or could reasonably be linked, directly or indirectly, with a particular consumer or household.”
2 Cal. Civ. Code § 1798.140(v).

3 It is against this backdrop that the CAADCA was enacted. The CAADCA goes far beyond
4 the scope of protections offered by COPPA and the CCPA. Whereas COPPA limits the collection
5 of user data by operators of websites and services “directed to children,” 15 U.S.C. § 6502(a)(1),
6 the CAADCA “declares that children should be afforded protections not only by online products
7 and services specifically directed at them but by all online products and services they are likely to
8 access,” CAADCA § 29. COPPA protects children under the age of 13, *see* 15 U.S.C. § 6501(1),
9 while the CAADCA protects children under the age of 18, *see* CAADCA § 30(b)(1). COPPA
10 gives parents authority to make decisions about use of their children’s personal information, *see*
11 16 C.F.R. § 312.3(b), and the CCPA gives users authority to make decisions about their own
12 personal information, *see* Cal. Civ. Code § 1798.135. In contrast, the CAADCA requires online
13 providers to create a Data Protection Impact Assessment (“DPIA”) report identifying, for each
14 offered online service, product, or feature likely to be accessed by children, any risk of material
15 detriment to children arising from the provider’s data management practices. *See* CAADCA §
16 30(a)(1). Providers must create a “timed plan to mitigate or eliminate” the risks identified in the
17 DPIA “before the online service, product, or feature is accessed by children,” *id.* § 30(a)(2), and
18 must provide the DPIA reports to the California Attorney General upon written request, *see id.* §
19 30(a)(2). The CAADCA also requires that online providers comply with a list of enumerated
20 mandates and prohibitions, discussed in detail below. *See id.* § 31(a)–(b).

21 Covered businesses must complete the required DPIA reports and satisfy related
22 requirements by July 1, 2024, and continue to do so on an ongoing basis. *See* CAADCA §§ 31,
23 33. The CAADCA authorizes the California Attorney General to bring a civil enforcement action
24 against any business that fails to comply with the Act’s requirements. *See id.* § 35. Violators are
25 subject to civil penalties of \$2,500 per child for each negligent violation and \$7,500 for each
26 intentional violation. *See id.*

27 NetChoice filed this suit on December 14, 2022, challenging the CAADCA as facially
28 unconstitutional and preempted by federal statute. The complaint asserts the following claims:

1 (1) violation of the First and Fourteenth Amendments to the U.S. Constitution, and Article I,
 2 Section 2(a) of the California Constitution; (2) violation of the Fourth Amendment to the U.S.
 3 Constitution; (3) void for vagueness under the First Amendment and Due Process Clause of the
 4 U.S. Constitution, and Article I, Section 7(a) of the California Constitution; (4) violation of the
 5 dormant Commerce Clause of the U.S. Constitution; (5) preemption by COPPA; and (6)
 6 preemption by Section 230. Compl. ¶¶ 76–122. The complaint requests declaratory and
 7 injunctive relief prohibiting enforcement of the CAADCA.

8 NetChoice now seeks a preliminary injunction enjoining enforcement of the CAADCA
 9 pending disposition of the suit.

10 **II. LEGAL STANDARD**

11 “Courts consider four factors in deciding whether to grant a preliminary injunction: the
 12 plaintiff’s likelihood of success on the merits; her likelihood of suffering irreparable harm in the
 13 absence of preliminary relief; whether the balance of equities tips in her favor; and whether an
 14 injunction is in the public interest.” *Garcia v. City of Los Angeles*, 11 F.4th 1113, 1118 (9th Cir.
 15 2021) (citing *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

16 In this circuit, “[l]ikelihood of success on the merits is the most important factor.”²
 17 *Apartment Ass’n of L.A. Cnty., Inc. v. City of Los Angeles*, 10 F.4th 905, 912 (9th Cir. 2021)
 18 (quoting *California v. Azar*, 911 F.3d 558, 575 (9th Cir. 2018)). “It is well-established that the
 19 first factor is especially important when a plaintiff alleges a constitutional violation and injury.”
 20 *Baird v. Bonta*, --- F.4th ---, 2023 WL 5763345, at *3 (9th Cir. Sept. 7, 2023). “If a plaintiff in
 21 such a case shows he is likely to prevail on the merits, that showing usually demonstrates he is
 22 suffering irreparable harm no matter how brief the violation.” *Id.* Finally, “[w]hen, like here, the
 23 nonmovant is the government, the last two *Winter* factors merge.” *Id.* at *2 (quotation marks and
 24 citation omitted).

25 _____
 26 ² Where the plaintiff cannot show a likelihood of success on the merits, “‘serious questions going
 27 to the merits’ and a hardship balance that tips sharply toward the plaintiff can support issuance of
 28 an injunction, assuming the other two elements of the *Winter* test are also met.” *All. for the Wild
 Rockies v. Cottrell*, 632 F.3d 1127, 1132 (9th Cir. 2011). The Court need not apply this alternative
 formulation of the *Winter* test here because, as discussed below, NetChoice makes a strong
 showing on likelihood of success and on the other *Winter* factors.

1 **III. DISCUSSION**

2 **A. Likelihood of Success on the Merits**

3 NetChoice argues that it is likely to succeed on the merits of its claims that the Act violates
4 free speech rights under the First Amendment (Claims 1 and 3), violates the dormant Commerce
5 Clause (Claim 4), and is preempted by both COPPA (Claim 5) and Section 230 (Claim 6). *See*
6 *Mot. 1; Compl. ¶¶ 76–122.*

7 **1. First Amendment (Claims 1 and 3)**

8 Claim 1 asserts that the CAADCA violates the First Amendment because it is an unlawful
9 prior restraint on protected speech, is unconstitutionally overbroad, and regulates protected
10 expression but fails strict scrutiny or any lesser standard of scrutiny that may apply. *See Compl.*
11 *¶¶ 76–88.* Claim 3 asserts that the CAADCA is void for vagueness under the First Amendment.
12 *See id. ¶¶ 93–103.* NetChoice argues that it is likely to succeed on its First Amendment claims
13 because the CAADCA: (1) is an unlawful prior restraint; (2) is unconstitutionally overbroad; (3)
14 is void for vagueness; and (4) is subject to and fails strict scrutiny. *Mot. 7–22.*

15 Before taking up these arguments, the Court notes that both parties appear to have accepted
16 the relaxed standard for standing in a First Amendment facial challenge. That is, although the
17 general rule of standing is that a party may not challenge a statute’s constitutionality “on the
18 ground that it may conceivably be applied unconstitutionally to others,” *Broadrick v. Oklahoma*,
19 413 U.S. 601, 610 (1973), a party making a First Amendment claim has standing to challenge the
20 impact of a regulation on both “its own expressive activities, as well as those of others,” *S.O.C.*
21 *Inc. v. County of Clark*, 152 F.3d 1136, 1142 (9th Cir. 1998). Accordingly, the parties have
22 made—and the Court will consider—arguments about the CAADCA’s alleged impact on the
23 expressive activities of individuals and entities who are not NetChoice members.

24 Turning to NetChoice’s four First Amendment arguments on likelihood of success, the
25 Court first addresses the argument that the Act regulates protected expression and fails the
26 applicable level of scrutiny. Because the argument is dispositive, the Court need not address
27 NetChoice’s additional First Amendment arguments based on prior restraint, overbreadth, and
28 vagueness.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28**a. Legal Framework re Scrutiny for Regulations of Speech**

“The First Amendment generally prevents government from proscribing speech, [] or even expressive conduct, [] because of disapproval of the ideas expressed.” *R.A.V. v. City of St. Paul*, 505 U.S. 377, 382 (1992) (internal citations omitted). A law compelling speech is no less subject to First Amendment scrutiny than a law prohibiting speech. *Frudden v. Pilling*, 742 F.3d 1199, 1203 (9th Cir. 2014) (citing *W. Va. State Bd. Of Educ. v. Barnette*, 319 U.S. 624, 633–34 (1943)).

The threshold question in a free speech analysis is whether the challenged law invokes the First Amendment at all. *See Int’l Franchise Ass’n v. City of Seattle*, 803 F.3d 389, 408 (9th Cir. 2015). “All manner of speech—from ‘pictures, films, paintings, drawings, and engravings,’ to ‘oral utterance and the printed word’—qualify for the First Amendment’s protections; no less can hold true when it comes to speech . . . conveyed over the Internet.” *303 Creative LLC v. Elenis*, 600 U.S. —, 143 S. Ct. 2298, 2312 (2023) (citations omitted). That is, the First Amendment’s protections apply not only to written or verbal speech, but to any expressive conduct. *See, e.g., Ward v. Rock Against Racism*, 491 U.S. 781, 790 (1989) (“Music, as a form of expression and communication, is protected under the First Amendment.”). In determining whether a law regulates protected expression, courts evaluate “whether [activity] with a ‘significant expressive element’ drew the legal remedy or the ordinance has the inevitable effect of ‘singling out those engaged in expressive activity.’” *Int’l Franchise*, 803 F.3d at 408 (quoting *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706–07 (1986)). For example, a tax on paper and ink that in effect “single[s] out the press for special treatment” regulates protected expression, although the application of a general sales tax to newspapers does not. *See Minneapolis Star & Tribune Co. v. Minn. Comm’r of Revenue*, 460 U.S. 575, 581–82 (1983). A regulation that restricts conduct without a “significant expressive element” is not subject to any level of First Amendment scrutiny. *See HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 684 (9th Cir. 2019); *see also Sorrell v. IMS Health Inc.*, 564 U.S. 552, 567 (2011) (“[T]he First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech.”).

If a court finds that a challenged law regulates some manner of protected expression, it must then “determine the scope of the [regulated] speech” in order to apply the appropriate level

1 of scrutiny. *Yim v. City of Seattle*, 63 F.4th 783, 791 (9th Cir. 2023). There are several levels of
2 scrutiny that may apply, depending on the type of expression at issue.

3 **i. Strict Scrutiny**

4 If the challenged regulation restricts only non-commercial speech, the level of scrutiny
5 depends on whether the law is content based or content neutral. “Government regulation of
6 speech is content based if a law applies to particular speech because of the topic discussed or the
7 idea or message expressed,” that is, if the regulation “draws distinctions based on the message a
8 speaker conveys.” *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015) (citations omitted). A law
9 is also content based if, even though facially neutral, it “cannot be justified without reference to
10 the content of the regulated speech, or . . . were adopted by the government because of
11 disagreement with the message the speech conveys.” *Id.* at 164 (internal punctuation marks and
12 citation omitted). If the court determines a law is content based, it applies strict scrutiny,
13 “regardless of the government’s benign motive, content-neutral justification, or lack of ‘animus
14 toward the ideas contained’ in the regulated speech.” *Porter v. Martinez*, 68 F.4th 429, 439 (9th
15 Cir. 2023) (citations omitted). Strict scrutiny “requires the Government to prove that the
16 restriction furthers a compelling interest and is narrowly tailored to achieve that interest.” *Reed*,
17 576 U.S. at 171; *see also Berger v. City of Seattle*, 569 F.3d 1029, 1050 (9th Cir. 2009) (“Under
18 that standard [of strict scrutiny], the regulation is valid only if it is the least restrictive means
19 available to further a compelling government.”) (citing *United States v. Playboy Ent. Grp., Inc.*,
20 529 U.S. 803, 813 (2000)).

21 **ii. Intermediate Scrutiny**

22 “By contrast, a content-neutral regulation of [non-commercial] expression must meet the
23 less exacting standard of intermediate scrutiny.” *Porter*, 68 F.4th at 439 (citation omitted). Under
24 this lower standard, “a regulation is constitutional ‘if it furthers an important or substantial
25 governmental interest; if the governmental interest is unrelated to the suppression of free
26 expression; and if the incidental restriction on alleged First Amendment freedoms is no greater
27 than is essential to the furtherance of that interest.’” *Id.* (quoting *United States v. O’Brien*, 394
28 U.S. 367, 377 (1968)).

1 **iii. Commercial Speech Scrutiny**

2 If a statute regulates only commercial speech—i.e., “expression related solely to the
3 economic interests of the speaker and its audience” that “does no more than propose a
4 commercial transaction,” *Am. Acad. of Pain Mgmt. v. Joseph*, 353 F.3d 1099, 1106 (9th Cir. 2004)
5 (citations omitted)—the court applies commercial speech scrutiny³ as established by *Central*
6 *Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980).
7 First, commercial speech is not entitled to any First Amendment protection if it is misleading or
8 related to illegal activity. *Cent. Hudson*, 447 U.S. at 563–64; *see also, e.g., Thompson v. W. States*
9 *Med. Ctr.*, 535 U.S. 357, 367 (2002). For all other commercial speech, the court asks “whether the
10 asserted governmental interest is substantial,” “whether the regulation directly advances the
11 governmental interest,” and “whether [the regulation] is not more extensive than is necessary to
12 serve that interest.” *Retail Digital Network, LLC v. Prieto*, 861 F.3d 839, 844 (9th Cir. 2017)
13 (quoting *Cent. Hudson*, 447 U.S. at 566). The regulation is constitutional only if the answer to all
14 three questions is “yes.” *See id.* This analysis applies to commercial speech regardless of
15 whether the regulation is content based or content neutral. *Yim*, 63 F.4th at 793 n.14 (citing *Valle*
16 *Del Sol, Inc. v. Whiting*, 709 F.3d 808, 820 (9th Cir. 2013)).

17 **iv. Scrutiny where Commercial and Non-Commercial**
18 **Speech is Inextricably Intertwined**

19 Finally, if a law regulates expression that “inextricably intertwines” commercial and non-
20 commercial components, the court does not “apply[] one test to one phrase and another test to
21 another phrase,” but instead treats the entire expression as non-commercial speech and applies the
22 appropriate level of scrutiny. *Riley v. Nat’l Fed’n of the Blind of N.C., Inc.*, 487 U.S. 781, 796
23 (1988) (applying strict scrutiny to content-based regulation of solicitation of charitable
24 contributions by professional fundraisers while assuming professional fundraiser’s financial
25 motivation for solicitation intertwined commercial interest with non-commercial advocacy).

26 With these principles in mind, the Court now assesses whether NetChoice has shown that it

27 _____
28 ³ The Court will use the phrase “commercial speech scrutiny” in this order to refer to the
“intermediate scrutiny standard codified in *Central Hudson*.” *Yim*, 63 F.4th at 793.

1 is likely to succeed both in establishing that the CAADCA regulates protected expression, and in
2 establishing that the CAADCA fails the applicable level of scrutiny.

3 **b. Protected Expression or Non-Expressive Conduct**

4 NetChoice argues that the CAADCA regulates speech by requiring internet content
5 providers to take various actions to protect minors from harmful messages, such as making
6 content-based assessments about potential harm to minors in order to comply with the DPIA
7 requirement, and necessarily reviewing content to adhere to the Act’s content policy enforcement
8 provision. *See* Mot. 19–21. The State argues that the Act merely regulates business practices
9 regarding the collection and use of children’s data, so that its restrictions are only of nonexpressive
10 conduct that is not entitled to First Amendment protection. *See* Opp’n 10–12. The State further
11 contends that the Act does not restrict speech because it does not prevent any particular content
12 from being shown to a minor—even if the content provider knows it would be harmful—as long
13 as the content provider does not use the minor’s personal information to do so. *See id.* at 12.

14 In evaluating whether the CAADCA regulates protected expression, the Court first notes
15 that determining whether the statute applies to a business will often require viewing the content of
16 the online service, product, or feature to evaluate whether it is “likely to be accessed by children”
17 because, for example, it contains “advertisements marketed to children.” CAADCA §§
18 29(b)(4)(C), 31(a). But having to view content to determine whether the statute applies does not
19 by itself mean that the statute regulates speech. *See, e.g., Am. Soc’y of Journalists & Authors, Inc.*
20 *v. Bonta*, 15 F.4th 954, 960–61 (9th Cir. 2021) (finding law classifying workers as employees or
21 independent contractors based on criteria including whether worker’s output was “to be
22 appreciated primarily or solely for its imaginative, aesthetic, or intellectual content” did not
23 regulate speech) (citing Cal. Labor Code § 2778(b)(2)(F)(ii)). The question is whether the law at
24 issue regulates expression “because of its message, its ideas, its subject matter, or its content.” *Id.*
25 at 960 (quoting *Reed*, 576 U.S. at 163). The Court will evaluate this question first with respect to
26 those portions of the statute that prohibit certain actions, *see* CAADCA § 31(b), and then turn to
27 the sections of the statute mandating specific acts, *see id.* § 31(a).

1 **i. The Act’s Prohibitions (CAADCA § 31(b))**

2 The CAADCA’s prohibitions forbid the for-profit entities covered by the Act from
 3 engaging—with some exceptions—in the collection, sale, sharing, or retention of children’s
 4 personal information, including precise geolocation information, for profiling or other purposes.
 5 *See generally id.* § 31(b). The State argues that the CAADCA’s regulation of “collection and use
 6 of children’s personal information” is akin to laws that courts have upheld as regulating economic
 7 activity, business practices, or other conduct without a significant expressive element. Opp’n 11–
 8 12 (citations omitted). There are two problems with the State’s argument. First, none of the
 9 decisions cited by the State for this proposition involved laws that, like the CAADCA, restricted
 10 the collection and sharing of information. *See id.*; *Rumsfeld v. Forum for Acad. & Inst. Rights,*
 11 *Inc.*, 547 U.S. 47, 66 (2006) (statute denying federal funding to educational institutions restricting
 12 military recruiting did not regulate “inherently expressive” conduct because expressive nature of
 13 act of preventing military recruitment necessitated explanatory speech); *Roulette v. City of Seattle,*
 14 97 F.3d 300, 305 (9th Cir. 1996) (ordinance prohibiting sitting or lying on sidewalk did not
 15 regulate “forms of conduct integral to, or commonly associated with, expression”); *Int’l*
 16 *Franchise*, 803 F.3d at 397–98, 408 (minimum wage increase ordinance classifying franchisees as
 17 large employers “exhibit[ed] nothing that even the most vivid imagination might deem uniquely
 18 expressive”) (citation omitted); *HomeAway.com*, 918 F.3d at 680, 685 (ordinance regulating forms
 19 of short-term rentals was “plainly a housing and rental regulation” that “regulate[d] nonexpressive
 20 conduct—namely, booking transactions”); *Am. Soc’y of Journalists & Authors*, 15 F.4th at 961–62
 21 (law governing classification of workers as employees or independent contractors “regulate[d]
 22 economic activity rather than speech”).

23 Second, in a decision evaluating a Vermont law restricting the sale, disclosure, and use of
 24 information about the prescribing practices of individual doctors—which pharmaceutical
 25 manufacturers used to better target their drug promotions to doctors—the Supreme Court held the
 26 law to be an unconstitutional regulation of speech, rather than conduct. *Sorrell*, 564 U.S. at 557,
 27 562, 570–71. The Supreme Court noted that it had previously held the “creation and
 28 dissemination of information are speech within the meaning of the First Amendment,” 564 U.S. at

1 570 (citing *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001); *Rubin v. Coors Brewing Co.*, 514 U.S.
 2 476, 481 (1995); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985)
 3 (plurality opinion)), and further held that even if the prescriber information at issue was a
 4 commodity, rather than speech, the law’s “content- and speaker-based restrictions on the
 5 availability and use of . . . identifying information” constituted a regulation of speech, *id.* at 570–
 6 71; *see also id.* at 568 (“An individual’s right to speak is implicated when information he or she
 7 possesses is subject to ‘restraints on the way in which the information might be used’ or
 8 disseminated.”) (quoting *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 32 (1984)).

9 The State argues that *Sorrell* does not necessitate the conclusion that the CAADCA’s
 10 prohibitions regulate speech because *Sorrell* (1) does not hold that a business has a right to collect
 11 data from individuals, and (2) is generally distinguishable on the facts because the physicians
 12 described in *Sorrell*, whose information was collected, were willing participants in the data
 13 generation who had the power to restrict the use of their information. *See* July 27, 2023 Hr’g Tr.
 14 (“Tr.”) 27:16–31:13; Opp’n 11–12; *see also id.* 1 (“Plaintiff’s members do not have a First
 15 Amendment right to children’s personal information.”). As for the first point, the State is correct
 16 that *Sorrell* does not address any general right to collect data from individuals. In fact, the
 17 Supreme Court noted that the “capacity of technology to find and publish personal information . . .
 18 presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to
 19 secure.” *Sorrell*, 564 U.S. at 579–80. But whether there is a general right to collect data is
 20 independent from the question of whether a law restricting the collection and sale of data regulates
 21 conduct or speech. Under *Sorrell*, the unequivocal answer to the latter question is that a law
 22 that—like the CAADCA—restricts the “availability and use” of information by some speakers but
 23 not others, and for some purposes but not others, is a regulation of protected expression. *Id.* at
 24 570–71. The State’s attempt to distinguish *Sorrell* based on the physicians’ ability to prevent their
 25 information from being collected, *see* Tr. 31:7–10, is not persuasive because the Supreme Court
 26 concluded that the law at issue regulated speech based on its restrictions on the use of the
 27 information after it was collected, without including any reasoning about the nature of the source
 28 of the information. *See Sorrell*, 564 U.S. at 570–71.

1 570 (“This Court has held that the creation and dissemination of information are speech within the
2 meaning of the First Amendment.”) (citations omitted).

3 Several sections require businesses to affirmatively provide information to users, and by
4 requiring speech necessarily regulate it. *See* CAADCA § 31(a)(7) (requiring businesses
5 “[p]rovide any privacy information . . . concisely, prominently, and using clear language suited to
6 the age of children likely to access that online service, product, or feature”); *id.* § 31(a)(8)
7 (requiring that businesses “provide an obvious signal to [a] child” if the child is being tracked or
8 monitored by a parent or guardian via an online service, product, or feature); *id.* § 31(a)(10)
9 (“Provide prominent, accessible, and responsive tools to help children . . . exercise their privacy
10 rights and report concerns.”); *see also, e.g., Rubin*, 514 U.S. at 481 (holding “information on beer
11 labels” constitutes speech). The CAADCA also requires a covered business to enforce its
12 “published terms, policies, and community standards”—*i.e.*, its content moderation policies.
13 CAADCA § 31(a)(9). Although the State argues that the policy enforcement provision does not
14 regulate speech because businesses are free to create their own policies, it appears to the Court that
15 NetChoice’s position that the State has no right to enforce obligations that would essentially press
16 private companies into service as government censors, thus violating the First Amendment by
17 proxy, is better grounded in the relevant binding and persuasive precedent. *See* Mot. 11; *Playboy*
18 *Ent. Grp.*, 529 U.S. at 806 (finding statute requiring cable television operators providing channels
19 with content deemed inappropriate for children to take measures to prevent children from viewing
20 content was unconstitutional regulation of speech); *NetChoice, LLC v. Att’y Gen., Fla.*
21 (*“NetChoice v. Fla.”*), 34 F.4th 1196, 1213 (11th Cir. 2022) (“When platforms choose to remove
22 users or posts, deprioritize content in viewers’ feeds or search results, or sanction breaches of their
23 community standards, they engage in First-Amendment-protected activity.”); *Engdahl v. City of*
24 *Kenosha*, 317 F. Supp. 1133, 1135–36 (E.D. Wis. 1970) (holding ordinance restricting minors
25 from viewing certain movies based on ratings provided by Motion Picture Association of America
26 impermissibly regulated speech).

27 The remaining two sections of the CAADCA require businesses to estimate the age of
28 child users and provide them with a high default privacy setting, or forgo age estimation and

1 provide the high default privacy setting to all users. CAADCA §§ 31(a)(5)–(6). The State argues
2 that “[r]equiring businesses to protect children’s privacy and data implicates neither protected
3 speech nor expressive conduct,” and notes that the provisions “say[] nothing about content and
4 do[] not require businesses to block any content for users of any age.” Opp’n 15. However, the
5 materials before the Court indicate that the steps a business would need to take to sufficiently
6 estimate the age of child users would likely prevent both children and adults from accessing
7 certain content. *See* Amicus Curiae Br. of Prof. Eric Goldman (“Goldman Am. Br.”) 4–7
8 (explaining that age assurance methods create time delays and other barriers to entry that studies
9 show cause users to navigate away from pages), ECF 34-1; Amicus Curiae Br. of New York
10 Times Co. & Student Press Law Ctr. (“NYT Am. Br.”) 6 (stating age-based regulations would
11 “almost certain[ly] [cause] news organizations and others [to] take steps to prevent those under the
12 age of 18 from accessing online news content, features, or services”), ECF 56-1. The age
13 estimation and privacy provisions thus appear likely to impede the “availability and use” of
14 information and accordingly to regulate speech. *Sorrell*, 564 U.S. at 570–71.

15 The Court is keenly aware of the myriad harms that may befall children on the internet,
16 and it does not seek to undermine the government’s efforts to resolve internet-based “issues with
17 respect to personal privacy and . . . dignity.” *See Sorrell*, 564 U.S. at 579; Def.’s Suppl. Br. 1
18 (“[T]he ‘serious and unresolved issues’ raised by increased data collection capacity due to
19 technological advances remained largely unaddressed [in *Sorrell*].”). However, the Court is
20 troubled by the CAADCA’s clear targeting of certain speakers—*i.e.*, a segment of for-profit
21 entities, but not governmental or non-profit entities—that the Act would prevent from collecting
22 and using the information at issue. As the Supreme Court noted in *Sorrell*, the State’s arguments
23 about the broad protections engendered by a challenged law are weakened by the law’s application
24 to a narrow set of speakers. *See Sorrell*, 564 U.S. at 580 (“Privacy is a concept too integral to the
25 person and a right too essential to freedom to allow its manipulation to support just those ideas the
26 government prefers”).

27 For the foregoing reasons, the Court finds that NetChoice is likely to succeed in showing
28 that the CAADCA’s prohibitions and mandates regulate speech, so that the Act triggers First

1 Amendment scrutiny.

2 **c. The Type of Speech Regulated by the CAADCA**

3 Because the Court has found the CAADCA likely regulates protected speech, it must now
 4 determine what type of speech is at issue in order to apply the appropriate level of scrutiny. As
 5 described above, *see* Part III(A)(1)(a), strict scrutiny applies to a law regulating non-commercial
 6 speech in a content-based manner, meaning the law “target[s] speech based on its communicative
 7 content.” *Reed*, 576 U.S. at 163. To survive strict scrutiny, the “the Government [must] prove
 8 that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest.”
 9 *Id.* at 171. A content-neutral regulation of non-commercial speech, on the other hand, “is
 10 constitutional as long as it withstands intermediate scrutiny—i.e., if: (1) ‘it furthers an important
 11 or substantial government interest’; (2) ‘the governmental interest is unrelated to the suppression
 12 of free expression’; and (3) ‘the incidental restriction on alleged First Amendment freedoms is no
 13 greater than is essential to the furtherance of that interest.’” *Jacobs v. Clark Cnty. Sch. Dist.*, 526
 14 F.3d 419, 434 (9th Cir. 2008) (quoting *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 661–62
 15 (1994)). And if the speech at issue is commercial, courts apply intermediate scrutiny under the
 16 four-part test articulated by the Supreme Court in *Central Hudson*, which the Ninth Circuit has
 17 described as follows:

18 (1) [I]f “the communication is neither misleading nor related to unlawful activity,”
 19 then it merits First Amendment scrutiny as a threshold matter; [and] in order for the
 20 restriction to withstand such scrutiny, (2) “[t]he State must assert a substantial
 21 interest to be achieved by restrictions on commercial speech;” (3) “the restriction
 must directly advance the state interest involved;” and (4) it must not be “more
 extensive than is necessary to serve that interest.”

22 *Metro Lights, L.L.C. v. City of Los Angeles*, 551 F.3d 898, 903 (9th Cir. 2009) (quoting *Cent.*
 23 *Hudson*, 447 U.S. at 564–66); *see also Junior Sports Mags. Inc. v. Bonta*, --- F.4th ----, 2023 WL
 24 5945879, at *4 (9th Cir. Sept. 13, 2023).

25 NetChoice argues that the CAADCA regulates non-commercial speech because the speech
 26 at issue goes beyond proposing a commercial transaction, Reply 10, and that the speech is
 27 “content-based in many obvious respects” because its “very premise [is] that providers must
 28 prioritize content that promotes the ‘well-being’ of minors,” Mot. 19. Accordingly, NetChoice

1 contends that the Act is subject to strict scrutiny. *See* Mot. 19–21; Reply 9–10. The State
2 counters that any protected expression regulated by the Act is at most commercial speech, so that
3 the Act is subject to the lower level of scrutiny described in *Central Hudson*. Opp’n 19. The State
4 argues that the Act affects how businesses persuade consumers to engage with their products—
5 such as by posting policies that aid consumers in deciding whether to engage with certain
6 products—and that consumer engagement in turn drives the regulated businesses’ revenue. *Id.*
7 Based on this revenue model, the State concludes that “there can be no doubt that regulated
8 businesses have ‘an economic motive for engaging in the [alleged] speech’ with regard to the
9 specific products—services likely to be accessed by children—that the Act regulates.” *Id.*
10 (quoting *Am. Acad. of Pain Mgmt.*, 353 F.3d at 1106).

11 Based on the record before it, the Court finds it difficult to determine whether the Act
12 regulates only commercial speech. NetChoice argues in fairly conclusory fashion that the Act
13 “regulates speech that does far more than ‘propose a commercial transaction’” and that the for-
14 profit nature of a website “does not render [its] content commercial speech” because many
15 covered businesses rely on advertisements to support the expressive content and services they
16 provide. Reply 10; *see* Mot. 2, 19–21. NetChoice provides some support for the latter argument.
17 *See, e.g.*, Roin Decl. ¶ 10 (stating that the Goodreads application earns the vast majority of its
18 revenue from advertising, including personalized advertisements targeted to registered users).
19 However, the Court notes that some sections of the CAADCA, such as those prohibiting the sale
20 of personal information, *see generally* CAADCA § 31(b), may well be analyzed as regulating only
21 commercial speech. *See, e.g., Hunt v. City of Los Angeles*, 638 F.3d 703, 715–16 (9th Cir. 2011)
22 (finding speech commercial because it was “directed to their products and why a consumer should
23 buy them” and not “inextricably intertwined” with non-commercial speech). Ultimately, the Court
24 finds that NetChoice has not provided sufficient material to demonstrate that it is likely to succeed
25 in showing that the Act regulates either purely non-commercial speech or non-commercial speech
26 that is inextricably intertwined with commercial speech. It is NetChoice’s burden to make that
27 showing in order to trigger application of strict scrutiny. *See, e.g., Yim*, 63 F.4th at 793 (“The
28 parties on appeal dispute whether the Ordinance regulates commercial speech and calls for the

1 application of intermediate scrutiny, or whether the Ordinance regulates [content-based] non-
2 commercial speech and is subject to strict scrutiny review.”).

3 However, as the Ninth Circuit reasoned in *Yim*, the Court “need not decide that question, . .
4 . because [it] conclude[s] that the [Act] does not survive the intermediate scrutiny standard of
5 review” for commercial speech. *Id.*; see also *Junior Sports Mags.*, 2023 WL 5945879, at *4 (“We
6 need not decide this issue because ‘the outcome is the same whether a special commercial speech
7 inquiry or a stricter form of judicial scrutiny is applied.’”) (quoting *Sorrell*, 564 U.S. at 571).
8 Accordingly, the Court will assume for the purposes of the present motion that only the lesser
9 standard of intermediate scrutiny for commercial speech applies because, as shown below, the
10 outcome of the analysis here is not affected by the Act’s evaluation under the lower standard of
11 commercial speech scrutiny.

12 **d. Application of Commercial Speech Scrutiny to the CAADCA**

13 Under the standard for commercial speech scrutiny, if the regulation restricts speech that is
14 neither misleading nor related to unlawful activity, it is the State’s burden to show “at least that
15 the statute directly advances a substantial governmental interest and that the measure is drawn to
16 achieve that interest.” *Sorrell*, 564 U.S. at 572 (citations omitted); *Junior Sports Mags.*, 2023 WL
17 5945879, at *5 (“Under *Central Hudson*, a state seeking to justify a restriction on commercial
18 speech bears the burden to prove that its law directly advances that [substantial] interest to a
19 material degree.”). That is, “the restriction must directly advance the state interest involved,” and
20 it must not be “more extensive than is necessary to serve that interest.” *Cent. Hudson*, 447 U.S. at
21 66. These “last two steps of the *Central Hudson* analysis basically involve a consideration of the
22 fit between the legislature’s ends and the means chosen to accomplish those ends.” *Hunt*, 638
23 F.3d at 717 (quoting *Rubin*, 514 U.S. at 786) (internal quotation marks omitted). The government
24 need not employ the least restrictive means to advance its interest, but the means employed may
25 not be “substantially excessive.” *Id.* (quoting *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S.
26 469, 479 (1989)).

27 **i. Substantial State Interest**

28 There is no dispute that the CAADCA regulates speech that is neither misleading nor

1 related to unlawful activity. The Court thus turns directly to the question of whether the State can
 2 show a substantial state interest to which the CAADCA is geared. The State asserts a substantial⁴
 3 interest in “protecting the physical, mental, and emotional health and well-being of minors.”
 4 Def.’s Suppl. Br. 1–2; *see also* Opp’n 20 (describing substantial state interest in ““safeguarding
 5 the physical and psychological well-being of a minor”); Tr. 71:6–13 (accord); *id.* at 74:25–75:3
 6 (“[T]he government has a compelling interest [in] the nature of online space for children.”).
 7 NetChoice does not dispute that “the well-being of children is a compelling interest in the
 8 abstract,” but argues that the CAADCA does not identify a sufficiently concrete harm that the law
 9 addresses. Mot. 21–22. However, the State has presented evidence that children are currently
 10 harmed by lax data and privacy protections online. *See* Radesky Decl. ¶¶ 45–47 (privacy settings
 11 often allow unwanted contact), ¶¶ 64–68 (profiling leads to children being targeted with ads for
 12 monetization and extreme dieting). In light of this evidence, and given that the Supreme Court has
 13 repeatedly recognized a compelling interest in “protecting the physical and psychological well-
 14 being of minors,” the Court finds that NetChoice is not likely to show that the State has not
 15 satisfied its burden of showing a substantial interest under the commercial speech scrutiny
 16 standard. *Sable Comm’cns of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989); *see also New York v.*
 17 *Ferber*, 458 U.S. 747, 756 (1982) (“It is evident beyond the need for elaboration that a State’s
 18 interest in ‘safeguarding the physical and psychological well-being of a minor’ is ‘compelling.’”) (quoting
 19 *Globe Newspaper Co. v. Super. Ct.*, 457 U.S. 596, 607 (1982)).

20 ii. Means-Ends Fit

21 After the State shows a substantial interest, the Court evaluates the commercial speech
 22 regulation under the last two prongs of the *Central Hudson* analysis, *i.e.*, whether the “restriction .
 23 . . directly advance[s] the state interest involved” and whether it is not “more extensive than is
 24 necessary to serve that interest.” *Metro Lights, L.L.C.*, 551 F.3d at 903 (quoting *Cent. Hudson*,
 25 447 U.S. at 564–66). As noted above, the “last two steps of the *Central Hudson* analysis basically
 26

27 ⁴ Because the State argues that the CAADCA satisfies both strict scrutiny and commercial speech
 28 scrutiny, it occasionally describes its interest as “compelling,” rather than “substantial.” *See, e.g.*,
 Opp’n 19–20. The Court treats those arguments as supporting the State’s position that it has a
 substantial state interest as required by the commercial speech scrutiny standard.

1 involve a consideration of the fit between the legislature’s ends and the means chosen to
2 accomplish those ends.” *Hunt*, 638 F.3d at 717 (citation omitted). Once again, it is the State’s
3 burden to show that the statute satisfies the standards set forth by *Central Hudson*. *Junior Sports*
4 *Mags.*, 2023 WL 5945879, at *4 (citations omitted); *see also Sorrell*, 564 U.S. at 572.

5 NetChoice argues that certain provisions of the CAADCA—namely, CAADCA §§
6 31(a)(1)–(7), 31(a)(9), 31(b)(1)–(4), and 31(b)(7)—fail commercial speech scrutiny, and that the
7 entire statute must be enjoined because the invalid provisions are not severable from the otherwise
8 valid remainder.⁵ *See* Pl.’s Suppl. Br. in Suppl. of Mot. for Prelim. Inj. (“Pl.’s Suppl. Br.”), ECF
9 71, at 2–7. The State argues that all of the mandates and prohibitions of the CAADCA satisfy
10 commercial speech scrutiny because each provision is appropriately tailored to the State’s
11 substantial interest in protecting the physical, mental, and emotional health and well-being of
12 minors. *See* Def.’s Suppl. Br. 2–7. The Court will first address whether the specific provisions of
13 the Act challenged by NetChoice survive commercial speech scrutiny before turning to the issue
14 of severability.

15 (1) DPIA Report Requirement (CAADCA § 31(a)(1)-(4))

16 The State contends that the CAADCA’s DPIA report requirement furthers its substantial
17 interest in protecting children’s safety because the provisions will cause covered businesses to
18 proactively assess “how their products use children’s data and whether their data management
19 practices or product designs pose risks to children,” so that “fewer children will be subject to
20 preventable harms.” Def.’s Suppl. Br. 2–3. According to the State’s expert, “[c]hildren’s digital
21 risks and opportunity are shaped by the *design* of digital products, services, and features,” and
22 businesses currently take a reactive approach by removing problematic features only after harm is
23 discovered. *See* Radesky Decl. ¶ 40 (emphasis added). For example, the mobile application
24 Snapchat ended the use of a speed filter after the feature was linked to dangerous incidents of
25 reckless driving by adolescents. *Id.* ¶ 41.

26
27
28 ⁵ The Court refers to those portions of the Act not challenged by NetChoice as a “valid remainder”
for the purposes of its decision on the motion for preliminary injunction, but does not intend to
suggest it has conducted an analysis and found those unchallenged provisions to be legally valid.

1 Accepting the State’s statement of the harm it seeks to cure, the Court concludes that the
2 State has not met its burden to demonstrate that the DPIA provisions in fact address the identified
3 harm. For example, the Act does not require covered businesses to assess the potential harm of
4 product *designs*—which Dr. Radesky asserts cause the harm at issue—but rather of “the risks of
5 material detriment to children that arise from the *data management practices* of the business.”
6 CAADCA § 31(a)(1)(B) (emphasis added). And more importantly, although the CAADCA
7 requires businesses to “create a timed plan to mitigate or eliminate the risk before the online
8 service, product, or feature is accessed by children,” *id.* § 31(a)(2), there is no actual requirement
9 to adhere to such a plan. *See generally id.* § 31(a)(1)-(4); *see also* Tr. 26:9–10 (“As long as you
10 write the plan, there is no way to be in violation.”), ECF 66.

11 “A restriction ‘directly and materially advances’ the government’s interests if the
12 government can show ‘the harms it recites are real and that its restriction will in fact alleviate them
13 to a material degree.’” *Yim*, 63 F.4th at 794 (quoting *Fla. Bar v. Went For It, Inc.*, 515 U.S. 618,
14 626 (1995)). Because the DPIA report provisions do not require businesses to assess the potential
15 harm of the design of digital products, services, and features, and also do not require actual
16 mitigation of any identified risks, the State has not shown that these provisions will “in fact
17 alleviate [the identified harms] to a material degree.” *Id.* The Court accordingly finds that
18 NetChoice is likely to succeed in showing that the DPIA report provisions provide “only
19 ineffective or remote support for the government’s purpose” and do not “directly advance” the
20 government’s substantial interest in promoting a proactive approach to the design of digital
21 products, services, and feature. *Id.* (citations omitted). NetChoice is therefore likely to succeed in
22 showing that the DPIA report requirement does not satisfy commercial speech scrutiny. *See*
23 *Junior Sports Mags.*, 2023 WL 5945879, at *4 (“Because California fails to satisfy its burden to
24 justify the proposed speech restriction, [Plaintiff] is likely to prevail on the merits of its First
25 Amendment claim.”).

26 (2) Age Estimation (CAADCA § 31(a)(5))

27 The CAADCA requires that covered businesses “[e]stimate the age of child users with a
28 reasonable level of certainty appropriate to the risks that arise from the data management practices

1 of the business or apply the privacy and data protections afforded to children to all consumers.”
 2 CAADCA § 31(a)(5). The State argues that CAADCA § 31(a)(5) promotes the well-being of
 3 children by requiring covered businesses to “provide data and privacy protections to users based
 4 on estimated age or, if the business does not estimate age, apply child-appropriate data and privacy
 5 protections to all users.”⁶ Def.’s Suppl. Br. 3. This argument relies on the state legislature’s
 6 finding that greater data privacy “necessarily means greater security and well-being.” *Id.* (quoting
 7 AB 2273 § 1(a)(4)). NetChoice counters that the age estimation provision does not directly
 8 advance the State’s substantial interest in children’s well-being because the practical process of
 9 such estimation involves further information collection that is itself invasive. *See* Reply 5–6;
 10 Goldman Am. Br. 2–4.

11 As described above, for the Act to survive commercial speech scrutiny, the State must
 12 show that the CAADCA’s challenged provisions directly advance a substantial government
 13 interest by materially alleviating real harms. *See Yim*, 63 F.4th at 794; *Junior Sports Mags.*, 2023
 14 WL 5945879, at *5. Based on the materials before the Court, the CAADCA’s age estimation
 15 provision appears not only unlikely to materially alleviate the harm of insufficient data and
 16 privacy protections for children, but actually likely to exacerbate the problem by inducing covered
 17 businesses to require consumers, including children, to divulge additional personal information.
 18 The State argues that age estimation is distinct from the more onerous exercise of age verification,
 19 that the statute requires only a level of estimation that is appropriate to the risk presented by a
 20 business’s data management practices, and that there are “minimally invasive” age estimation
 21 tools, some of which are already used by NetChoice’s member companies. *See* Opp’n 15–16. But
 22 even the evidence cited by the State about the supposedly minimally invasive tools indicates that
 23 consumers might have to permit a face scan, or that businesses might use “locally-analyzed and
 24 stored biometric information” to signal whether the user is a child or not. *See id.* at 16 (citing
 25

26 ⁶ The Court notes that the age estimation provision does not itself require any specific protections;
 27 the required data and privacy protections for either minors (if the business estimates age) or all
 28 users (if the business does not estimate age) are set forth in the remainder of the statute, and
 especially at CAADCA §§ 31(b)(1)–(8).

1 Radesky Decl. ¶ 96); *see also* Radesky Decl. ¶ 96(b) & n.92 (noting Google’s use of facial age-
 2 estimation software),⁷ ¶ 96(d) (noting businesses receive signals from hardware devices based on
 3 “locally-analyzed and stored biometric information” that indicate whether a user is a child).
 4 Further, as noted in Professor Goldman’s amicus brief, age estimation is in practice quite similar
 5 to age verification, and—unless a company relies on user self-reporting of age, which provides
 6 little reliability—generally requires either documentary evidence of age or automated estimation
 7 based on facial recognition. *See* Goldman Am. Br. 3–4. Such measures would appear to counter
 8 the State’s interest in increasing privacy protections for children. For these reasons, the State has
 9 not met its burden under *Central Hudson* and thus NetChoice is likely to succeed in showing that
 10 the age estimation clause does not satisfy commercial speech scrutiny. *See Yim*, 63 F.4th at 794
 11 (“[A] statute cannot meaningfully advance the government’s stated interests if it contains
 12 exceptions that ‘undermine and counteract’ those goals.”) (quoting *Rubin*, 514 U.S. at 489).

13 If a business does not estimate age, it must “apply the privacy and data protections
 14 afforded to children to all consumers.” CAADCA § 31(a)(5). Doing so would clearly advance the
 15 government’s interest in increasing data and privacy protections for children. NetChoice argues,
 16 however, that the effect of this requirement would be to restrain a great deal of protected speech.
 17 *See* Mot. 13–14, Reply 12. The Court is indeed concerned with the potentially vast chilling effect
 18 of the CAADCA generally, and the age estimation provision specifically. The State argues that
 19 the CAADCA does not prevent any specific content from being displayed to a consumer, even if
 20 the consumer is a minor; it only prohibits a business from profiling a minor and using that
 21 information to provide targeted content. *See, e.g.*, Opp’n 16. Yet the State does not deny that the
 22 end goal of the CAADCA is to reduce the amount of harmful content displayed to children. *See*
 23 *id.* (“[T]he Act prevents businesses from attempting to increase their profits by using children’s
 24 data to deliver them things they do not want and have not asked for, such as ads for weight loss
 25 supplements and content promoting violence and self-harm.”); Def.’s Suppl. Br. 6 (“Children are

26
 27 ⁷ Although Dr. Radesky states that Google’s current system involves facial recognition only by
 28 adults who have been placed in “child mode” through a machine-learning analysis, Radesky Decl.
 ¶ 96(b), there is nothing to suggest that companies would not request all consumers to undergo
 such a process.

1 unable to avoid harmful unsolicited content—including extreme weight loss content and gambling
2 and sports betting ads—directed at them based on businesses’ data collection and use practices.”).

3 Putting aside for the moment the issue of whether the government may shield children
4 from such content—and the Court does not question that the content is in fact harmful—the Court
5 here focuses on the logical conclusion that data and privacy protections intended to shield children
6 from harmful content, if applied to adults, will also shield adults from that same content. That is,
7 if a business chooses not to estimate age but instead to apply broad privacy and data protections to
8 all consumers, it appears that the inevitable effect will be to impermissibly “reduce the adult
9 population . . . to reading only what is fit for children.” *Butler v. Michigan*, 352 U.S. 380, 381, 383
10 (1957). And because such an effect would likely be, at the very least, a “substantially excessive”
11 means of achieving greater data and privacy protections for children, *see Hunt*, 638 F.3d at 717
12 (citation omitted), NetChoice is likely to succeed in showing that the provision’s clause applying
13 the same process to all users fails commercial speech scrutiny.

14 For these reasons, even accepting the increasing of children’s data and privacy protections
15 as a substantial governmental interest, the Court finds that the State has failed to satisfy its burden
16 to justify the age estimation provision as directly advancing the State’s substantial interest in
17 protecting the physical, mental, and emotional health and well-being of minors, so that NetChoice
18 is likely to succeed in arguing that the provision fails commercial speech scrutiny. *See Junior*
19 *Sports Mags.*, 2023 WL 5945879, at *4.

20 (3) High Default Privacy Settings (CAADCA § 31(a)(6))

21 CAADCA § 31(a)(6) requires covered businesses to “[c]onfigure all default privacy
22 settings provided to children . . . to settings that offer a high level of privacy, unless the business
23 can demonstrate a compelling reason that a different setting is in the best interests of children.”
24 The State argues that high privacy settings “demonstrably keep children safe.” Def.’s Suppl. Br.
25 3–4 (citing Radesky Decl. ¶¶ 57–60). The evidence before the Court indicates that lower default
26 privacy settings may quickly lead to individuals perceived as adolescents “receiv[ing] direct
27 messages from accounts they did not follow, including being added to group chats with strangers
28 and contacts from marketers of detrimental material such as pornography and diet products.”

1 Radesky Decl. ¶ 59. Accordingly, the Court finds that the State is likely to establish a real harm,
2 as required under commercial speech scrutiny. *See Yim*, 63 F.4th at 794.

3 The instant provision, however, does not make clear whether it applies only to privacy
4 settings on accounts created by children—which is the harm discussed in the State’s materials,
5 *see, e.g.*, Radesky Decl. ¶ 59—or if it applies, for example, to any child visitor of an online
6 website run by a covered business. NetChoice has provided evidence that uncertainties as to the
7 nature of the compliance required by the CAADCA is likely to cause at least some covered
8 businesses to prohibit children from accessing their services and products altogether. *See, e.g.*,
9 NYT Am. Br. 5–6 (asserting CAADCA requirements that covered businesses consider various
10 potential harms to children would make it “almost certain that news organizations and others will
11 take steps to prevent those under the age of 18 from accessing online news content, features, or
12 services”). Although the State need not show that the Act “employs . . . the least restrictive
13 means” of advancing the substantial interest, the Court finds it likely, based on the evidence
14 provided by NetChoice and the lack of clarity in the provision, that the provision here would serve
15 to chill a “substantially excessive” amount of protected speech to the extent that content providers
16 wish to reach children but choose not to in order to avoid running afoul of the CAADCA. *See*
17 *Hunt*, 638 F.3d at 717 (citation omitted). Accordingly, the State has not met its burden under
18 *Central Hudson* of showing “a reasonable fit between the means and ends of the regulatory
19 scheme,” *Junior Sports Mags.*, 2023 WL 5945879, at *7 (quoting *Lorillard Tobacco Co. v. Reilly*,
20 533 U.S. 525, 561 (2001)), so that NetChoice is likely to succeed in showing the restriction fails
21 commercial speech scrutiny.

22 (4) Age-Appropriate Policy Language (CAADCA § 31(a)(7))

23 The CAADCA next requires covered businesses to “[p]rovide any privacy information,
24 terms of service, policies, and community standards concisely, prominently, and using clear
25 language suited to the age of children likely to access that online service, product, or feature.”
26 CAADCA § 31(a)(7). The State argues this provision “protects the safety and well-being of
27 minors” by “giving children the tools to make informed decisions about the services with which
28 they interact.” Def.’s Suppl. Br. 4.

1 The evidence submitted by the State indicates that the harm it seeks to address is a lack of
2 consumer understanding of websites’ privacy policies. *See id.* (citing Egelman Decl.); *see also*
3 Egelman Decl. ¶ 52. The State has shown that internet users generally do not read privacy
4 policies, and that the reason may be that such policies are often “written at the college level and
5 therefore may not be understood by a significant proportion of the population (much less
6 children).” Egelman Decl. ¶ 27; *see id.* ¶ 24. The Court notes that the research-based claims in
7 Dr. Egelman’s declaration do not appear to be based on studies involving minors and the impact of
8 policy language on their use of online services. *See id.* at, e.g., ¶¶ 18–19, 24–27, 52.

9 Even accepting that the manner in which websites present “privacy information, terms of
10 service, policies, and community standards,” CAADCA § 31(a)(7), constitutes a real harm to
11 children’s well-being because it deters children from implementing higher privacy settings, the
12 State has not shown that the CAADCA’s policy language provision would directly advance a
13 solution to that harm. The State points only to a sentence in Dr. Egelman’s declaration stating that
14 he “believe[s] the [Act] addresses this issue [of lack of consumer understanding of privacy
15 policies] by requiring the language to be understandable by target audiences (when their online
16 services are likely to be accessed by children).” Egelman Decl. ¶ 52; *see* Def.’s Suppl. Br. 4
17 (citing same). Nothing in the State’s materials indicates that the policy language provision would
18 materially alleviate a harm to minors caused by current privacy policy language, let alone by the
19 terms of service and community standards that the provision also encompasses. NetChoice is
20 therefore likely to succeed in showing that the provision fails commercial speech scrutiny. *See*
21 *Yim*, 63 F.4th at 794.

22 (5) Internal Policy Enforcement (CAADCA § 31(a)(9))

23 CAADCA § 31(a)(9) requires covered businesses to “[e]nforce published terms, policies,
24 and community standards established by the business, including, but not limited to, privacy
25 policies and those concerning children.” As an initial matter, although the State argues that
26 “businesses have to be accountable for the commitments they make to [] consumers” for “children
27 and parents to make informed decisions about the products children access,” Def.’s Suppl. Br. 5,
28 the State fails to establish a concrete harm. The State points to Dr. Radesky’s declaration, which

1 asserts that “[s]tudies have shown that businesses are not enforcing their privacy policies,”
2 “mak[ing] it challenging for consumers to make informed decisions about whether they want to
3 join different online communities [without] knowing whether stated policies and standards will be
4 followed.” Radesky Decl. ¶ 93; *see* Def.’s Suppl. Br. 5. The State has not provided anything
5 remotely nearing a causal link between whether a business consistently follows its “published
6 terms, policies, and community standards”—or even children’s difficulty in making better-
7 informed decisions about whether to use online services—and some harm to children’s well-being.
8 On this basis alone, NetChoice is likely to succeed in showing that the policy enforcement
9 provision fails commercial speech scrutiny. *See Yim*, 63 F.4th at 794 (noting the government must
10 show that “the harms it recites are real”) (citation omitted).

11 Further, even if the State is able to show a concrete harm to children’s well-being, the
12 provision on its face goes beyond enforcement of policies related to children, or even privacy
13 policies generally. *See* CAADCA § 31(a)(9) (requiring enforcement of terms “including, but not
14 limited to, privacy policies and those concerning children”). The lack of any attempt at tailoring
15 the proposed solution to a specific harm suggests that the State here seeks to force covered
16 businesses to exercise their editorial judgment in permitting or prohibiting content that may, for
17 instance, violate a company’s published community standards. The State argues that businesses
18 have complete discretion to set whatever policies they wish, and must merely commit to following
19 them. *See* Opp’n 14; Def.’s Suppl. Br. 5. It is that required commitment, however, that flies in
20 the face of a platform’s First Amendment right to choose in any given instance to permit one post
21 but prohibit a substantially similar one. *See NetChoice v. Fla.*, 34 F.4th at 1204–05, 1228 (finding
22 content moderation restrictions impinged on business’s protected curation of content).

23 Lastly, the Court is not persuaded by the State’s argument that the provision is necessary
24 because there is currently “no law holding online businesses accountable for enforcing their own
25 policies,” Def.’s Suppl. Br. 5, as the State itself cites to a Ninth Circuit case permitting a lawsuit to
26 proceed where the plaintiff brought a breach of contract suit against an online platform for failure
27 to adhere to its terms. *See id.*; *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1108–09 (9th Cir. 2009).

28 For the multiplicity of reasons described above, Court finds that the State has not met its

1 burden of justifying the policy enforcement provision, and that NetChoice is therefore likely to
 2 succeed in showing that the provision fails commercial speech scrutiny.

3 (6) Knowingly Harmful Use of Children’s Data (CAADCA § 31(b)(1))

4 As previously noted, CAADCA § 31(a) contains the Act’s mandates, and CAADCA §
 5 31(b) enumerates its prohibitions. The first of these prohibitions forbids a covered business from
 6 “[using] the personal information of any child in a way that the business knows, or has reason to
 7 know, is materially detrimental to the physical health, mental health, or well-being of a child.”
 8 CAADCA § 31(b)(1).

9 The Third Circuit’s decision in *ACLU v. Mukasey* is instructive here. In *Mukasey*, which
 10 went up to the Supreme Court twice and was finally decided by the Court of Appeals, the court
 11 held that a law prohibiting the transmission of “material that is harmful to minors” was not
 12 narrowly tailored because it required evaluation of a wide range of material that was not in fact
 13 harmful, and because the law’s definition of a “minor” as anyone under 17 years of age would
 14 cause “great uncertainty in deciding what minor could be exposed to” the material. *ACLU v.*
 15 *Mukasey*, 534 F.3d 181, 191, 193 (3d Cir. 2008) (cert. denied). The Third Circuit also rejected the
 16 government’s affirmative defense that regulated companies could use age verification techniques
 17 to achieve greater certainty as to what material was prohibited to a given user. *Id.* at 196–97.

18 The CAADCA does not define what uses of information may be considered “materially
 19 detrimental” to a child’s well-being, and it defines a “child” as a consumer under 18 years of age.
 20 *See* CAADCA § 30. Although there may be some uses of personal information that are
 21 objectively detrimental to children of any age, the CAADCA appears generally to contemplate a
 22 sliding scale of potential harms to children as they age. *See, e.g.*, Def.’s Suppl. Br. 3, 4
 23 (describing Act’s requirements for “age-appropriate” protections). But as the Third Circuit
 24 explained, requiring covered businesses to determine what is materially harmful to an “infant, a
 25 five-year old, or a person just shy of age seventeen” is not narrowly tailored. *Mukasey*, 534 F.3d
 26 at 191. Although the law in *Mukasey* was evaluated under a strict scrutiny standard, the Court
 27 finds the same concerns apply here, so that the State has not met its burden of showing the instant
 28 provision is reasonably tailored to the State’s substantial interest, and thus NetChoice is likely to

1 succeed in showing that the provision fails commercial speech scrutiny. NetChoice has provided
 2 evidence that covered businesses might well bar all children from accessing their online services
 3 rather than undergo the burden of determining exactly what can be done with the personal
 4 information of each consumer under the age of 18. *See, e.g.*, NYT Am. Br. 5–6 (asserting
 5 CAADCA requirements that covered businesses consider various potential harms to children
 6 would make it “almost certain that news organizations and others will take steps to prevent those
 7 under the age of 18 from accessing online news content, features, or services”). The provision at
 8 issue would likely “burden substantially more speech than is necessary to further the government’s
 9 legitimate interests,” and therefore NetChoice is likely to succeed in demonstrating that it fails
 10 commercial speech scrutiny. *See Yim*, 63 F.4th at 795–96 (quoting *Fox*, 492 U.S. at 478).

11 (7) Profiling Children by Default (CAADCA § 31(b)(2))

12 CAADCA § 31(b)(2) prevents a covered business from “[p]rofil[ing] a child by default
 13 unless” (1) the business “can demonstrate it has appropriate safeguards in place to protect
 14 children” and (2) either of the following conditions is met: (a) the profiling is “necessary to
 15 provide the online service, product, or feature requested and only with respect to the aspects of the
 16 online service, product, or feature with which the child is actively engaged” or (b) the business can
 17 “demonstrate a compelling reason that profiling is in the best interests of children.” The State
 18 argues this provision protects children’s well-being because businesses commonly profile children
 19 by default and place them into target audience categories for products related to harmful content
 20 such as smoking, gambling, alcohol, or extreme weight loss. Def.’s Suppl. Br. 5–6; Radesky Decl.
 21 ¶ 66. The Court accepts the State’s assertion of a concrete harm to children’s well-being, *i.e.*, the
 22 use of profiling to advertise harmful content to children, and turns to the issue of tailoring.

23 NetChoice has provided evidence indicating that profiling and subsequent targeted content
 24 can be beneficial to minors, particularly those in vulnerable populations. For example, LGBTQ+
 25 youth—especially those in more hostile environments who turn to the internet for community and
 26 information—may have a more difficult time finding resources regarding their personal health,
 27 gender identity, and sexual orientation. *See Amicus Curiae Br. of Chamber of Progress, IP*
 28 *Justice, & LGBT Tech Inst.* (“LGBT Tech Am. Br.”), ECF 42-1, at 12–13. Pregnant teenagers are

1 another group of children who may benefit greatly from access to reproductive health information.
2 *Id.* at 14–15. Even aside from these more vulnerable groups, the internet may provide children—
3 like any other consumer—with information that may lead to fulfilling new interests that the
4 consumer may not have otherwise thought to search out. The provision at issue appears likely to
5 discard these beneficial aspects of targeted information along with harmful content such as
6 smoking, gambling, alcohol, or extreme weight loss.

7 The State argues that the provision is narrowly tailored to “prohibit[] profiling by default
8 when done solely for the benefit of businesses, but allows it . . . when in the best interest of
9 children.” Def.’s Suppl. Br. 6. But as amici point out, what is “in the best interest of children” is
10 not an objective standard but rather a contentious topic of political debate. *See* LGBT Tech Am.
11 Br. 11–14. The State further argues that children can still access any content online, such as by
12 “actively telling a business what they want to see in a recommendations profile – e.g., nature,
13 dance videos, LGBTQ+ supportive content, body positivity content, racial justice content, etc.”
14 Radesky Decl. ¶ 89(b). By making this assertion, the State acknowledges that there are wanted or
15 beneficial profile interests, but that the Act, rather than prohibiting only certain targeted
16 information deemed harmful (which would also face First Amendment concerns), seeks to prohibit
17 likely beneficial profiling as well. NetChoice’s evidence, which indicates that the provision would
18 likely prevent the dissemination of a broad array of content beyond that which is targeted by the
19 statute, defeats the State’s showing on tailoring, and the Court accordingly finds that State has not
20 met its burden of establishing that the profiling provision directly advances the State’s interest in
21 protecting children’s well-being. NetChoice is therefore likely to succeed in showing that the
22 provision does not satisfy commercial speech scrutiny. *See Yim*, 63 F.4th at 794 (noting
23 regulation that burdens substantially more speech than is necessary or undermines and counteracts
24 the state’s interest fails commercial speech scrutiny).

25 (8) Restriction on Collecting, Selling, Sharing, and Retaining Children’s Data
26 (CAADCA § 31(b)(3))

27 CAADCA § 31(b)(3) states that a covered business shall not “[c]ollect, sell, share, or retain
28 any personal information that is not necessary to provide an online service, product, or feature

1 with which a child is actively and knowingly engaged . . . unless the business can demonstrate a
 2 compelling reason that [such an action] is in the best interests of children likely to access the
 3 online service, product, or feature.” The State argues that “[e]xcessive data collection and use
 4 undoubtedly harms children” because children are “unable to avoid harmful unsolicited content—
 5 including extreme weight loss content and gambling and sports betting ads—directed at them” due
 6 to the data collection. Def.’s Suppl. Br. 6. As with the previous provision prohibiting profiling,
 7 this restriction throws out the baby with the bathwater. In seeking to prevent children from being
 8 exposed to “harmful unsolicited content,” the Act would restrict neutral or beneficial content,
 9 rendering the restriction poorly tailored to the State’s goal of protecting children’s well-being.
 10 And—in light of the State’s admission that it seeks to prevent children from consuming particular
 11 content—the Court emphasizes that the compelling and laudable goal of protecting children does
 12 not permit the government to shield children from harmful content by enacting greatly
 13 overinclusive or underinclusive legislation. *See, e.g., Brown v. Ent. Merchants Ass’n*, 564 U.S.
 14 786, 802–04 (2011) (holding California law prohibiting sale or rental of violent video games to
 15 minors failed strict scrutiny). For the same reasons described above, *see supra*, at Part
 16 III(A)(1)(a)(iv)(9), CAADCA § 31(b)(3) NetChoice is likely to succeed in showing the provision
 17 fails commercial speech scrutiny.

18 (9) Unauthorized Use of Children’s Personal Information (CAADCA §
 19 31(b)(4))

20 CAADCA § 31(b)(4) prohibits a covered business from using a child’s “personal
 21 information for any reason other than a reason for which that personal information was collected,
 22 unless the business can demonstrate a compelling reason that use of the personal information is in
 23 the best interests of children.” The State clarifies this fairly circular restriction with an example:
 24 “a business that uses a child’s IP address solely to provide access to its platform cannot also use
 25 the IP address to sell ads.” Def.’s Suppl. Br. 6. However, the State provides no evidence of a
 26 harm to children’s well-being from the use of personal information for multiple purposes. *See id.*
 27 To the extent the harm is the same profiling concern discussed in the prior two sections, the State
 28 has not met its burden to show that the instant provision is not similarly overbroad. *See supra*, at

1 Parts III(A)(1)(a)(iv)(7)–(8). Because the State has not established a real harm that the provision
2 materially alleviates, NetChoice will likely succeed in showing that the provision fails commercial
3 speech scrutiny. *See Yim*, 63 F.4th at 794.

4 (10) Use of Dark Patterns (CAADCA § 31(b)(7))

5 The last CAADCA provision challenged by NetChoice prohibits the “[u]se [of] dark
6 patterns to lead or encourage children to provide personal information beyond what is reasonably
7 expected to provide that online service, product, or feature[,] to forego privacy protections, or to
8 take any action that the business knows, or has reason to know, is materially detrimental to the
9 child’s physical health, mental health, or well-being.” CAADCA § 31(b)(7). Dark patterns are
10 design features that “nudge” individuals into making certain decisions, such as spending more
11 time on an application. Def.’s Suppl. Br 7; *see also* Opp’n 9 (describing dark patterns as
12 “interfaces designed or manipulated with the substantial effect of subverting or impairing user
13 autonomy, decision-making, or choice”); Radesky Decl. ¶ 54 (“[D]esign features that manipulate
14 or nudge the user in a way that meets the technology developer’s best interests – at the expense of
15 the user’s interests (i.e., time, money, sleep) – have been termed ‘dark patterns.’”). The State
16 argues that businesses use dark patterns to “nudge children into making decisions that are
17 advantageous to businesses,” and that “dark patterns can make it difficult or impossible for
18 children to avoid harmful content.” Def.’s Suppl. Br. 7. NetChoice contends that the term “dark
19 patterns” has also been “construed by scholars to reach commonplace features that simplify and
20 improve user experience, such as standard ‘autoplay’ and ‘newsfeed’ functions that recommend
21 personalized content.” Mot. 6 (citation omitted).

22 The instant provision can be analytically divided into three parts. It first prohibits the use
23 of dark patterns to encourage children to “provide personal information beyond what is reasonably
24 expected to provide that online service, product, or feature.” CAADCA § 31(b)(7). This
25 prohibition is similar to the profiling restrictions discussed above in that (1) the State has not
26 shown a harm resulting from the provision of more personal information “beyond what is
27 reasonably expected” for the covered business to provide its online service, product, or feature,
28 and (2) to the extent the harm is the use of profiling information to present harmful content to a

1 child, the State has not shown that the instant provision is sufficiently tailored to survive
2 commercial speech scrutiny. *See supra*, at Parts III(A)(1)(a)(iv)(7)–(9).

3 Second, the provision prohibits the use of dark patterns to encourage a child to “forego
4 privacy protections.” CAADCA § 31(b)(7). However, the State has not shown that dark patterns
5 causing children to forego privacy protections constitutes a real harm. *See Yim*, 63 F.4th at 794.
6 Many of the examples of dark patterns cited by the State’s experts—such as making it easier to
7 sign up for a service than to cancel it or creating artificial scarcity by using a countdown timer,
8 Egelman Decl. ¶ 51, or sending users notifications to reengage with a game or auto-advancing
9 users to the next level in a game, Radesky Decl. ¶ 55—are not causally connected to an identified
10 harm. *See Brown*, 564 U.S. at 799 (finding lack of “direct causal link between violent video
11 games and harm to minors” showed government had not identified “actual problem in need of
12 solving,” so that law failed strict scrutiny); *Yim*, 63 F.4th at 794 (noting commercial speech
13 scrutiny requires government to show “the harms it recites are real”)

14 The most concrete potential harm the Court can find is in Dr. Radesky’s assertion that
15 “[m]anipulative dark patterns are known to cause monetary harm to children,” based on a March
16 2023 FTC complaint requiring a game developer to pay \$245 million “as a penalty for the use of
17 dark patterns to manipulate users into making purchases.” Radesky Decl. ¶ 56. The State does
18 not, however, suggest that the CAADCA is an attempt to address monetary harms to children. *See*
19 *generally* Opp’n; Def.’s Suppl. Br. Similarly, although the State points to an existing federal law
20 limiting the practice of making it inconvenient for users to prevent their data from being sold or
21 shared, *see* Def.’s Suppl. Br. 7 (citing 16 CFR § 312.7), the State does not show how this law
22 indicates a harm to minors caused by the sale of personal information. *See generally id.*; Radesky
23 Decl.; Egelman Decl. To the extent the harm is the use of data to profile users, including children,
24 the State has not shown that the provision is appropriately tailored to survive commercial speech
25 scrutiny for the same reasons described above. *See supra*, at Parts III(A)(1)(a)(iv)(7)–(9). The
26 Court accordingly finds that the State is not likely to show a harm in dark patterns causing
27 children to forego privacy protections, so that NetChoice is likely to succeed in showing that this
28 restriction fails commercial speech scrutiny. *See Junior Sports Mags.*, 2023 WL 5945879, at *7

1 (reversing denial of preliminary injunction and reasoning that “[i]n the end, California spins a web
2 of speculation—not facts or evidence—to claim that its restriction on speech will significantly
3 curb” an alleged harm).

4 The last of the three prohibitions of CAADCA § 31(b)(7) concerns the use of dark patterns
5 to “take any action that the business knows, or has reason to know, is materially detrimental” to a
6 child’s well-being. The State here argues that dark patterns cause harm to children’s well-being,
7 such as when a child recovering from an eating disorder “must both contend with dark patterns
8 that make it difficult to unsubscribe from such content and attempt to reconfigure their data
9 settings in the hope of preventing unsolicited content of the same nature.” Def.’s Suppl. Br. 7; *see*
10 *also* Amicus Curiae Br. of Fairplay & Public Health Advocacy Inst. (“Fairplay Am. Br.”) 4
11 (noting that CAADCA “seeks to shift the paradigm for protecting children online,” including by
12 “ensuring that children are protected from manipulative design (dark patterns), adult content, or
13 other potentially harmful design features.”) (citation omitted), ECF 53-1. The Court is troubled by
14 the “has reason to know” language in the Act, given the lack of objective standard regarding what
15 content is materially detrimental to a child’s well-being. *See supra*, at Part III(A)(1)(a)(iv)(7).
16 And some content that might be considered harmful to one child may be neutral at worst to
17 another. NetChoice has provided evidence that in the face of such uncertainties about the statute’s
18 requirements, the statute may cause covered businesses to deny children access to their platforms
19 or content. *See* NYT Am. Br. 5–6. Given the other infirmities of the provision, the Court declines
20 to wordsmith it and excise various clauses, and accordingly finds that NetChoice is likely to
21 succeed in showing that the provision as a whole fails commercial speech scrutiny.

22 **iii. Conclusion re Commercial Speech Scrutiny**

23 For the foregoing reasons, the Court finds that NetChoice is likely to succeed in showing
24 that the CAADCA’s challenged mandates and prohibitions fail commercial speech scrutiny and
25 therefore are invalid.

26 **e. Severability**

27 NetChoice argues that the CAADCA must be enjoined in its entirety because the
28 challenged provisions of the CAADCA—which are likely invalid—cannot be severed from the

1 Act’s remaining prohibitions and mandates, or from other provisions related to the CAADCA’s
2 application, penalties, and compliance. Pl.’s Suppl. Br. 6–7 (discussing CAADCA § 31(a)(8),
3 31(a)(10), 31(b)(5)–(6), 31(b)(8), 32, 33, and 35). The State argues that almost every provision is
4 severable, and urges the Court to sustain any provisions not found invalid. Def.’s Suppl. Br. 2.

5 “Severability is a matter of state law.” *Sam Francis Found. v. Christies, Inc.*, 784 F.3d
6 1320, 1325 (9th Cir. 2015) (quoting *Leavitt v. Jane L.*, 518 U.S. 137, 139 (1996)) (alterations
7 omitted). Under California law, the severability of the invalid parts of a statute depends on
8 whether such provisions are grammatically, functionally, and volitionally severable from the valid
9 remainder. *See Calfarm Ins. Co. v. Deukmejian*, 48 Cal. 3d 805, 821–22 (1989) (en banc).
10 Putting aside the CAADCA provisions setting forth the statute’s title, findings, and definitions,
11 CAADCA §§ 28–30, the valid remainder of the statute involve: restrictions on monitoring
12 children’s online behavior and tracking location, CAADCA § 31(a)(8); the provision of responsive
13 tools for children to exercise their privacy rights and report concerns, *id.* § 31(a)(10); the
14 collection of precise geolocation data, *id.* §§ 31(b)(5)–(6); the use of age-estimation information,
15 *id.* § 31(b)(8); the creation of a working group to deliver a report on best practices under the
16 CAADCA, *id.* § 32; the July 1, 2024 deadline for covered businesses to complete DPIA reports,
17 *id.* § 33; and the penalties for violations of the CAADCA, *id.* § 35. *See* Pl.’s Suppl. Br. 6–7.

18 The Court first notes that there is no severability clause in the CAADCA that would create
19 a presumption in favor of “sustaining the valid part” of the statute. *See Garcia*, 11 F.4th at 1120
20 (citing *Cal. Redevelopment Ass’n v. Matosantos*, 53 Cal. 4th 231, 270 (2011)). Turning to the
21 question of functional severability, the Court finds dispositive the status of the DPIA provisions.
22 As noted by NetChoice, the CAADCA provides that the State shall not initiate an action for any
23 violation of the statute without providing written notice to a covered business identifying specific
24 provisions of the Act that are alleged to have been violated. CAADCA § 35(c); *see* Pl.’s Suppl.
25 Br. 7. The Court’s determination that NetChoice is likely to succeed in showing that the DPIA
26 report requirement is invalid, *see supra*, at Part III(A)(1)(d)(ii)(1), similarly renders likely invalid
27 a condition precedent for enforcement of the remainder of the statute. Because the CAADCA is
28 not capable of “separate enforcement” without the DPIA requirement, the DPIA provisions are not

1 functionally severable from the otherwise valid portions of the statute. *People’s Advocate, Inc. v.*
2 *Super. Ct.*, 181 Cal. App. 3d 316, 332 (1986) (“The remaining provisions must stand on their own,
3 unaided by the invalid provisions nor rendered vague by their absence nor inextricably connected
4 to them by policy considerations. They must be capable of separate enforcement.”).

5 Although the Court need not review the severability of any other provision in light of the
6 DPIA report requirement’s impact on the entire CAADCA, it notes that the age estimation
7 provision, CAADCA § 31(a)(5), is the linchpin of most of the CAADCA’s provisions, which
8 specify various data and privacy protections for children. *See id.* §§ 31(a)(6), (b)(1)–(8). The
9 State concedes only that CAADCA § 31(b)(8)—which prevents the use of personal information
10 collected to estimate age for any other purpose—is rendered obsolete if the age estimation
11 provision is deemed unconstitutional. Def.’s Suppl. Br. 3. However, compliance with the
12 CAADCA’s requirements would appear to generally require age estimation to determine whether
13 each user is in fact under 18 years old. The age estimation provision is thus also not functionally
14 severable from the remainder of the statute. *See People’s Advocate*, 181 Cal. App. at 1332.

15 The futility of severance is apparent when one considers the outcome if the Court were to
16 preliminarily enjoin only the challenged provisions that NetChoice has shown are likely violative
17 of the First Amendment. The Act would consist of the provisions setting forth the statute’s title,
18 findings, and definitions; two mandates; three prohibitions; and provisions establishing a working
19 group, DPIA report deadlines, and penalties for violating the Act. *See* CAADCA §§ 28–30,
20 31(a)(8), 31(a)(10), 31(b)(5)–(6), 31(b)(8), 32–33, 35. The DPIA report deadline, *id.* § 33, is
21 meaningless without a DPIA report requirement. Five of the six required recommendations of the
22 working group track provisions of the Act that are likely invalid. *See id.* § 32(d)(1)–(5). Further,
23 even the State agrees that one of the three remaining prohibitions—that on collecting age
24 estimation data, *id.* § 31(b)(8)—“would be made obsolete” in the absence of § 31(a)(5), which
25 NetChoice has shown is likely invalid. Def.’s Suppl. Br. 3. Accordingly, the only meat left of the
26 Act would be four unchallenged mandates and prohibitions that together would require covered
27 businesses to provide children with obvious tracking signals and prominent and responsive tools to
28 exercise their privacy rights, and to refrain from collecting children’s precise geolocation data.

1 *See* CAADCA §§ 31(a)(8), 31(a)(10), 31(b)(5)–(6). All of these provisions require businesses to
 2 know their users’ ages, but the Court has found NetChoice will likely succeed in showing the age
 3 estimation provision does not pass commercial speech scrutiny. And none of the provisions can
 4 be enforced without the penalty provision, *id.* § 35, which, as described above, is hamstrung if the
 5 State cannot determine whether a covered business is in substantial compliance with the likely-
 6 invalid DPIA report requirement. These interdependencies indicate how intertwined with—and
 7 thus inseverable from—the challenged provisions are with respect to the valid remainder.

8 Given that multiple provisions of the CAADCA will be preliminarily enjoined by this
 9 order, and the Court’s determination that these provisions are not functionally severable from the
 10 presumably valid remainder of the statute, the Court concludes that it cannot sever the likely
 11 invalid portions from the statute and sustain the remainder. *See Acosta v. City of Costa Mesa*, 718
 12 F.3d 800, 820 (9th Cir. 2013) (refusing to “rewrite[e] the ordinance in order to save it”) (internal
 13 alterations and citation omitted).

14 **f. Conclusion re First Amendment Arguments (Claims 1 and 3)**

15 Based on the foregoing, the Court concludes that NetChoice has demonstrated a likelihood
 16 of success on Claim 1, which asserts that the CAADCA violates the First Amendment because the
 17 Act’s “speech restrictions . . . fail strict scrutiny and also would fail a lesser standard of scrutiny.”
 18 Compl. ¶ 82. As noted above, *see supra*, at Part III(A)(1), the Court need not and does not here
 19 address NetChoice’s likelihood of success on its allegations of additional First Amendment
 20 violations in Claims 1 and 3.

21 **2. Other Claims**

22 NetChoice has demonstrated a likelihood of success on the merits of Claim 1 brought
 23 under the First Amendment and, as discussed below, has satisfied the remaining *Winter* factors
 24 with respect to Claim 1. NetChoice is entitled to preliminary injunctive relief on that basis. Under
 25 these circumstances, the Court must determine whether it is necessary or advisable to address the
 26 likelihood of success of NetChoice’s other claims for relief at this time: Claim 4, asserting that
 27 the CAADCA violates the dormant Commerce Clause; Claim 5, asserting that the CAADCA is
 28 preempted by COPPA; and Claim 6, asserting that the CAADCA is preempted by Section 230.

1 Once a plaintiff demonstrates that a preliminary injunction is warranted based on the
2 likelihood of success on one claim, district courts in this circuit generally do not consider whether
3 the same injunctive relief could be granted based on other claims. *See, e.g., Shawarma Stackz*
4 *LLC v. Jwad*, No. 21-CV-01263-BAS-BGS, 2021 WL 5827066, at *19 (S.D. Cal. Dec. 8, 2021)
5 (“The Court need not reach the merits of the remaining state torts claims that SSL raises because
6 the Lanham Act claim and the UCL claim are sufficient to sustain a preliminary injunction.”);
7 *Seiko Epson Corp. v. Nelson*, No. 5:21-cv-00320-JWH-SPx, 2021 WL 5033486, at *3 (C.D. Cal.
8 Mar. 31, 2021) (“The Court therefore finds that Plaintiffs have demonstrated a likelihood of
9 success on the merits with respect to their first claim for relief. Plaintiffs have thus satisfied the
10 preliminary injunction standard; the Court need not analyze Plaintiffs’ other two claims for
11 relief.”); *Faison v. Jones*, 440 F. Supp. 3d 1123, 1136 n.3 (E.D. Cal. 2020) (“Because the Court
12 finds Plaintiffs are likely to succeed on the merits of their viewpoint discrimination theory, the
13 Court need not and does not address Plaintiffs’ remaining theories.”); *Medina v. Becerra*, No.
14 3:17-CV-03293 CRB, 2017 WL 5495820, at *12 (N.D. Cal. Nov. 16, 2017) (“As Medina has
15 shown a likelihood of success on the merits for his First Amendment claim, this Court need not
16 address Medina’s other claims for relief.”). This Court sees no reason to depart from the approach
17 adopted by other district courts in the Ninth Circuit.

18 Deferring consideration of NetChoice’s Commerce Clause claim is particularly appropriate
19 here, because the claim presents thorny constitutional issues that the parties briefed prior to
20 receiving the Supreme Court’s latest guidance in *Nat’l Pork Producers Council v. Ross*, 598 U.S.
21 356 (2023).⁸ *Ross* provides a comprehensive review of case law on the dormant Commerce
22 Clause, emphasizing that “the Commerce Clause prohibits the enforcement of state laws driven by
23 economic protectionism—that is, regulatory measures designed to benefit in-state economic
24 interests by burdening out-of-state competitors,” and clarifying that this “antidiscrimination
25 principle lies at the ‘very core’ of the Court’s dormant Commerce Clause jurisprudence.” *Id.*

26
27
28 ⁸ The motion and opposition were filed before *Ross* issued. The reply was filed approximately one week after *Ross* was decided, and *Ross* is cited once therein as secondary authority for an assertion made in the brief. *See* Reply 13.

1 (quotation marks, alterations, and citation omitted). The decision may call into question the
2 dormant Commerce Clause’s application where, as here, the state law at issue does not
3 discriminate against out-of-state competitors but does have an extraterritorial effect. *Ross*
4 observes that “[i]n our interconnected national marketplace, many (maybe most) state laws have
5 the ‘practical effect of controlling’ extraterritorial behavior,” and concludes that extraterritorial
6 effects alone are insufficient to implicate the dormant Commerce Clause. *See id.* at 1156–57. In
7 the Court’s view, it would be imprudent to engage in an analysis of NetChoice’s dormant
8 Commerce Clause claim where such analysis is unnecessary to a ruling on the present motion and
9 the Court does not have the benefit of the parties’ views on the impact of *Ross*.

10 With respect to NetChoice’s preemption claims, the Court’s initial view is that neither
11 would support the requested preliminary injunction. Claim 5 asserts that the CAADCA is
12 preempted by COPPA, which contains a preemption clause providing, “No State or local
13 government may impose any liability for commercial activities or actions by operators in interstate
14 or foreign commerce in connection with an activity or action described in this chapter that is
15 *inconsistent* with the treatment of those activities or actions under this section.” 15 U.S.C.A. §
16 6502(d) (emphasis added). NetChoice claims that the CAADCA is “inconsistent” with COPPA in
17 the following respects: the CAADCA applies broadly to services “likely to be accessed” by
18 children, whereas COPPA applies only to online services “directed” to children; the CAADCA
19 imposes privacy obligations that are not required by COPPA; and the CAADCA imposes
20 substantive obligations that far exceed those imposed by COPPA. *See id.* ¶¶ 114–16. NetChoice
21 additionally claims that the statutes are inconsistent because the CAADCA prohibits conduct that
22 is permitted under COPPA, including profiling a child by default and using dark patterns to
23 encourage children to provide personal information. *See id.* ¶ 117.

24 The Ninth Circuit recently held in *Jones v. Google LLC*, 73 F.4th 636, 642 (9th Cir. 2023),
25 that a state law is not “inconsistent” with COPPA for preemption purposes unless the state law
26 contains requirements that contradict those of COPPA or “stand as obstacles to federal objectives”
27 embodied in COPPA. A state law that supplements or requires the same thing as COPPA is not
28 inconsistent with COPPA. *See id.* In the Court’s view, it is not clear that the cited provisions of

1 the CAADCA contradict, rather than supplement, those of COPPA. Nor is it clear that the cited
2 provisions of the CAADCA would stand as an obstacle to enforcement of COPPA. An online
3 provider might well be able to comply with the provisions of both the CAADCA and COPPA,
4 with the possible exception of the CAADCA provisions identified in paragraph 117 of the
5 complaint. However, a determination whether those are inconsistent with COPPA for preemption
6 purposes would require a careful and nuanced analysis. It would make little sense to engage in
7 such analysis at this stage of the proceedings in light of the fact that NetChoice is entitled to the
8 requested injunctive relief based on its First Amendment claims.

9 Claim 6 asserts that the CAADCA is preempted by Section 230. Section 230 “protects
10 certain internet-based actors from certain kinds of lawsuits.” *Barnes*, 570 F.3d at 1099. As
11 relevant here, Section 230(c)(1) provides that “[n]o provider or user of an interactive computer
12 service shall be treated as the publisher or speaker of any information provided by another
13 information content provider.” 47 U.S.C. § 230(c)(1). Section 230(c)(2) provides that “[n]o
14 provider or user of an interactive computer service shall be held liable on account of . . . any action
15 voluntarily taken in good faith to restrict access to or availability of material that the provider or
16 user considers to be . . . objectionable[.]” 47 U.S.C. § 230(c)(2)(A). NetChoice contends that the
17 CAADCA’s requirement that online providers enforce their “published terms, policies, and
18 community standards,” CAADCA § 31(a)(9), and restrictions on the use of minors’ personal
19 information, CAADCA § 31(b)(1), (3), (4), (7), are inconsistent with Section 230. NetChoice
20 claims that those inconsistencies result in preemption of the CAADCA under § 230(e), which
21 provides that “[n]o cause of action may be brought and no liability may be imposed under any
22 State or local law that is inconsistent with this section.” 47 U.S.C. § 230(e)(3). Section 230 may
23 be implicated by an online provider’s enforcement of its policies and other acts in compliance with
24 the CAADCA, but it is difficult (if not impossible) to make that determination without knowing
25 what policies or acts are at issue. For that reason, it is the Court’s view that a facial challenge to
26 the CAADCA is not the appropriate context in which to consider the applicability of § 230.

27 Accordingly, the Court need not and does not determine whether NetChoice is likely to
28 succeed on the merits of its claims grounded in the dormant Commerce Clause, COPPA, and

1 Section 230. The Court limits its consideration of the remaining *Winter* factors to Claim 1 under
2 the First Amendment, namely, irreparable harm, the balance of equities, and the public interest.

3 **B. Irreparable Harm**

4 “The loss of First Amendment freedoms, for even minimal periods of time, unquestionably
5 constitutes irreparable injury.” *Elrod v. Burns*, 427 U.S. 347, 373 (1976); *see also Baird*, 2023
6 WL 5763345, at *3. Loss of free speech rights resulting from a threat of enforcement rather than
7 actual enforcement constitutes irreparable harm. *See Cuvillo v. City of Vallejo*, 944 F.3d 816,
8 833 (9th Cir. 2019). Consequently, “[i]rreparable harm is relatively easy to establish in a First
9 Amendment case.” *CTIA - The Wireless Ass’n v. City of Berkeley*, 928 F.3d 832, 851 (9th Cir.
10 2019). “[A] party seeking preliminary injunctive relief in a First Amendment context can
11 establish irreparable injury . . . by demonstrating the existence of a colorable First Amendment
12 claim.” *Id.* (quotation marks and citation omitted). As discussed above, NetChoice has done more
13 than merely assert a colorable First Amendment claim; it has established a likelihood of success
14 on the merits of its claim that the CAADCA violates the First Amendment.

15 The Court finds unpersuasive the State’s argument that the threat of enforcement is
16 insufficient to establish irreparable injury because the Act’s challenged provisions do not take
17 effect until July 1, 2024. That date is less than a year away. “One does not have to await the
18 consummation of threatened injury to obtain preventive relief. If the injury is certainly impending,
19 that is enough.” *Pac. Gas & Elec. Co. v. State Energy Res. Conservation & Dev. Comm’n*, 461
20 U.S. 190, 201 (1983) (citation omitted). Moreover, NetChoice presents evidence that businesses
21 already are expending time and funds preparing for enforcement of the CAADCA. *See Roin Decl.*
22 ¶¶ 20, 24–25; *Cairella Decl.* ¶¶ 14, 19–22; *Masnack Decl.* ¶¶ 12, 14–19; *Paolucci Decl.* ¶¶ 16–18;
23 *Szabo Decl.* ¶¶ 5–7, 12–17. Requiring businesses to proceed with such preparations without
24 knowing whether CAADCA is valid “would impose a palpable and considerable hardship” on
25 them. *See Pac. Gas & Elec.*, 461 U.S. at 201–02 (“To require the industry to proceed without
26 knowing whether the moratorium is valid would impose a palpable and considerable hardship on
27 the utilities[.]”).

28 The Court has no difficulty finding that NetChoice has established a likelihood of

1 irreparable harm absent issuance of the requested preliminary injunction.

2 **C. Balance of Equities / Public Interest**

3 “Where the government is a party to a case in which a preliminary injunction is sought, the
4 balance of the equities and public interest factors merge.” *Roman v. Wolf*, 977 F.3d 935, 940-41
5 (9th Cir. 2020); *see also Baird*, 2023 WL 5763345, at *2. As discussed above, NetChoice has
6 demonstrated a likelihood of success in proving that the CAADCA violates the First Amendment.
7 “[I]t is always in the public interest to prevent the violation of a party’s constitutional rights.”
8 *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012) (quotation marks and citation omitted).
9 Moreover, the State “cannot reasonably assert that it is harmed in any legally cognizable sense by
10 being enjoined from constitutional violations.” *Zepeda v. U.S. I.N.S.*, 753 F.2d 719, 727 (9th Cir.
11 1983).

12 The State cites *Maryland v. King*, 567 U.S. 1301, 1303 (2012), for the proposition that
13 “[a]ny time a State is enjoined by a court from effectuating statutes enacted by representatives of
14 its people, it suffers a form of irreparable injury.” *King* did not involve a motion for preliminary
15 injunction, but rather Maryland’s application for a stay of a state appellate court’s decision
16 overturning King’s rape conviction pending disposition of Maryland’s petition for writ of
17 certiorari. *See id.* at 1301. The state appellate court had determined that Maryland’s DNA
18 collection statute, which had authorized law enforcement officers to collect King’s DNA sample,
19 violated the Fourth Amendment. *See id.* The Supreme Court found that a stay was warranted
20 based on its determination that there was a reasonable probability it would grant certiorari. *See id.*
21 at 1302. It was in that context that the Supreme Court discussed the harm to the State of Maryland
22 flowing from its inability to effectuate its DNA collection statute. *See id.* at 1303. The quoted
23 language has no application here, where (unlike the State of Maryland) the State of California has
24 not made a showing that the challenged statute passes constitutional muster.

25 The Court finds that NetChoice has established that the last two factors, the balance of
26 equities and the public interest, favor issuance of the requested injunction.

27 **D. Conclusion**

28 In conclusion, the Court finds that all of the *Winter* factors favor granting the requested

1 preliminary injunction. With respect to the first and most important factor, likelihood of success
2 on the merits, NetChoice has demonstrated that it is likely to succeed on at least one of its First
3 Amendment theories set forth in Claim 1 of the complaint. NetChoice also has satisfied the
4 second factor by demonstrating a likelihood that it will suffer irreparable injury if the requested
5 preliminary injunction does not issue. Finally, NetChoice has satisfied the third and fourth factors
6 by showing that the balance of the equities and the public interest favor issuance of the requested
7 preliminary injunction.

8 “If a movant makes a sufficient demonstration on all four *Winter* factors (three when as
9 here the third and fourth factors are merged), a court must not shrink from its obligation to enforce
10 his constitutional rights, regardless of the constitutional right at issue.” *Baird*, 2023 WL 5763345,
11 at *3 (quotation marks, citation, and brackets omitted). “It may not deny a preliminary injunction
12 motion and thereby allow constitutional violations to continue simply because a remedy would
13 involve intrusion into an agency’s administration of state law.” *Id.* (quotation marks and citation
14 omitted).

15 NetChoice’s motion for preliminary injunction is GRANTED.

16 **E. Security**

17 Federal Rule of Civil Procedure 65(c) provides that “[t]he court may issue a preliminary
18 injunction or a temporary restraining order only if the movant gives security in an amount that the
19 court considers proper to pay the costs and damages sustained by any party found to have been
20 wrongfully enjoined or restrained.” Fed. R. Civ. P. 65(c). The Ninth Circuit has “recognized that
21 Rule 65(c) invests the district court with discretion as to the amount of security required, *if any.*”
22 *Jorgensen v. Cassidy*, 320 F.3d 906, 919 (9th Cir. 2003) (internal quotation marks and citation
23 omitted) (italics in original). Thus, the district court has discretion to dispense with the filing of a
24 bond altogether, or to require only a nominal bond. *See id.* (“The district court may dispense with
25 the filing of a bond when it concludes there is no realistic likelihood of harm to the defendant from
26 enjoining his or her conduct.”); *see also Save Our Sonoran, Inc. v. Flowers*, 408 F.3d 1113, 1126
27 (9th Cir. 2005) (“The district court has discretion to dispense with the security requirement, or to
28 request mere nominal security, where requiring security would effectively deny access to judicial

1 review.”) (citation omitted).

2 Neither party addresses the issue of security in its briefing. NetChoice’s proposed order,
3 filed with its motion for preliminary injunction, provides that the requested injunctive relief will
4 issue without the requirement of any security bond because NetChoice has shown a likelihood of
5 success and the State will not suffer any harm from maintaining the status quo. *See* Proposed
6 Order, ECF 29-31. The State argues, as a reason to deny injunctive relief altogether, that issuance
7 of the injunction “would inflict irreparable harm upon California by preventing enforcement of a
8 statute enacted by representatives of the people.” Opp’n at 30. The State’s argument gives no
9 indication, however, whether the State believes a bond should be required in the event a
10 preliminary injunction issues, or the appropriate amount of such bond. *See id.*

11 The Court finds it appropriate to issue the preliminary injunction without requiring security
12 based on NetChoice’s showing that it is likely to prevail on its claim that enforcement of the
13 CAADCA violates the First Amendment—and thus could not be lawfully enforced by the State—
14 and the absence of any argument that a security bond should be required.

15 //

16 //

17 //

18

19

20

21

22

23

24

25

26

27


28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IV. ORDER

- (1) Plaintiff NetChoice’s motion for preliminary injunction is GRANTED as follows:
- (a) Rob Bonta, Attorney General of the State of California, and anyone acting in concert with his office are ENJOINED from enforcing the California Age-Appropriate Design Code Act;
 - (b) This preliminary injunction shall issue without the requirement of a security bond; and
 - (c) This preliminary injunction shall take effect immediately and shall remain in effect until otherwise ordered by the Court.
- (2) This order terminates ECF 29.

Dated: September 18, 2023



BETH LABSON FREEMAN
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
No. 5:22-CV-00518

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	
v.)	COMPLAINT FOR PERMANENT
)	INJUNCTION, CIVIL PENALTIES, AND
EPIC GAMES, INC.,)	OTHER RELIEF
)	
Defendant.)	

Plaintiff, the United States of America, acting upon notification and on behalf of the Federal Trade Commission (“Commission” or “FTC”), for its Complaint alleges:

1. Plaintiff brings this action under Sections 5(a)(1), 5(m)(1)(A), 13(b), 16(a)(1), and 19 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), 56(a)(1), 57b, and Sections 1303(c) and 1306(d) of the Children’s Online Privacy Protection Act of 1998 (“COPPA”), 15 U.S.C. §§ 6502(c), 6505(d), to obtain monetary civil penalties, a permanent injunction, and other relief for Defendant’s violations of Section 5 of the FTC Act and the Children’s Online Privacy Protection Rule (“Rule” or “COPPA Rule”), 16 C.F.R. pt. 312.

SUMMARY OF CASE

2. Epic Games, Inc. (“Epic,” “Epic Games,” or “Defendant”) is the developer and distributor of the hit online video game “Fortnite.” Through Fortnite, Epic matches

children and teens with strangers around the world in interactive gameplay, encourages real-time communications by featuring on-by-default voice and text chat features, and publicly broadcasts players' account names. Even though Fortnite is directed to children, and even when Epic had actual knowledge that Fortnite users were children, Epic failed to comply with the COPPA Rule's parental notice, consent, review, and deletion requirements. Although Epic has changed its practices over time, those changes have not cured the violations.

3. Ultimately, Epic's matchmaking children and teens with strangers while broadcasting players' account names and imposing live on-by-default voice and text communications has caused substantial injury that is neither offset by countervailing benefits nor reasonably avoidable by consumers. Children and teens have been bullied, threatened, and harassed within Fortnite, including sexually. Children and teens have also been exposed to dangerous and psychologically traumatizing issues, such as suicide and self-harm, through Fortnite. And the few relevant privacy and parental controls Epic has introduced over time have not meaningfully alleviated these harms or empowered players to avoid them.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

5. Venue is proper in this District under 28 U.S.C. § 1391(b)(1), (b)(2), (c)(2), and (d), and 15 U.S.C. § 53(b).

SECTION 5 OF THE FTC ACT

6. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair or deceptive acts or practices in or affecting commerce.”

CHILDREN’S ONLINE PRIVACY PROTECTION RULE

7. Congress enacted COPPA in 1998 to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children’s personal information online by operators of Internet websites and online services. COPPA directed the Commission to promulgate a rule implementing COPPA. The Commission promulgated the COPPA Rule on November 3, 1999, under Section 1303(b) of COPPA, 15 U.S.C. § 6502(b), and Section 553 of the Administrative Procedure Act, 5 U.S.C. § 553. The Rule went into effect on April 21, 2000. The Commission promulgated revisions to the Rule that went into effect on July 1, 2013. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57(a)(d)(3), a violation of the Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

8. The Rule applies to any operator of a commercial website or online service directed to children under 13 years of age that collects, uses, and/or discloses personal information from children, and to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children. The Rule requires an operator to meet specific requirements prior to

collecting, using, or disclosing children’s personal information online, including but not limited to:

- a) Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information the operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures set forth in the Rule;
- b) Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents;
- c) Obtaining verifiable parental consent prior to collecting, using, and/or disclosing personal information from children;
- d) Providing a reasonable means for parents to review personal information collected from children online, at a parent’s request; and
- e) Deleting personal information collected from children online, at a parent’s request.

DEFINITIONS

9. For purposes of this Complaint, the terms “child,” “collects,” “collection,” “disclose,” “disclosure,” “Internet,” “obtaining verifiable parental consent,” “online contact information,” “operator,” “parent,” “personal information,” and “Web site or online service directed to children,” are defined as those terms are defined in Section 312.2 of the COPPA Rule, 16 C.F.R. § 312.2.

DEFENDANTS

10. Defendant Epic Games, Inc. is a Maryland corporation with its principal place of business at 620 Crossroads Blvd., Cary, North Carolina 27518. Epic transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Epic has advertised, marketed, distributed, or sold the video game Fortnite and in-game Fortnite content to consumers throughout the United States.

COMMERCE

11. At all times relevant to this Complaint, Epic has maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

EPIC’S BUSINESS ACTIVITIES

About Epic and Fortnite

12. Epic is the developer of Fortnite, a hit online video game available to players on multiple consoles, including the Sony PlayStation, Microsoft Xbox, and Nintendo Switch, mobile devices with Android or iOS operating systems, and personal computers with Windows or MacOS operating systems. Launched in July 2017, Fortnite quickly caught the attention of young consumers—teens and children under age 13—in the United States and abroad and, today, has more than 400 million players.

13. Available in different modes, Fortnite is generally free to download and play (although one mode, called “Save the World,” costs money). Epic has earned

billions of dollars in revenue through Fortnite, primarily by selling Fortnite players in-game digital content like costumes (called “cosmetics” or “skins”) and dance moves (called “emotes”) for their avatars, and through licensing partnerships with companies selling Fortnite-branded merchandise.

Epic Collects Personal Information From Fortnite Players

14. To play Fortnite using a personal computer or mobile device, players must first create an Epic Games account. Prior to September 2019, anyone could create an Epic Games account by providing Epic Games with their first name, last name, and email address, and choosing a name (called a “display name”) for their account. This remains the process for players located outside the United States and Europe. For players in the United States or Europe, however, Epic began requiring birthdate information as part of the account creation process on September 11, 2019 (for U.S. players), September 2, 2021 (for U.K. players), and November 30, 2021 (for European players outside the U.K.).

15. To play Fortnite on a PlayStation, Xbox, or Switch console, players can choose to create an Epic Games account, register their console to an already-created Epic Games account, or access Fortnite using what Epic refers to as a “nameless” account. If a player chooses this last option to play Fortnite on their PlayStation, Xbox, or Switch console, Epic creates a “nameless” Epic Games account for that player on Epic’s backend automatically—generating a unique account ID for the player, associating that unique account ID to the player’s PlayStation, Xbox, or Switch console, and collecting the

player's PlayStation, Xbox, or Switch account name for use as the player's display name within Fortnite.

16. Regardless of the console or type of account a player uses, several social features are enabled within Fortnite by default that convert the game into a platform for connecting with other players. Among other things, these social features allow players to find and friend each other (by display name), play matches together, exchange personal information, and converse with each other in real time by voice and text. On the backend, Epic collects and uses various unique device IDs, account IDs, and other persistent identifiers to keep track of players' progress, purchases, settings, and friends lists, among other player-specific information.

Fortnite Is Directed to Children Under 13

17. Considering the factors set forth in the COPPA Rule, including the game's subject matter, use of animation, child-oriented activities and language, and music content, evidence of intended audience, and empirical evidence about the game's player demographics, Fortnite is directed to children under age 13.

Fortnite's Gameplay, Visual Content, and Features are Directed to Children

18. Revolving around a "shooter-survival" style of gameplay, Fortnite's various game modes include "build-and-create" mechanics like those in other games popular with children, and feature other elements that appeal to children, like cartoony graphics and colorful animation. For example, in Fortnite's popular "Battle Royale" mode, players' colorful avatars enter the game by hang gliding to various places in a

virtual world (e.g., “Loot Lake,” “Tilted Towers,” “Retail Row”) after jumping from a whimsical flying blue school bus, called the “Battle Bus.”



19. Akin to digital laser tag, there is no blood or gore in Fortnite, and players are “eliminated” from the game (not “killed”).



20. Prominent in Fortnite gameplay is an emphasis on building “forts” and other creations—offering children a digital playground to explore. As Epic noted when announcing the game’s release in 2017, the “soul of Fortnite” derives from the common childhood experience of fort-building—“whether it was blankets and couch cushions, or building a fort in the woods by your house, you and your friends could spend Saturday afternoons hiding out, or repelling hordes of imaginary creatures”—and the game incorporates “sculpted ‘puzzle pieces’ to create interesting play spaces to explore.”¹

Fortnite Theming Decisions Ensure Content Appeals to Children

21. Epic strives to create a “Living room safe, but barely” environment using content that appeals to children when making Fortnite theming decisions, including potential music, celebrity, and brand partnerships. In so doing, Epic Games employees have explained:

- “We want to be living room safe, but barely. We don’t want your mom to love the game – just accept it compared to alternatives”
- “Agree with the idea that, generally, all theming should be relevant to a 8-14 y.o., as a litmus test”
- “We are NOT adult: experience must allow for parental comfort for ages 10+”

Based on these guiding principles, Fortnite has promoted and hosted live in-game concerts featuring celebrities popular with children, such as Marshmello, Travis Scott, Ariana Grande, and BTS.

¹ See, e.g., Darren Sugg, *Build, Explore, Craft, and Fight on July 25*, EpicGames.com (June 8, 2017), <https://www.epicgames.com/fortnite/en-US/news/build-explore-craft-and-fight-on-july-25?lang=en-US>.

***Epic Has Made Millions in Royalties Selling Official
Fortnite Toys, Halloween Costumes, and Youth Apparel***

22. Further evidencing the game’s intended audience, Epic has made millions in royalties by partnering with companies to sell officially licensed Fortnite merchandise for children. Within a year of Fortnite’s public release, Epic retained a licensing agent and launched a consumer products program to give players official Fortnite-branded merchandise.

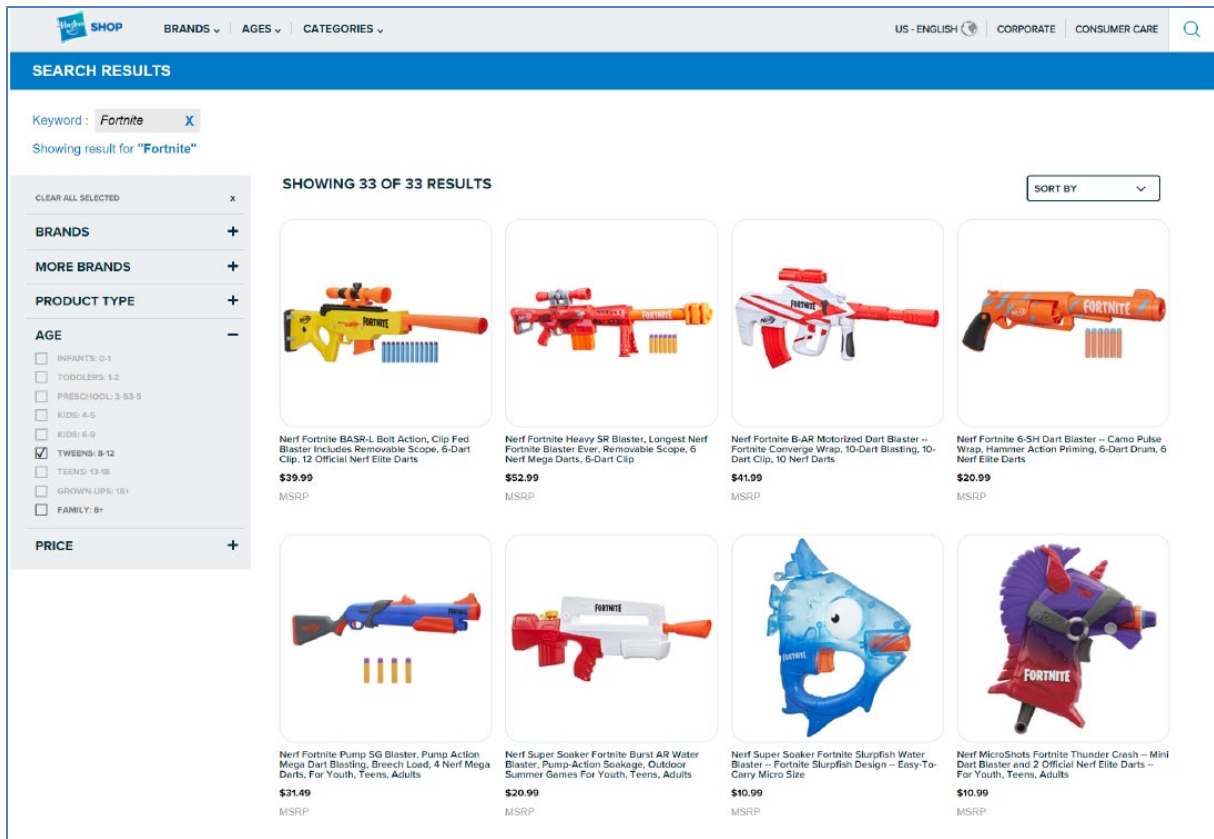
23. Acknowledging that “Youth and Kids are obsessed with Fortnite” and “want to show their allegiance to their favorite pastime,” Epic’s agent developed a licensing plan with a “core” component that targeted “Kids” and “Youth Universes,” and worked closely with Epic to broker partnerships between Epic and other companies to create Fortnite-branded costumes, toys, books, youth-sized apparel, and “back to school” merchandise (e.g., backpacks, pencil cases, etc.). And while Epic’s licensing agent has helped source and manage these merchandising partnerships, Epic carefully scrutinizes all potential licensees, sets the terms governing each partnership, and approves every Fortnite-branded product that gets produced—including the product’s design and packaging, and related advertising and marketing plans.

24. In its first consumer products deal, Epic partnered with Spirit Halloween to offer officially licensed Fortnite Halloween costumes. Available in children’s sizes, these costumes have been very popular with kids and spawned articles with headlines like

“Excited Kids Are Baffling Adults With Their *Fortnite* Halloween Fervor.”² Indeed, Spirit Halloween sold hundreds of thousands of child-sized *Fortnite* costumes between 2018 and 2020, which account for more than half of all *Fortnite* costumes sold by Spirit Halloween during those years.

25. In another early consumer products deal, Epic partnered with Hasbro to offer players *Fortnite*-branded Nerf guns, Super Soaker water guns, and other popular kids’ toys. Consistent with the core demographic for Hasbro’s Nerf products, the “*Fortnite X Nerf*” product line launched in early 2019 using a “#*Fortnite*IRL [In Real Life]” tagline with paid advertisements in media channels targeting “6-11 year old boys.” Today, through its partnership with Epic, Hasbro offers more than 40 different officially licensed *Fortnite* toys on its website, including three Super Soaker products for “Kids: 6-9,” and 33 different Nerf, Super Soaker, and other toys for “Tweens: 8-12” (as reflected in the screenshot below).

² Gita Jackson, *Excited Kids Are Baffling Adults With Their Fortnite Halloween Fervor*, Kotaku.com (Oct. 26, 2018, 3:30 pm), <https://kotaku.com/excited-kids-are-baffling-adults-with-their-fortnite-ha-1830029419>. See also Cady Lang, *The Most Popular Halloween Costume This Year Is So 2018*, Time.com (Oct. 19, 2018, 11:02 am), <https://time.com/5429462/best-halloween-costumes-2018/>; Chloe Wilt, *The 10 Most Popular Halloween Costume Ideas This Year, According to Google*, Money.com (Oct. 11, 2019), <https://money.com/top-halloween-costumes-2019-deals/>; Kyler Alvord, *Google’s Most-Searched Halloween Costumes of 2020 Could Be Better*, Thrillist.com (Oct. 29, 2020), <https://www.thrillist.com/news/nation/googles-most-searched-halloween-costumes-2020>.



26. In addition to Hasbro, Epic has partnered with other companies like Jazwares and Moose Toys to produce official Fortnite action figures, playsets, and other toys. As with the Epic-Hasbro partnership, toys from the Epic-Jazwares and Epic-Moose Toys partnerships were marketed to and for kids, including through television commercials targeting those aged 12-17 that aired on the Cartoon Network, Nickelodeon, and Nicktoons (Epic-Jazwares), and video advertisements on YouTube and Twitch intended to reach “Fortnite fans 8-12” and “Fortnite fans 13-21” (Epic-Moose Toys). And toys from all three partnerships were marketed through seasonal toy catalogs from retailers like Amazon, Target, and Walmart (including the 2019 Walmart toy catalog excerpted below).



27. Notably, a toy from the Epic-Jazwares partnership—the Fortnite Llama Loot Pinata—tied with Lego’s Harry Potter products to win the “Toys / Games / Novelties for Ages 0-12” category at the 2019 International Licensing Awards. As the head of Epic’s consumer products program explained internally, Epic won the “Newcomer” award that year after Fortnite or Fortnite-branded products won first place awards in five categories—despite being “up against some heavy hitters like Harry Potter, Jurassic World, and Lego.”

28. By the first half of 2020, Epic’s consumer products program had generated more than \$1 billion in gross sales of Fortnite-branded merchandise, bringing more than \$130 million in gross royalties to Epic and its licensing agent. Most of this success was

driven by the popularity of Epic’s official Fortnite toys, which accounted for nearly 70% (~\$650 million) of all Fortnite-branded merchandise sales, and more than 60% (~\$80 million) of the royalties from such sales, through the first quarter of 2020.

Many Children Play Fortnite, and Many Fortnite Players Are Children

29. Not surprisingly, empirical evidence shows that many children play Fortnite, which is disproportionately popular with “tweens.” For example, publicly available survey results from a 2019 report show that 53% of U.S. children aged 10-12 played Fortnite weekly, compared to 33% of U.S. teens aged 13-17, and 19% of the U.S. population aged 18-24.³ And Epic, which had previously contracted with the company that conducted this survey (to conduct a different survey in connection with Fortnite), received pre-publication copies of the survey results along with a private briefing by the researchers who conducted the survey.

30. Results from Epic’s own player surveys are consistent with this data. While Epic avoided collecting Fortnite players’ precise ages (until it instituted the limited age gating described below in Paragraphs 54 through 58), Epic has consistently asked about players’ living situation and occupation through player surveys—and used the results as a proxy for players’ age demographics. The results show that most Fortnite players (i.e., approximately 70%) live at home with their parents or guardians, and, of those who live with their parents or guardians, most (i.e., approximately 80%) identify as

³ National Research Group, *Fortnite: The New Social Media?* (June 4, 2019), available at <https://www.nationalresearchgroup.com/news/fortnite-the-new-social-media>.

students. And when soliciting potential brand partnerships for Fortnite, Epic has used social media data to emphasize Fortnite's popularity among young gamers—noting that a third of Fortnite players, based on social media data, are teens aged 13-17 (i.e., the youngest age demographic available in the social media data, which cuts off at age 13).

Epic Knows that Children Play Fortnite

31. Epic knows that children play Fortnite. Epic employees and player support agents review and respond to thousands of player-related requests, reports, and complaints that come in each day, many of which identify specific Fortnite players as being children under 13.

32. Epic and its employees also regularly monitor, read, and circulate news articles and social media posts chronicling Fortnite's popularity among children, and sometimes incorporate kids' ideas directly into the game. For example, the concept behind a popular "cosmetic" (i.e., outfit for players' in-game avatars) in Fortnite, called "Tender Defender," originated in the mind of an eight-year-old Fortnite player whose father had shared his son's idea on the social media site Reddit.com, where it caught the attention of Epic's Fortnite development team.

33. Epic, too, has sent Fortnite "swag"—i.e., Fortnite-branded merchandise—intended for children under 13, including in response to celebrities' swag requests for their "Fortnite obsessed" children. And to help Epic evaluate potential new features, the former Game Director for Fortnite would bring his son, who was under 13 years old, to participate in internal company playtests of Fortnite.

34. Further, when Epic lobbied Microsoft and Sony to support cross-console gameplay, allowing, e.g., Xbox Fortnite users to play with PlayStation Fortnite users, Epic stressed the feature's impact on kids, noting for example that "many Fortnite players are kids" and that cross-console gameplay would "bring together current and potential gamers in real-world social groups: college dorms, high school classes, even kids . . ."

35. Epic's records include other acknowledgements, too. In numerous internal communications, Epic employees have reported being inundated with Fortnite questions and requests during in-person conversations with players under 13, watching kids perform Fortnite dances in public, and receiving notes from teachers about Fortnite's popularity with their middle and elementary school students. In other ordinary course business communications, Epic employees have noted that "a large portion of our player base" consists of "underage kids," acknowledged Fortnite's "high penetration among tweens/teens," flagged "that Fortnite is enjoyed by a very young audience at home and abroad," and described putting on Fortnite "dance cam," "makeup booth (for kids)," and other events at public gaming conferences (where most attendees were "very young")—including events where "[t]he idea was that any kid or teenager playing could feel like a pro."

Fortnite's Unfair Default Settings Have Harmed Children and Teens

36. Predictably, Epic has caused substantial harm by matching children and teens with strangers in interactive gameplay while publicly broadcasting players' display

names and imposing real-time communications through on-by-default voice and text chat.

37. Epic has known about this harm and nevertheless allowed it to persist. Shortly after Fortnite's launch, Epic's then Director of User Experience ("UX") emailed Epic leadership in August 2017 seeking "basic toxicity prevention" mechanisms—noting that "surely a lot of kids" were currently playing the game, and imploring Epic to "avoid voice chat or have it opt-in at the very least." To no avail. Voice chat remained on by default, including in Fortnite's Battle Royale mode when Epic enabled voice chat for that mode in October 2017. While Epic contemporaneously added a toggle on a settings page enabling those who happened to find it to switch voice chat off, the feature remained on as part of Fortnite's default configuration for all players.

38. Within two weeks of Epic's October 2017 decision to enable voice chat in Battle Royale, a high-profile gamer verbally harassed a young player while publicly streaming to an audience of thousands of viewers. As an Epic Games employee acknowledged: ". . . we honestly should have seen this coming or [at least] expected this with an on-by-default voice chat system. Situations like this are bound to happen . . ." But Epic again declined to modify its on-by-default voice chat system (or implement any other changes) to stop subjecting kids to such abuse within Fortnite.

39. Eight months later, in June 2018, Epic's UX research team analyzed the parental and privacy controls offered by a wide range of other games and game platforms, and presented the results of their assessment to Epic executives and other

employees. Epic’s UX team reiterated their recommendation to move to an opt-in voice chat configuration for Fortnite, noting that most players did not use the feature when playing with strangers, which presented “a risk in terms of negative social behavior,” and acknowledging “[f]rom social/media stories we have seen both ‘Fortnite is positive’ and ‘child charity warns parents about predators in Fortnite’ . . .” Epic leadership praised the “very well-researched and thoughtful” work, but the UX team “got no traction” around opt-in voice chat. Epic continued to reject the UX team’s recommendation.

40. All the while, kids have been bullied, threatened, and harassed, including sexually, through Fortnite. Numerous news stories chronicle reports of predators blackmailing, extorting, or coercing children and teens they met through Fortnite into sharing explicit images or meeting offline for sexual activity. Such issues are also the subject of numerous player support tickets submitted to Epic by distressed parents and players.

41. In addition, Epic’s Fortnite practices have exposed kids to dangerous and psychologically traumatizing issues, such as suicide and self-harm. For example, in a May 2018 email to Epic’s customer support leads, one employee noted that Epic’s player support tickets included “834 cases created in the last year that contain the words ‘kill myself’ and 485 containing the word ‘suicide,’” including “cases such as toxicity reports from players who were told to kill themselves by others.” As one parent explained in an email to Epic, “[t]his morning, while on Fortnite, my 9 year old son had a ‘friend’

(someone he doesn't know in real life, but has been playing with for months) tell him that he was going to kill himself tonight. It shook him to the core.”

42. As reflected in internal exchanges between Epic employees, these harms are not outweighed by countervailing benefits, nor are they reasonably avoidable by consumers. Shortly before the UX team's unsuccessful push to convince leadership to change Fortnite's default settings in June 2018, an Epic employee who had helped create Fortnite emailed Epic's PR manager and Epic's Creative Director:

I think you both know this, but our voice and chat controls are total crap as far as kids and parents go. It's not a good thing. It was on my list a year ago, but never bubbled to the surface. This is one of those things that the company generally has weak will to pursue, but really impacts our overall system and perception. I've made a coppa [sic] compliant game and we are far from it, but we don't need to be that far . . .

To which Epic's PR manager responded:

100% agree here. Communication-wise, we are staying out of the debate, even though Fortnite is right in the middle of it. We'd come out looking way better if we offered the proper tools across the board here. I agree the best response is doing the right thing, and not debating it . . .

The employee then forwarded the exchange to Epic's lead UX researcher, who replied “I would really like to see even the small step of on first load asking if people want voice on or off. Even hardcore games like Monster Hunter have done this.” And when articulating the UX team's position to Epic executives a week later, Epic's lead UX researcher noted a good opt-in system yielded only upside: it would align with players' reported preferences (“when playing with strangers the majority [of Fortnite players] are not typically using it to talk or listen to them”), preserve the feature's utility (“[t]here is

no doubt that voice is strongly valued by folks when talking to people they know, and by a significant minority who like to use it to talk to strangers . . . A good opt-in system should maintain this”), and reduce toxicity (“[f]or example when Riot moved to opt-in text chat they saw the same volume of chat usage, but reduced toxicity as those who want to chat were able to communicate and those that did not were not exposed”).

43. As noted in Paragraph 37, Epic did introduce a toggle switch allowing Fortnite players to turn voice chat off, but the control was buried on a hard-to-find settings page. As one Fortnite programmer lamented:

So when I was at my brothers house, and was watching my 10 yr old nephew play. I’m like, hey, why is there no sound on the TV? And he’s like, we turn off the volume because you can hear people talking. People related to me by blood were no sh[**] muting the TV instead of looking for a way to disable voice chat. Not a proud day . . . The settings are not a land most folks venture to, certainly not technophobic parents . . .

When this message was forwarded to Epic’s lead UX researcher, he responded with exasperation: “Sigh. Can we just suggest popping up a dialog asking people if they want it on or not?”

Epic’s Changes Have Not Cured the Law Violations

44. Over time, Epic has introduced a few changes to Fortnite in weak-willed attempts to provide players and their parents with some privacy and parental controls, and

comply with COPPA’s parental notice, consent, review, and deletion requirements. But these overdue efforts have not cured the law violations.

Epic Has Consistently Resisted, Deprioritized, and Delayed Privacy and Parental Controls

45. Fortnite launched with no parental controls and minimal privacy settings. Initially, the only such options consisted of a few settings allowing players to “mute,” “block,” or “kick” (i.e., remove from shared gameplay activities)⁴ individual problematic players they encountered, or narrow the set of players who could join them in collaborative gameplay (i.e., by changing their “Party Privacy” setting from “public” to “friends of friends,” “friends,” or “private”). Neither players nor their parents could prevent a player’s display name from being publicly broadcast or disable voice and text chat (except by using parental controls and voice chat settings when playing Fortnite on gaming consoles that provide such controls and settings).

46. Shortly after launch, Epic introduced the toggle switch discussed above, allowing Fortnite players to disable voice chat, but did not inform players of the setting’s availability and placed the control in the middle of a detailed settings page. Seven months later, in May 2018, Epic introduced a setting called “Streamer Mode” that, when enabled, hid a player’s display name and the display names of those the player

⁴ These settings enable one to ignore incoming voice and text chat messages from a particular Fortnite player (via the “Mute Player” setting); defriend a particular player, ignore any subsequent friend requests from that player, and stop the blocked player from participating in voice or text chats (via the “Block Player” setting); and remove a particular player from collaborative gameplay (via the “Kick Player” setting).

encountered during gameplay. After surveying players and finding that many who enabled this control were seeking to avoid harassment—and were not actual “streamers” (i.e., players who publicly live-streamed their gameplay)—Epic split the feature into an “Anonymous Mode” setting (which hides a player’s display name during gameplay, when enabled) and “Hide Other Player Names” setting (which hides other players’ display names during gameplay, when enabled) in January 2019. In between, Epic added settings allowing Fortnite players to hide their display name from appearing in global game statistic leaderboards (in September 2018) and disable friend requests from other players (in January 2019).

47. In June 2019, nearly two years after Fortnite’s launch, Epic finally introduced parental controls to the game. Starting on that date, parents could set a PIN code that must be entered to adjust various privacy settings—i.e., Auto Decline Friend Requests, Hide Other Player Names, Anonymous Mode, and Voice Chat.⁵ Of course, to enable parental controls, parents would first need to know they existed, have access to their child’s or teen’s Fortnite account, and know where to find the controls.

For More Than Two Years, Epic Took No Steps to Seek Parental Consent Before Collecting Children’s Personal Information or Explain How the Company Handled It

48. From July 2017, when Fortnite launched, until September 2019, Epic took no steps to (a) provide a direct notice to parents describing Epic’s practices regarding the

⁵ Two months later, in August 2019, Epic began offering a setting to disable text chat within Fortnite and included this setting within the scope of its parental controls initiative.

collection, use, and disclosure of children’s personal information; (b) explain what information Epic collected from children through Fortnite; or (c) seek verifiable parental consent (“VPC”) from parents before collecting their children’s personal information through Fortnite.

49. Instead, Epic included one paragraph on the second-to-last page of its global privacy policy disavowing that it directed any services to children or intentionally collected any personal information from such players, and asking parents to contact Epic if they believed Epic had received personal information from their child:

Epic does not direct its websites, games, game engines, or applications to children (usually considered to be under the age of 13, depending on the country where you reside). We also do not intentionally collect personal information from children through our websites, games, game engines, or applications. If you are the parent or guardian of a child and you believe that we have inadvertently received personal information about that child, please contact us as described in the How to Contact Us section of this policy and we will delete the information from our records.

50. When parents contacted Epic to review or delete the information Epic collected from their child through Fortnite, or delete their child’s Epic Games account, and those parents did not have access to their child’s Fortnite account, Epic made those parents jump through extraordinary hoops to “verify” their parental status. For example, Epic required some parents to provide all IP addresses used by their child to play Fortnite, the date the child’s Epic Games account was created, an invoice ID for an Epic Games purchase, the locations (city, state/province) where purchases were made, the last 4 digits of the first payment card used on the child’s Epic Games account, the date of their child’s last Fortnite login, their child’s original Epic Games account display name,

and the names of any PlayStation, Xbox, or Switch consoles connected to their child's Epic Games account. Where parents were able to provide such information, Epic sometimes required them to provide even more information before Epic would agree to process the parent's review or deletion request—like the name of a cosmetic item their child purchased more than 30 days ago and a copy of the parent's passport, identification card, or recent rent or mortgage statement.

51. Even when Epic obtained actual knowledge that particular Fortnite players were under 13, Epic took no steps to comply with COPPA. Indeed, Epic went to great lengths to pretend it never obtained actual knowledge at all.

52. In March 2018, Microsoft personnel told Epic that Epic would have to block Xbox accounts belonging to children under 13 from participating in cross-console gameplay through Fortnite. In particular, Microsoft wanted Epic to use an existing Xbox mechanism (an API called the UserAgeGroup) to check whether a given Xbox player was using an “Adult,” “Child,” “Teen,” or “Unknown” Xbox account, and block any Xbox players using “Child” accounts (defined as accounts belonging to players under age 13) from using Fortnite's cross-console gameplay feature. In other words, Microsoft wanted Epic to use Microsoft's API to determine which Xbox accounts belonged to children under age 13 and block those accounts from participating in Fortnite's cross-console gameplay feature.

53. Although Epic initially resisted, the company ultimately acquiesced and began blocking Xbox accounts identified via the UserAgeGroup API as belonging to a

player under 13 from participating in cross-console gameplay within Fortnite. But Epic did not take any other steps to limit those players' communications with third parties, seek VPC for them, provide their parents with any notices explaining how Epic handled children's personal information, or otherwise comply with COPPA. Instead, as reflected in company records, Epic pretended they had no idea these players were children for any purpose other than determining whether they could participate in cross-console gameplay.

Epic's Dilatory COPPA Measures Fail to Comply With The Law

54. Epic eventually began to change its approach to COPPA compliance. On September 11, 2019—long after Epic obtained empirical evidence pointing to large numbers of Fortnite players under 13, received actual knowledge that many particular players were under 13, and profited from Fortnite-branded merchandise clearly directed to children—Epic introduced an age gate to the account creation process for prospective Fortnite players attempting to create an Epic Games account on the Epic Games website from an internet connection with a U.S. IP address. For any such prospective player who self-identified as being 12 years old or younger, Epic would collect a parent's email address from the player and send an email to the player's parent describing how Epic handled children's personal information and asking the parent to complete a VPC process—such as using a credit card to make a small refundable charge.

55. But this initiative had no effect on the default configurations of Fortnite players' privacy controls—which continue to enable the public broadcast of players' display names and direct communication between players, regardless of a player's age.

56. Nor did this initiative apply to those seeking to play Fortnite using new nameless accounts (i.e., accounts generated by Epic for PlayStation, Xbox, or Switch users, as described in Paragraph 15), or those creating Epic Games accounts from internet connections with an IP address outside the U.S.

57. Nor did Epic's September 11, 2019, changes apply to the hundreds of millions of Fortnite players who already had accounts, with a few limited exceptions. In the weeks before implementation, Epic employees searched Fortnite player support tickets to find those with indicia that a U.S. player may be under the age of 13. These efforts surfaced 36,000 such tickets, which Epic associated with 15,300 identifiable Fortnite players. Regardless of whether a ticket specifically identified a particular player as being under 13, or merely suggested that a player might be under 13, Epic logged all 15,300 players out of their accounts and asked them to provide their birthdate the next time the player attempted to log in—emailing parents a direct notice and asking them to complete a VPC process only if the player then self-identified as being under age 13.

58. Contemporaneously, Epic began instructing player support agents to flag accounts belonging to U.S. Fortnite players associated with new player support tickets in which players self-identified (or were identified by others) as being 12 years old or younger. Beginning on September 11, 2019, Epic started logging out any accounts with

such a flag and requiring the player to pass Epic's age gate the next time the player attempted to log in, with Epic requesting a parent's email address, sending a direct notice, and asking the parent to complete a VPC process only if the player then self-identified as being under 13.

59. Around the same time, Epic began changing how it handled emails identifying specific Fortnite players as being age 12 or younger. Previously, Epic did not take any steps to ensure the company sought VPC for such players or provided such players' parents with any notices describing how Epic handled their children's personal information. But starting in late 2019, Epic began forwarding these types of emails to player support agents, who try to determine whether the underlying player is based in the U.S. If so, and if the player has not already been subjected to Epic's age gate, the player is logged out and required to provide their birthdate the next time the player attempts to log in. Only if the player then self-identifies as being twelve or younger does Epic send their parent a direct notice and seek VPC.

60. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendant is violating or is about to violate laws enforced by the Commission.

VIOLATIONS OF THE COPPA RULE AND FTC ACT

Count I COPPA Rule

61. As described in Paragraphs 10 through 16 above, Defendant is an “operator” subject to the COPPA Rule.

62. In numerous instances, in connection with the acts and practices described above, Defendant collected, used, and disclosed personal information from children younger than age 13 in violation of the Rule by:

- a) Failing to provide notice on its website or online service of the information it collects online from children, how it uses such information, and its disclosure practices, among other required content, in violation of Section 312.4(d) of the Rule, 16 C.F.R. § 312.4(d);
- b) Failing to provide direct notice to parents of the information it collects online from children, how it uses such information, and its disclosure practices for such information, among other required content, in violation of Section 312.4(b) of the Rule, 16 C.F.R. § 312.4(b);
- c) Failing to obtain consent from parents before any collection or use of personal information from children, in violation of Section 312.5(a)(1) of the Rule, 16 C.F.R. § 312.5(a)(1);

d) Failing to provide, at the request of parents, a means of reviewing any personal information collected from children, in violation of Section 312.6(a)(3) of the Rule, 16 C.F.R. § 312.6(a)(3); and

e) Failing to delete, at the request of parents, personal information collected from children, in violation of Section 312.6(a)(2) of the Rule, 16 C.F.R. § 312.6(a)(2).

63. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

64. Defendant violated the Rule as described above with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

65. Each collection, use, or disclosure of a child's personal information in which Defendant violated the Rule in one or more of the ways described above constitutes a separate violation for which Plaintiff seeks monetary civil penalties.

66. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461; the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Public Law 114-74, sec. 701, 129 Stat. 599 (2015); and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), authorizes this Court to award monetary civil penalties of not more than \$46,517 for each violation of the Rule after January 10, 2022.

Count II
Unfair Default Settings

67. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair or deceptive acts or practices in or affecting commerce.”

68. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

69. As described in Paragraphs 10 through 35 above, Defendant has developed and operated, and continues to develop and operate, a ubiquitous, freely-available, and internet-enabled video game directed at children and teens that publicly broadcasts players’ display names while putting children and teens in direct, real-time contact with others through on-by-default lines of voice and text communication. Even after instituting an age gate on its service, Defendant has continued to broadcast display names and enable such direct communication by default for all players, including children who identify themselves as under 13 and young teens.

70. As described in Paragraphs 36 through 43 above, Defendant’s actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

71. Therefore, Defendant's acts or practices as set forth in Paragraph 69 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

CONSUMER INJURY

72. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act and the Rule. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

73. Wherefore, Plaintiff United States of America requests that the Court:
- A. Enter a permanent injunction to prevent future violations of the FTC Act and the Rule by Defendant;
 - B. Award Plaintiff monetary civil penalties from Defendant for each violation of the Rule alleged in this Complaint; and
 - C. Award any additional relief as the Court determines to be just and proper.

Dated: December 19, 2022

Respectfully submitted,

FOR THE FEDERAL TRADE
COMMISSION:

BENJAMIN WISEMAN
Acting Associate Director
Division of Privacy & Identity
Protection

MARK EICHORN
Assistant Director

ANDREW HASTY
JAMES TRILLING
AMANDA KOULOUSIAS
Attorneys
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2861 (Hasty)
(202) 326-3497 (Trilling)
(202) 326-3334 (Koulousias)
ahasty@ftc.gov
jtrilling@ftc.gov
akoulousias@ftc.gov

FOR THE UNITED STATES OF
AMERICA:

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

AMANDA N. LISKAMM
Acting Director, Consumer Protection Branch

LISA K. HSIAO
Assistant Director, Consumer Protection Branch

JOSHUA A. FOWKES
Trial Attorney

BY: /s/ Michael J. Wadden
MICHAEL J. WADDEN
Trial Attorney
Consumer Protection Branch
Civil Division
U.S. Department of Justice
Attorney for Plaintiff United States
450 5th Street, NW
Washington, DC 20530
Telephone: (202) 305-7133
Facsimile: (202) 514-8742
E-mail: michael.j.wadden@usdoj.gov
NY Bar No. 5577903

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

United States of America

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)
Michael J. Wadden, United States Department of Justice,
450 5th St., NW, Washington DC 20001

DEFENDANTS

Epic Games, Inc.

County of Residence of First Listed Defendant Wake
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

Robert Van Arnam, Williams Mullen
301 Fayetteville St., Suite 1700, Raleigh, NC 27601

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- | | |
|---|--|
| <input checked="" type="checkbox"/> 1 U.S. Government Plaintiff | <input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party) |
| <input type="checkbox"/> 2 U.S. Government Defendant | <input type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III) |

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input type="checkbox"/> 4
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS			
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- | | | | | | | |
|---|---|--|---|--|--|---|
| <input checked="" type="checkbox"/> 1 Original Proceeding | <input type="checkbox"/> 2 Removed from State Court | <input type="checkbox"/> 3 Remanded from Appellate Court | <input type="checkbox"/> 4 Reinstated or Reopened | <input type="checkbox"/> 5 Transferred from Another District (specify) | <input type="checkbox"/> 6 Multidistrict Litigation - Transfer | <input type="checkbox"/> 8 Multidistrict Litigation - Direct File |
|---|---|--|---|--|--|---|

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Federal Trade Commission Act and Children's Online Privacy Protection Act of 1998
Brief description of cause:
Unlawful collection of children's personal information

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ _____ CHECK YES only if demanded in complaint:
civil penalties in an amount of \$ _____ JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE: December 19, 2022 SIGNATURE OF ATTORNEY OF RECORD: /s/ Michael J. Wadden

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT PAID BY PLAINTIFF _____ JUDGE _____ JUDGE _____ JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

United States of America

Plaintiff(s)

v.

Epic Games, Inc.

Defendant(s)

Civil Action No. 5:22-00518

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) Epic Games, Inc.
620 Crossroads Blvd.,
Cary, North Carolina 27518

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Michael J. Wadden
U.S. Department of Justice
450 5th Street, NW
Washington, DC 20530
michael.j.wadden@usdoj.gov

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. 5:22-00518

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____ .

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*:

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
No. 5:22-CV-00518-BO

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	
v.)	STIPULATED ORDER FOR PERMANENT
)	INJUNCTION AND CIVIL PENALTY
EPIC GAMES, INC.,)	JUDGMENT
)	
Defendant.)	

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission (“Commission” or “FTC”), filed its Complaint for Civil Penalties, Permanent Injunction, and Other Relief (“Complaint”), for a permanent injunction, civil penalties, and other relief in this matter, pursuant to Sections 13(b), 16(a)(1), and 19 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b), 56(a)(1), and 57(b), the Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6502(c) and 6505(d), and the Commission’s Children’s Online Privacy Protection Rule (“COPPA Rule”), 16 C.F.R. Part 312. Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Permanent Injunction and Civil Penalty Judgment (“Order”) to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges that Defendant violated the COPPA Rule and the FTC Act by developing and operating an Internet-enabled video game with unfair default information sharing settings for Children and Teens; by failing to provide notice on Defendant's website or online service, and direct notice to Parents, of the Personal Information Defendant Collects online from Children, how Defendant uses such information, and Defendant's Disclosure practices; by failing to Obtain Verifiable Parental Consent before any Collection or use of Personal Information from Children; by failing to provide, at the request of Parents, a description of the specific types or categories of Personal Information Collected from Children; and by failing to Delete, at the request of Parents, Personal Information Collected from Children.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agree to bear their own costs and attorney fees.

5. Defendant waives all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

- A. **"Affirmative Express Consent"** means any freely given, specific, informed, and unambiguous indication of an individual's wishes

demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual of: (i) all information required by sub-Provision III.C; (ii) a simple, easily-located means for the individual to withdraw consent; (iii) any limitations on the individual's ability to withdraw such consent; and (iv) all other information material to the provision of consent. The Clear and Conspicuous disclosure must be separate from any "privacy policy," "terms of service," "terms of use," or other similar document. The following do not constitute Affirmative Express Consent:

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or
2. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.

B. **"Biometric Information"** means data that depicts or describes the physical or biological traits of an identified or identifiable individual, including: (1) identifiable depictions or identifiable information derived therefrom (e.g., extracts, models, or transcripts derived from image or video files); (2) copies of, or identifiable information derived from, an individual's facial features (e.g., faceprints, face embeddings, iris scans, retina scans, etc.), fingerprints, handprints, voice, genetics, or other physical or biological features; or (3) copies of, or identifiable information derived from, an

individual's characteristic movements or gestures (e.g., gait or typing patterns).

C. **“Child”** or **“Children”** means an individual or individuals under the age of 13.

D. **“Clear(ly) and Conspicuous(ly)”** means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.
2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
3. An audible disclosure, including streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 8. When the representation or sales practice targets a specific audience, such as Children, Teens, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- E. **“Collects,” “Collected,” “Collecting,” or “Collection”** means, for the purposes of Definitions L, N, P, T, X, Z, AA, and Provision I of this Order only, the gathering of any Personal Information from a Child by any means, including but not limited to:
1. Requesting, prompting, or encouraging a Child to submit Personal Information online;
 2. Enabling a Child to make Personal Information publicly available in identifiable form; or
 3. Passive tracking of a Child online.

- F. **“Compliance Date”** means thirty (30) days after entry of this Order.
- G. **“Covered Business”** means: (1) Defendant; and (2) any business that Defendant controls, directly or indirectly, that (i) discloses Covered Information collected from one user to another user, (ii) enables the disclosure of Covered Information from one user to another user, or (iii) enables any user to communicate with any other user. For purposes of this Order, to the extent that, after entry of this Order, Defendant obtains direct or indirect control over a business that discloses Covered Information collected from one user to another user, enables the disclosure of Covered Information from one user to another user, or enables any user to communicate with any other user, such business becomes a Covered Business sixty (60) days after the date on which Defendant obtained such control.
- H. **“Covered Information”** means the following information from or about an individual consumer: (1) Personal Information; (2) Biometric Information; (3) the content of any communication from an individual; (4) credit or debit card information; (5) a date of birth; (6) a first and last name; (7) a home or other physical address including street name and name of a city or town; (8) Online Contact Information; (9) a screen or user name where it functions in the same manner as Online Contact Information; (10) a telephone number; (11) a Social Security number; (12) a Persistent Identifier; (13) geolocation information sufficient to identify street name and name of a city or town; or

(14) information concerning an individual collected online and combined with a Persistent Identifier.

- I. **“Covered Product or Service”** means any Internet-enabled product or service controlled or operated, directly or indirectly, by any Covered Business, that: (1) discloses Covered Information collected from one user to another user; (2) enables the disclosure of Covered Information from one user to another user; or (3) enables any user to communicate with any other user.
- J. **“Defendant”** means Epic Games, Inc., a corporation, and its successors and assigns.
- K. **“Delete”** means to remove Personal Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.
- L. **“Disclose,” “Disclosed,” “Disclosing,” or “Disclosure”** means, with respect to Personal Information, for the purposes of Definitions N, X, Z, AA, and Provision I of this Order only:
 - 1. The Release of Personal Information Collected by an Operator from a Child in identifiable form for any purpose, except where an Operator provides such information to a Person who provides Support for the Internal Operations of the Website or Online Service; and
 - 2. Making Personal Information Collected by an Operator from a Child publicly available in identifiable form by any means, including but not

limited to a public posting through the Internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

- M. **“Internet”** means collectively the myriad of computer and telecommunication facilities, including equipment and operating software, which comprises the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.
- N. **“Obtain, Obtained, or Obtaining Verifiable Parental Consent”** means making any reasonable effort (taking into consideration available technology) to ensure that before Personal Information is Collected from a Child, a Parent of the Child:
1. Receives notice of the Operator’s Personal Information Collection, use, and Disclosure practices; and
 2. Authorizes any Collection, use, or Disclosure of the Personal Information.
- O. **“Online Contact Information”** means an email address or any other substantially similar identifier that permits direct contact with a Person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat identifier.

- P. “**Operator**” means any Person who operates a website located on the Internet or an online service and who Collects or maintains Personal Information from or about the users of or visitors to such website or online service, or on whose behalf such information is Collected and maintained, or offers products or services for sale through the website or online service, where such website or online service is operated for commercial purposes involving commerce among the several States, or with one or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or nation; or between the District of Columbia and any State, territory, or foreign nation.
- Q. “**Parent**” includes a legal guardian.
- R. “**Persistent Identifier**” means an identifier that can be used to recognize a user over time and across different websites or online services. Such Persistent Identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier.
- S. “**Person**” means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.
- T. “**Personal Information**” means individually identifiable information about an individual Collected online, including:
1. A first and last name;

2. A home or other physical address including street name and name of a city or town;
3. Online Contact Information;
4. A screen or user name where it functions in the same manner as Online Contact Information;
5. A telephone number;
6. A Social Security number;
7. A Persistent Identifier;
8. A photograph, video, or audio file where such file contains a Child's image or voice;
9. Geolocation information sufficient to identify street name and name of a city or town; or
10. Information concerning the Child or the Parents of that Child that the Operator Collects online from the Child and combines with a Persistent Identifier.

U. **“Principal Executive Officer”** means Timothy Sweeney for so long as he serves as Chief Executive Officer of Defendant, or such other officer (regardless of title) that is designated in Defendant's bylaws or by resolution of Defendant's board of directors as being the most senior executive officer of Defendant, acting solely in his official capacity on behalf of Defendant; or if Timothy Sweeney no longer serves in such a position, then such other individual serving as the Chief Executive Officer

of Defendant, or such other officer (regardless of title) that is designated in Defendant's bylaws or by resolution of Defendant's board of directors as being the most senior executive officer of Defendant, acting solely in their official capacity on behalf of Defendant. In the event that Timothy Sweeney is not the Principal Executive Officer and such position is jointly held by two or more individuals, then each of such individuals must be deemed to be a Principal Executive Officer.

- V. **"Privacy Setting"** means any control or setting that allows a user of a Covered Product or Service, or their Parent, to enable, and subsequently disable, restrict, or otherwise control, any disclosure of the user's Covered Information to, or ability of the user to communicate with or receive communications from, any other user of the Covered Product or Service.
- W. **"Release of Personal Information"** means the sharing, selling, renting, or transfer of Personal Information to any Third Party.
- X. **"Support for the Internal Operations of the Website or Online Service"** means:
 - 1. Those activities necessary to:
 - a. Maintain or analyze the functioning of the website or online service;
 - b. Perform network communications;
 - c. Authenticate users of, or personalize the content on, the website or online service;

- d. Serve contextual advertising on the website or online service or cap the frequency of advertising;
 - e. Protect the security or integrity of the user, website, or online service;
 - f. Ensure legal or regulatory compliance; or
 - g. Fulfill a request of a Child as permitted by 16 C.F.R. §§ 312.5(c)(3) and (4);
2. So long as the information Collected for the activities listed in paragraphs (1)(a)-(g) of this definition is not used or Disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.
- Y. “**Teen**” means an individual aged 13, 14, 15, 16, or 17.
- Z. “**Third Party**” means, for the purpose of Definition W only, any Person who is not:
- 1. An Operator with respect to the Collection or maintenance of Personal Information on the Web site or online service; or
 - 2. A Person who provides Support for the Internal Operations of the Web site or Online Service and who does not use or Disclose information protected under the COPPA Rule (attached as Appendix A) for any other purpose.

AA. **“Website or Online Service Directed to Children”** means a commercial website or online service, or portion thereof, that is targeted to Children.

1. In determining whether a website or online service, or a portion thereof, is directed to Children, the Commission will consider its subject matter, visual content, use of animated characters or Child-oriented activities and incentives, music or other audio content, age of models, presence of Child celebrities who appeal to Children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to Children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.
2. A website or online service shall be deemed directed to Children when it has actual knowledge that it is Collecting Personal Information directly from users of another website or online service directed to Children.
3. A website or online service that is directed to Children under the criteria set forth in paragraph (1) of this definition, but that does not target Children as its primary audience, shall not be deemed directed to Children if it:
 - a. Does not Collect Personal Information from any visitor prior to Collecting age information; and

- b. Prevents the Collection, use, or Disclosure of Personal Information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of the COPPA Rule (attached as Appendix A).
- 4. A website or online service shall not be deemed directed to Children solely because it refers or links to a commercial website or online service directed to Children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

ORDER

I. INJUNCTION CONCERNING THE COLLECTION OF PERSONAL INFORMATION FROM CHILDREN

IT IS FURTHER ORDERED that, no later than the Compliance Date, Defendant and Defendant's officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with being an Operator of any Website or Online Service Directed to Children or of any website or online service with actual knowledge that it is Collecting or maintaining Personal Information from a Child, are hereby permanently restrained and enjoined from:

- A. Failing to make reasonable efforts, taking into account available technology, to ensure that a Parent of a Child receives direct notice of the Operator's practices with regard to the Collection, use, or Disclosure of Personal Information from Children, including notice of any material

change in the Collection, use, or Disclosure practices to which the Parent has previously consented, unless the COPPA Rule (attached as Appendix A), provides an exception to providing such notice;

- B. Failing to post a prominent and clearly labeled link to an online notice of the Operator's information practices with regard to Children, if any, on the home or landing page or screen of its website or online service, and at each area of the website or online service where Personal Information is Collected from Children, unless the COPPA Rule (attached as Appendix A), provides an exception to providing such notice;
- C. Failing 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, unless the COPPA Rule (attached as Appendix A), provides an exception to Obtaining Verifiable Parental Consent;
- D. Failing to Delete a Child's Personal Information at the request of a Parent;
- E. Retaining a Child's Personal Information for longer than is reasonably necessary to fulfill the purpose for which the information was Collected; and
- F. Violating the COPPA Rule (attached as Appendix A).

II. INJUNCTION CONCERNING CHILDREN'S PERSONAL INFORMATION PREVIOUSLY COLLECTED

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this Order, must:

- A. Within sixty (60) days of the Compliance Date, Delete all Personal Information that is associated, at the time of the Compliance Date, with any Fortnite user, unless:
 - 1. the user has provided age information through a neutral age gate identifying the user as age 13 or older; or
 - 2. Defendant has provided direct notice and Obtained Verifiable Parental Consent; and
- B. Within ninety (90) days of the Compliance Date, provide a written statement to the Commission, sworn under penalty of perjury, that:
 - 1. Describes all processes through which Defendant provided direct notice and sought to Obtain Verifiable Parental consent for any accounts covered by this Provision II;
 - 2. Identifies the total number of accounts for which (i) direct notice was provided; (ii) Defendant Obtained Verifiable Parental Consent; (iii) verifiable parental consent was affirmatively declined; and (iv) no response was provided;

3. Describes in detail any Personal Information Defendant retains in accordance with sub-Provisions II.C or II.D, the basis for such retention, and, as applicable, the specific government agency, law, regulation, or court order that requires such retention; and
4. Confirms that all Personal Information required to be Deleted by this Provision II has been Deleted.

Provided, however, that:

- C. Persistent Identifiers that Defendant is otherwise required to Delete by this Provision II need not be Deleted to the extent they are used solely for Support for the Internal Operations of the Website or Online Service; and
- D. Personal Information that Defendant is otherwise required to Delete by this Provision II may be retained, and may be disclosed, as requested by a government agency or required by law, regulation, or court order. Within thirty (30) days after the obligation to retain any such Personal Information has ended, Defendant shall Delete such Personal Information and provide an additional written statement to the Commission, sworn under penalty of perjury, confirming that Defendant has Deleted such Personal Information.

III. DEFAULT PRIVACY SETTINGS FOR CHILDREN AND TEENS

IT IS FURTHER ORDERED that, within thirty (30) days of the Compliance Date, Defendant, Defendant's officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this

Order, in connection with any Covered Product or Service, are permanently restrained and enjoined from disclosing a Child's or Teen's Covered Information to, enabling a Child or Teen to disclose their Covered Information to, or enabling a Child or Teen to converse with or be party to conversations between or among, any other user of the Covered Product or Service, unless:

- A. For a Child user, the Child's Parent has provided, and not withdrawn, their Affirmative Express Consent through an easily-located Privacy Setting; and
- B. For a Teen user, the Teen (or the Teen's Parent) has provided, and not withdrawn, their Affirmative Express Consent through an easily-located Privacy Setting.
- C. Each Clear and Conspicuous disclosure required pursuant to sub-Provisions III.A. and III.B. must identify: (1) each type of Covered Information that will be disclosed; (2) each category of Persons to which each type of Covered Information will be disclosed; (3) each type of communication the Child or Teen will be able to make or receive; and (4) each category of Persons to, or from which, the Child or Teen will be able to make, or receive, each type of communication.
- D. For the purposes of this Provision III:
 - 1. Any user of any Covered Product or Service that is a Website or Online Service Directed to Children must be deemed a Child, provided, however, that for any such Covered Product or Service that does not target Children as its primary audience, Defendant may collect age

information from users before collecting any other Covered Information and treat each user accordingly unless and until Defendant has actual knowledge that the user is a Child or Teen;

2. Any user of any Covered Product or Service that is not a Website or Online Service Directed to Children may be treated as neither a Child nor a Teen unless and until Defendant has actual knowledge that the user is a Child or Teen; and
3. To the extent that a display name of a Child or Teen is disclosed in a multiuser game or other interactive multiuser experience to identify participating users, such display name will not be considered Covered Information. Provided, however, Defendant must describe: (i) in a direct notice to parents, any such disclosure of a Child's display name; and (ii) in Defendant's privacy policy, any such disclosure of a Child's or Teen's display name.

IV. MANDATED PRIVACY PROGRAM

IT IS FURTHER ORDERED that each Covered Business, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must, within thirty (30) days of the Compliance Date, establish and implement, and thereafter maintain, a comprehensive privacy program (the "Privacy Program") that protects the privacy of such Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Privacy Program;
- B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or governing body, or if no such board or equivalent governing body exists, to a senior officer responsible for the Privacy Program at least once every twelve (12) months;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Privacy Program;
- D. Assess and document, at least once every twelve (12) months, internal and external risks to the privacy of Covered Information that could result in the unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information;
- E. Design, implement, maintain, and document safeguards that control for the material internal and external risks the Covered Business identifies to the privacy of Covered Information identified in response to sub-Provision IV.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information. Such safeguards must include:
 - 1. Policies, procedures, and technical measures to comply with COPPA and the COPPA Rule;

2. Policies, procedures, and technical measures to comply with Provision III;
 3. Regular COPPA Rule training on at least an annual basis for all employees and contractors providing services to the Covered Business whose responsibilities include any of the following: (a) access to Covered Information; (b) Covered Products or Services design, engineering, or implementation; or (c) Privacy Settings design, engineering, or implementation; and
 4. Regular privacy training programs for all employees and contractors providing services to the Covered Business, updated on at least an annual basis to address any identified material internal or external risks and safeguards implemented pursuant to this Order;
- F. Assess, at least once every twelve (12) months, the sufficiency of any safeguards in place to address the internal and external risks to the privacy of Covered Information, and modify the Privacy Program as needed based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months, and modify the Privacy Program as needed based on the results;
- H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from the Covered Business, and contractually require service providers to implement and maintain

safeguards sufficient to address the internal and external risks to the privacy of Covered Information; and

- I. Evaluate and adjust the Privacy Program in light of any changes to the Covered Business's operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in sub-Provision IV.D of this Order, or any other circumstances that the Covered Business knows or has reason to know may have an impact on the effectiveness of the Privacy Program or any of its individual safeguards. At a minimum, the Covered Business must evaluate the Privacy Program at least once every twelve (12) months and modify the Privacy Program as needed based on the results.

V. PRIVACY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with Provision IV of this Order titled Mandated Privacy Program, Defendant must obtain initial and biennial assessments ("Assessments"):

- A. The Assessment must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Privacy Program; (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. The

Assessor may not withhold any documents from the Commission on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

- B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in their sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the Privacy Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after the entry date of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire assessment period:
 - 1. Determine whether each Covered Business has implemented and maintained the Privacy Program required by Provision IV of this Order, titled Mandated Privacy Program;
 - 2. Assess the effectiveness of each Covered Business's implementation and maintenance of sub-Provisions IV.A-I;
 - 3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Privacy Program;

4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Privacy Program that were identified in any prior Assessment required by this Order; and
5. Identify specific evidence (including but not limited to documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of the Covered Business's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by a Covered Business's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Privacy Program and did not rely primarily on assertions or attestations by a Covered Business's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that a Covered Business adds, materially revises, or materially updates one or more safeguards required under Provision IV of this Order during an Assessment period, the Assessment must assess the effectiveness of the added, materially revised, or materially updated safeguard(s) for the time period in which it was in effect, and provide a

separate statement detailing the basis for each additional, materially revised, or materially updated safeguard.

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendant must submit an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure of the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “United States v. Epic Games, Inc., FTC File No. 2223087.” Defendant must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy suitable for public disclosure of each subsequent biennial Assessment until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words “DPIP Assessment” in red lettering.

**VI. COOPERATION WITH THIRD-PARTY
PRIVACY ASSESSOR**

IT IS FURTHER ORDERED that Defendant, whether acting directly or indirectly, in connection with any Assessment required by Provision V of this Order titled Privacy Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about each Covered Business's network(s), and all of each Covered Business's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's:
 - (1) determination of whether Defendant has implemented and maintained the Privacy Program required by Provision IV of this Order, titled Mandated Privacy Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions IV.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Privacy Program.

VII. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that, one year after the Compliance Date, and each year thereafter for ten (10) years after the Compliance Date:

- A. Defendant must provide the Commission with a certification from the Principal Executive Officer that: (1) Defendant has established, implemented, and maintained the requirements of this Order; and (2) Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the Principal Executive Officer or subject matter experts upon whom the Principal Executive Officer reasonably relies in making the certification.
- B. Defendant must provide the Commission with a certification from a senior officer of each Covered Business other than Defendant responsible for each such Covered Business's Privacy Program that: (1) each Covered Business other than Defendant has established, implemented, and maintained the requirements of this Order; and (2) each Covered Business other than Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

- C. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “United States v. Epic Games, Inc., FTC File No. 2223087.”

VIII. MONETARY JUDGMENT FOR CIVIL PENALTY

IT IS FURTHER ORDERED that:

- A. Judgment in the amount of two hundred seventy five million dollars (\$275,000,000) is entered in favor of Plaintiff against Defendant as a civil penalty.
- B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, two hundred seventy five million dollars (\$275,000,000), which, as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment to Plaintiff. Such payment must be made within seven (7) days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of Plaintiff.
- C. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

- D. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order.
- E. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security Numbers or Employer Identification Numbers), which Defendant must submit to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. §7701.

IX. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendant obtain acknowledgments of receipt of this Order:

- A. Defendant, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after entry of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibilities for conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all

others, delivery must occur before they assume their responsibilities.

- C. From each individual or entity to which Defendant delivered a copy of this Order, Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

X. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendant make timely submissions to the Commission:

- A. One (1) year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury:
 - 1. Defendant must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and Plaintiff may use to communicate with Defendant; (b) identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Defendant is in compliance with each provision of this Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.
- B. For ten (10) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within 14 days of any

change in the following:

1. Defendant must report any change in: (a) any designated point of contact; or (b) the structure of Defendant or any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Defendant within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission,

600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “United States v. Epic Games, Inc., FTC File No. 2223087.”

XI. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for ten (10) years after entry of the Order, and retain each such record for five (5) years.

Specifically, Defendant must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold in connection to any Covered Product or Service;
- B. Personnel records showing, for each Person providing services in connection to any Covered Product or Service, whether as an employee or otherwise, that Person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints and refund requests concerning the subject matter of the Order, whether received directly or through any domestic government regulatory authority; and
- D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant’s compliance with this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or Plaintiff, Defendant must: submit

additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission and Plaintiff are also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69, provided that Defendant, after attempting to resolve a dispute without court action and for good cause shown, may file a motion with this Court seeking an order for one or more of the protections set forth in Rule 26(c).

- B. For matters concerning this Order, the Commission and Plaintiff are authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission and Plaintiff to interview any employee or other Person affiliated with Defendant who has agreed to such an interview. The Person interviewed may have counsel present.
- C. The Commission and Plaintiff may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this ___ day of _____, 202__.

UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

FOR PLAINTIFF:

THE UNITED STATES OF AMERICA

BRIAN M. BOYNTON

Principal Deputy Assistant Attorney General, Civil Division

ARUN G. RAO

Deputy Assistant Attorney General

AMANDA N. LISKAMM

Acting Director, Consumer Protection Branch

LISA K. HSIAO

Assistant Director, Consumer Protection Branch



Date: 12/16/22

Michael J. Wadden

Joshua A. Fowkes

Trial Attorneys

Consumer Protection Branch

Civil Division

U.S. Department of Justice

450 5th Street, NW

Washington, DC 20530

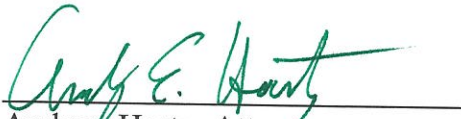
(202) 305-7133

michael.j.wadden@usdoj.gov

FOR THE FEDERAL TRADE COMMISSION

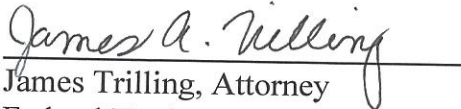
Benjamin Wiseman
Acting Associate Director
Division of Privacy and Identity Protection

Mark Eichorn
Assistant Director
Division of Privacy and Identity Protection



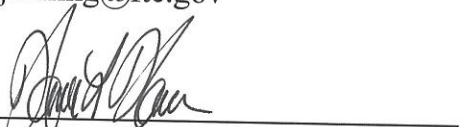
Andrew Hasty, Attorney
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2861
ahasty@ftc.gov

Date: 12/15/2022



James Trilling, Attorney
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-3497
jtrilling@ftc.gov

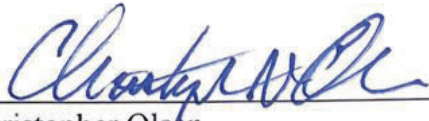
Date: 12/15/2022



Amanda Koulousias, Attorney
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-3334
akoulousias@ftc.gov

Date: 12/15/22

FOR DEFENDANT:



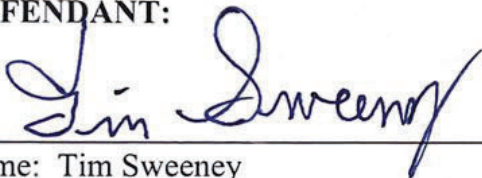
Date: 12/6/22

Christopher Olsen
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW
Washington, DC 20006
(202) 973-8803
colsen@wsgr.com

Libby Weingarten
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW
Washington, DC 20006
(202) 973-8861
lweingarten@wsgr.com

Counsel for Epic Games, Inc.,

DEFENDANT:



Date: 12-2-2022

Name: Tim Sweeney
Title: Chief Executive Officer
Epic Games, Inc.

Appendix A

average firm-wide billing rate (partners and associates) in 2011 was \$403, the average partner rate was \$482, and the average associate rate was \$303.

The Commission believes it reasonable to assume that the workload among law firm partners and associates for COPPA compliance questions could be competently addressed and efficiently distributed among attorneys at varying levels of seniority, but would be weighted most heavily to more junior attorneys. Thus, assuming an apportionment of two-thirds of such work is done by associates, and one-third by partners, a weighted average tied to the average firm-wide associate and average firm-wide partner rates, respectively, in the *National Law Journal* 2011 survey would be about \$365 per hour. The Commission believes that this rate B which is very near the mean of TIA's stated range of purported hourly rates that its members typically pay to engage counsel for COPPA compliance questions B is an appropriate measure to calculate the cost of legal assistance for operators to comply with the final Rule amendments.³⁹⁶

TIA also states that the 2012 SNPRM estimate of \$42 per hour for technical support is too low, and that engaging expert technical personnel can, on average, involve hourly costs that range from \$72 to \$108.³⁹⁷ Similar to TIA's hours estimate, discussed above, the Commission believes that TIA's estimate may have been based on implementing requirements that, ultimately, the Commission has determined not to adopt. For example, technical personnel will not need to "ensure" the security procedures of third parties; operators that have been eligible to use email plus for parental consents will not be required to implement new systems to replace it. It is unclear whether TIA's estimate for technical support is based on the types of disclosure-related tasks that the final Rule amendments would actually require, other tasks that the final Rule amendments would not require, or non-disclosure tasks not covered by the PRA. Moreover, unlike its estimate for lawyer assistance, TIA's

³⁹⁶ Cf. Civil Division of the United States Attorney's Office for the District of Columbia, United States Attorney's Office, District of Columbia, Laffey Matrix B 2003-2013, available at http://www.justice.gov/usao/dc/divisions/Laffey_Matrix_2003-2013.pdf (updated "Laffey Matrix" for calculating "reasonable" attorneys fees in suits in which fee shifting is authorized can be evidence of prevailing market rates for litigation counsel in the Washington, DC area; rates in table range from \$245 per hour for most junior associates to \$505 per hour for most senior partners).

³⁹⁷ Toy Industry Association (comment 89, 2012 SNPRM), at 18.

estimates for technical labor are not accompanied by an adequate explanation of why estimates for technical support drawn from BLS statistics are not an appropriate basis for the FTC's PRA analysis. Accordingly, the Commission believes it is reasonable to retain the 2012 SNPRM estimate of \$42 per hour for technical assistance based on BLS data.

Thus, for the 180 new operators per year not previously accounted for under the FTC's currently cleared estimates, 10,800 cumulative disclosure hours would be composed of 9,000 hours of legal assistance and 1,800 hours of technical support. Applied to hourly rates of \$365 and \$42, respectively, associated labor costs for the 180 new operators potentially subject to the proposed amendments would be \$3,360,600 (*i.e.*, \$3,285,000 for legal support plus \$75,600 for technical support).

Similarly, for the estimated 2,910 existing operators covered by the final Rule amendments, 58,200 cumulative disclosure hours would consist of 48,500 hours of legal assistance and 9,700 hours for technical support. Applied at hourly rates of \$365 and \$42, respectively, associated labor costs would total \$18,109,900 (*i.e.*, \$17,702,500 for legal support plus \$407,400 for technical support). Cumulatively, estimated labor costs for new and existing operators subject to the final Rule amendments is \$21,470,500.

(2) Reporting

The Commission staff assumes that the tasks to prepare augmented safe harbor program applications occasioned by the final Rule amendments will be performed primarily by lawyers, at a mean labor rate of \$180 an hour.³⁹⁸ Thus, applied to an assumed industry total of 120 hours per year for this task, incremental associated yearly labor costs would total \$21,600.

³⁹⁸ Based on Commission staff's experience with previously approved safe harbor programs, staff anticipates that most of the legal tasks associated with safe harbor programs will be performed by in-house counsel. Cf. Toy Industry Association (comment 89, 2012 SNPRM), at 19 (regional BLS statistics for lawyer wages can support estimates of the level of in-house legal support likely to be required on an ongoing basis). Moreover, no comments were received in response to the February 9, 2011 and May 31, 2011 **Federal Register** notices (76 FR at 7211 and 76 FR at 31334, respectively, available at <http://www.gpo.gov/fdsys/pkg/FR-2011-02-09/pdf/2011-2904.pdf> and <http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13357.pdf>), which assumed a labor rate of \$150 per hour for lawyers or similar professionals to prepare and submit a new safe harbor application. Nor was that challenged in the comments responding to the 2011 NPRM.

The Commission staff assumes periodic reports will be prepared by compliance officers, at a labor rate of \$28 per hour.³⁹⁹ Applied to an assumed industry total of 600 hours per year for this task, associated yearly labor costs would be \$16,800.

Cumulatively, labor costs for the above-noted reporting requirements total approximately \$38,400 per year.

G. Non-Labor/Capital Costs

Because both operators and safe harbor programs will already be equipped with the computer equipment and software necessary to comply with the Rule's new notice requirements, the final Rule amendments should not impose any additional capital or other non-labor costs.⁴⁰⁰

List of Subjects in 16 CFR Part 312

Children, Communications, Consumer protection, Electronic mail, Email, Internet, Online service, Privacy, Record retention, Safety, science and technology, Trade practices, Web site, Youth.

■ Accordingly, for the reasons stated above, the Federal Trade Commission revises part 312 of Title 16 of the Code of Federal Regulations to read as follows:

PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE

Sec.

- 312.1 Scope of regulations in this part.
- 312.2 Definitions.
- 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.
- 312.4 Notice.
- 312.5 Parental consent.
- 312.6 Right of parent to review personal information provided by a child.
- 312.7 Prohibition against conditioning a child's participation on collection of personal information.

³⁹⁹ See Bureau of Labor Statistics National Compensation Survey: Occupational Earnings in the United States, 2010, at Table 3, available at <http://www.bls.gov/ncs/ocs/sp/nctb1477.pdf>. This rate has not been contested.

⁴⁰⁰ NCTA commented that the Commission failed to consider costs "related to redeveloping child-directed Web sites" that operators would be "forced" to incur as a result of the proposed Rule amendments, including for "new equipment and software required by the expanded regulatory regime." NCTA (comment 113, 2011 NPRM), at 23. Similarly, TIA commented that the proposed Rule amendments would entail "increased monetary costs with respect to technology acquisition and implementation * * *." Toy Industry Association (comment 163, 2011 NPRM), at 17. These comments, however, do not specify projected costs or which Rule amendments would entail the asserted costs.

312.8 Confidentiality, security, and integrity of personal information collected from children.

312.9 Enforcement.

312.10 Data retention and deletion requirements.

312.11 Safe harbor programs.

312.12 Voluntary Commission Approval Processes.

312.13 Severability.

Authority: 15 U.S.C. 6501–6508.

§ 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, *et seq.*) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(1) Requesting, prompting, or encouraging a child to submit personal information online;

(2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(3) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(1) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and

(2) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(1) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(2) Authorizes any collection, use, and/or disclosure of the personal information.

Online contact information means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

Operator means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). Personal information is *collected or maintained on behalf of* an operator when:

(1) It is collected or maintained by an agent or service provider of the operator; or

(2) The operator benefits by allowing another person to collect personal information directly from users of such Web site or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(1) A first and last name;

(2) A home or other physical address including street name and name of a city or town;

(3) Online contact information as defined in this section;

(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(5) A telephone number;

(6) A Social Security number;

(7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;

(8) A photograph, video, or audio file where such file contains a child's image or voice;

(9) Geolocation information sufficient to identify street name and name of a city or town; or

(10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the Web site or online service means:

(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the Web site or online service;

(ii) Perform network communications;

(iii) Authenticate users of, or personalize the content on, the Web site or online service;

(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, Web site, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4);

(2) So long as The information collected for the activities listed in paragraphs (1)(i)–(vii) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a

profile on a specific individual, or for any other purpose.

Third party means any person who is not:

(1) An operator with respect to the collection or maintenance of personal information on the Web site or online service; or

(2) A person who provides support for the internal operations of the Web site or online service and who does not use or disclose information protected under this part for any other purpose.

Web site or online service directed to children means a commercial Web site or online service, or portion thereof, that is targeted to children.

(1) In determining whether a Web site or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

(2) A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children.

(3) A Web site or online service that is directed to children under the criteria set forth in paragraph (1) of this definition, but that does not target children as its primary audience, shall not be deemed directed to children if it:

(i) Does not collect personal information from any visitor prior to collecting age information; and

(ii) Prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(4) A Web site or online service shall not be deemed directed to children solely because it refers or links to a commercial Web site or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) *General principles of notice.* It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) *Direct notice to the parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) *Content of the direct notice to the parent—*(1) *Content of the direct notice to the parent under § 312.5(c)(1) (Notice*

to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information). This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section;

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) *Content of the direct notice to the parent under § 312.5(c)(2) (Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* Where an operator chooses to notify a parent of a child's participation in a Web site or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information;

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the child's participation in the Web site or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and

(iv) A hyperlink to the operator's online notice of its information

practices required under paragraph (d) of this section.

(3) *Content of the direct notice to the parent under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times)*. This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and

(vi) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety)*. This direct notice shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(d) *Notice on the Web site or online service*. In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, and, at each area of the Web site or online service

where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the Web site or online service. *Provided that:* The operators of a Web site or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the Web site or online service are also listed in the notice;

(2) 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; and

(3) That the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

§ 312.5 Parental consent.

(a) *General requirements*. (1) 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.

(2) 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.

(b) *Methods for verifiable parental consent*. (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated,

in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi) *Provided that*, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

(3) *Safe harbor approval of parental consent methods*. A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.

(c) *Exceptions to prior parental consent*. Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in this paragraph:

(1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the

operator must delete such information from its records;

(2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the purpose of collecting a child's name and online contact information is to:

(i) Protect the security or integrity of its Web site or online service;

(ii) Take precautions against liability;

(iii) Respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not be used for any other purpose;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or

(8) Where an operator covered under paragraph (2) of the definition of *Web site or online service directed to children* in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a Web site or online service, the operator of that Web site or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

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.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Data retention and deletion requirements.

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. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

§ 312.11 Safe harbor programs.

(a) *In general.* Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) *Criteria for approval of self-regulatory program guidelines.* Proposed safe harbor programs must demonstrate

that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines (“subject operators”) provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators’ compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator’s information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators’ non-compliance with self-regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self-regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or

(v) Any other equally effective action.

(c) *Request for Commission approval of self-regulatory program guidelines.* A proposed safe harbor program’s request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant’s business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators’ fitness for membership in the safe harbor program;

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and

(4) A statement explaining:

(i) How the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and

(ii) How the assessment mechanisms and compliance consequences required

under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) *Reporting and recordkeeping requirements.* Approved safe harbor programs shall:

(1) By July 1, 2014, and annually thereafter, submit a report to the Commission containing, at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section, a description of any disciplinary action taken against any subject operator under paragraph (b)(3) of this section, and a description of any approvals of member operators’ use of a parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators’ compliance required under paragraph (b)(2) of this section.

(e) *Post-approval modifications to self-regulatory program guidelines.* Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2) of this section. The statement required under paragraph (c)(4) of this section must describe how the proposed changes affect existing provisions of the guidelines.

(f) *Revocation of approval of self-regulatory program guidelines.* The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, by March 1, 2013, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

(g) *Operators’ participation in a safe harbor program.* An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or

bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator’s participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator’s non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

§ 312.12 Voluntary Commission Approval Processes.

(a) *Parental consent methods.* An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in § 312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1). The request shall be filed with the Commission’s Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request; and

(b) *Support for internal operations of the Web site or online service.* An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for internal operations. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for internal operations, and an analysis of their potential effects on children’s online privacy. The request shall be filed with the Commission’s Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request.

§ 312.13 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission’s intention that the remaining provisions shall continue in effect.

By direction of the Commission, Commissioner Rosch abstaining, and Commissioner Ohlhausen dissenting.

Donald S. Clark,
Secretary.

Dissenting Statement of Commissioner Maureen K. Ohlhausen

I voted against adopting the amendments to the Children's Online Privacy Protection Act (COPPA) Rule because I believe a core provision of the amendments exceeds the scope of the authority granted us by Congress in COPPA, the statute that underlies and authorizes the Rule.⁴⁰¹ Before I explain my concerns, I wish to commend the Commission staff for their careful consideration of the multitude of issues raised by the numerous comments in this proceeding. Much of the language of the amendments is designed to preserve flexibility for the industry while striving to protect children's privacy, a goal I support strongly. The final proposed amendments largely strike the right balance between protecting children's privacy online and avoiding undue burdens on providers of children's online content and services. The staff's great expertise in the area of children's privacy and deep understanding of the values at stake in this matter have been invaluable in my consideration of these important issues.

In COPPA Congress defined who is an operator and thereby set the outer boundary for the statute's and the COPPA Rule's reach.⁴⁰² It is undisputed that COPPA places obligations on operators of Web sites or online services directed to children or operators with actual knowledge that they are collecting personal information from

children. The statute provides, "It is unlawful for an operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed [by the FTC]." ⁴⁰³

The Statement of Basis and Purpose for the amendments (SBP) discusses concerns that the current COPPA Rule may not cover child-directed Web sites or services that do not themselves collect children's personal information but may incorporate third-party plug-ins that collect such information ⁴⁰⁴ for the plug-ins' use but do not collect or maintain the information for, or share it with, the child-directed site or service. To address these concerns, the amendments add a new proviso to the definition of operator in the COPPA Rule: "Personal information is collected or maintained on behalf of an operator when: (a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such Web site or online service." ⁴⁰⁵

The proposed amendments construe the term "on whose behalf such information is collected and maintained" to reach child-directed Web sites or services that merely derive from a third-party plug-in some kind of benefit, which may well be unrelated to the collection and use of children's

⁴⁰³ 15 U.S.C. 6502(a)(1).

⁴⁰⁴ If the third-party plug-ins are child-directed or have actual knowledge that they are collecting children's personal information they are already expressly covered by the COPPA statute. Thus, as the SBP notes, a behavioral advertising network that targets children under the age of 13 is already deemed an operator. The amendment must therefore be aimed at reaching third-party plug-ins that are either not child-directed or do not have actual knowledge that they are collecting children's personal information, which raises a question about what harm this amendment will address. For example, it appears that this same type of harm could occur through general audience Web sites and online services collecting and using visitors' personal information without knowing whether some of the data is children's personal information, which is a practice that COPPA and the amendments do not prohibit.

⁴⁰⁵ 16 CFR 312.2 (Definitions).

information (e.g., content, functionality, or advertising revenue). I find that this proviso—which would extend COPPA obligations to entities that do not collect personal information from children or have access to or control of such information collected by a third-party does not comport with the plain meaning of the statutory definition of an operator in COPPA, which covers only entities "on whose behalf such information is collected and maintained." ⁴⁰⁶ In other words, I do not believe that the fact that a child-directed site or online service receives any kind of benefit from using a plug-in is equivalent to the collection of personal information by the third-party plug-in on behalf of the child-directed site or online service.

As the Supreme Court has directed, an agency "must give effect to the unambiguously expressed intent of Congress." ⁴⁰⁷ Thus, regardless of the policy justifications offered, I cannot support expanding the definition of the term "operator" beyond the statutory parameters set by Congress in COPPA.

I therefore respectfully dissent.

[FR Doc. 2012–31341 Filed 1–16–13; 8:45 am]

BILLING CODE 6750-01-P

⁴⁰⁶ This expanded definition of operator reverses the Commission's previous conclusion that the appropriate test for determining an entity's status as an operator is to "look at the entity's relationship to the data collected," using factors such as "who owns and/or controls the information, who pays for its collection and maintenance, the pre-existing contractual relationships regarding collection and maintenance of the information, and the role of the Web site or online service in collecting and/or maintaining the information (i.e., whether the site participates in collection or is merely a conduit through which the information flows to another entity.)" Children's Online Privacy Protection Rule 64 FR 59888, 59893, 59891 (Nov. 3, 1999) (final rule).

⁴⁰⁷ *Chevron v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842–43 (1984) ("When a court reviews an agency's construction of the statute which it administers, it is confronted with two questions. First, always, is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress.")

⁴⁰¹ 15 U.S.C. 6501–6506.

⁴⁰² COPPA, 15 U.S.C. 6501(2), defines the term "operator" as "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about users of or visitors to such Web site or online service, or on whose behalf such information is collected and maintained * * *" As stated in the Statement of Basis and Purpose for the original COPPA Rule, "The definition of 'operator' is of central importance because it determines who is covered by the Act and the Rule." Children's Online Privacy Protection Rule 64 FR 59888, 59891 (Nov. 3, 1999) (final rule).