

1 ROB BONTA
Attorney General of California
2 ANYA M. BINSACCA, SBN 189613
Supervising Deputy Attorney General
3 NICOLE KAU, SBN 292026
ELIZABETH K. WATSON, SBN 295221
4 Deputy Attorneys General
455 Golden Gate Avenue, Suite 11000
5 San Francisco, CA 94102-7004
Telephone: (415) 510-3847
6 E-mail: Elizabeth.Watson@doj.ca.gov
Attorneys for Defendant
7

8 IN THE UNITED STATES DISTRICT COURT
9 FOR THE NORTHERN DISTRICT OF CALIFORNIA
10 SAN JOSE DIVISION
11

12 **NETCHOICE, LLC d/b/a NetChoice,**
13

14 Plaintiff,

15 v.

16 **ROB BONTA, ATTORNEY GENERAL OF**
17 **THE STATE OF CALIFORNIA, in his**
official capacity,

18 Defendant.
19
20
21
22
23
24
25
26
27
28

Case No. 5:22-cv-08861-BLF

**DEFENDANT'S OPPOSITION TO
PLAINTIFF'S MOTION FOR
PRELIMINARY INJUNCTION**

Judge: Hon. Beth Labson Freeman
Hearing Date: July 27, 2023
Time: 1:30 PM
Dept: Courtroom 1– 5th Floor

Action Filed: December 14, 2022

TABLE OF CONTENTS

	Page
Introduction	1
Background	1
I. Existing Practices & Regulation.....	1
A. Online Businesses’ Collection and Use of Personal Information.....	1
B. User Tools for Limiting Collection and Use of Personal Information	2
II. Children on the Internet	3
A. Children’s Internet Use	3
B. Laws Regulating Children’s Online Experience	4
C. Businesses’ Interaction with Children Online	4
D. Unique Vulnerabilities of Children Online	5
III. The California Age-Appropriate Design Code Act.....	6
A. Regulated Businesses	6
B. Requirements for Regulated Businesses	7
1. Proactive Steps to Protect Children’s Privacy	7
2. Prohibitions	8
C. Enforcement & Guidance	9
IV. Plaintiff’s Challenge to AB 2273	10
Legal Standard.....	10
Argument	10
I. Plaintiff is not Likely to Succeed on the Merits.....	10
A. AB 2273 Does Not Violate the First Amendment	10
1. AB 2273 does not regulate speech or expressive conduct.....	10
2. None of the challenged provisions impose a prior restraint	12
3. AB 2273 is facially neutral	16
4. AB 2273 withstands any level of First Amendment scrutiny	18
a. At most, intermediate scrutiny applies.....	18
b. AB 2273 withstands strict scrutiny	19
5. AB 2273 is not overbroad.....	22
B. AB 2273 Is Not Unconstitutionally Vague	23
C. AB 2273 Does Not Violate the Dormant Commerce Clause	25
1. AB 2273 does not regulate extraterritorially.....	25
2. AB 2273 satisfies Pike balancing.....	26
D. AB 2273 Is Not Preempted by Federal Law	27

TABLE OF CONTENTS

(continued)

	Page
1. COPPA.....	27
2. Section 230 of the Communications Decency Act.....	29
II. Other Injunction Factors Weigh Against Relief.....	30
Conclusion.....	30

TABLE OF AUTHORITIES

Page**CASES**

<i>Alliance for Wild Rockies v. Cottrell</i> 632 F.3d 1127 (9th Cir. 2011).....	10
<i>Am. Acad. of Pain Mgmt. v. Joseph</i> 353 F.3d 1099 (9th Cir. 2004).....	19
<i>Am. Soc’y of Journalists & Authors v. Bonta</i> 15 F.4th 954 (9th Cir. 2021).....	11, 12, 15
<i>Anheuser-Busch, Inc. v. Schmoke</i> 101 F.3d 3250 (4th Cir. 1996).....	20
<i>Arizona v. United States</i> 567 U.S. 387 (2012).....	29
<i>Bantam Books v. Sullivan</i> 372 U.S. 58 (1963).....	13, 14
<i>Barnes v. Yahoo, Inc.</i> 570 F.3d 1096 (9th Cir. 2009).....	14, 29
<i>Bolger v. Youngs Drug Prods. Corp.</i> 463 U.S. 60 (1983).....	19
<i>Broadrick v. Oklahoma</i> 413 U.S. 601 (1973).....	22
<i>Butler v. Michigan</i> 352 U.S. 380 (1957).....	16
<i>Cal. Teachers Ass’n v. State Bd. of Educ.</i> 271 F.3d 1141 (9th Cir. 2001).....	23, 24, 25
<i>Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y.</i> 447 U.S. 557 (1980).....	15, 19
<i>Colacurcio v. City of Kent</i> 163 F.3d 545 (9th Cir. 1998).....	21
<i>Coyote Publ’g v. Miller</i> 598 F.3d 592 (9th Cir. 2010).....	19, 20
<i>Denver Area Telecomm. Consortium, Inc., v. FCC</i> 518 U.S. 727 (1996).....	12, 20

TABLE OF AUTHORITIES
(continued)

	<u>Page</u>
<i>Doe v. Harris</i> 772 F.3d 563 (9th Cir. 2014).....	17, 18
<i>Doe v. Internet Brands, Inc.</i> 824 F.3d 846 (9th Cir. 2016).....	29
<i>Dymo Indus., Inc. v. Tapeprinter, Inc.</i> 326 F.2d 141 (9th Cir. 1964) (per curiam)	10
<i>Edenfield v. Fane</i> 507 U.S. 761 (1993).....	19
<i>Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC</i> 521 F.3d 1157 (9th Cir. 2008).....	29, 30
<i>Ferris v. Santa Clara County</i> 891 F.2d 715 (9th Cir. 1989).....	20, 30
<i>Fla. Bar v. Went For It, Inc.</i> 515 U.S. 618 (1995).....	20
<i>G.K. Ltd. Travel v. City of Lake Oswego</i> 436 F.3d 1064 (9th Cir. 2006).....	21
<i>Ginsberg v. New York</i> 390 U.S. 629 (1968).....	21
<i>Goldie’s Bookstore, Inc. v. Sup. Ct. of Cal.</i> 739 F.2d 466 (9th Cir. 1984).....	30
<i>Gospel Missions of Am. v. City of Los Angeles</i> 419 F.3d 1042 (9th Cir. 2005).....	22, 23
<i>Greater L.A. Agency on Deafness, Inc. v. Cable News Network, Inc.</i> 742 F.3d 414 (9th Cir. 2014).....	13, 16, 26, 27
<i>Holder v. Humanitarian Law Project</i> 561 U.S. 1.....	25
<i>HomeAway.com v. City of Santa Monica</i> 918 F.3d 676 (9th Cir. 2019).....	11, 12, 29
<i>Hotel Emps. & Rest. Emps. Int’l Union v. Nev. Gaming Comm’n</i> 984 F.2d 1507 (9th Cir. 1993).....	13

TABLE OF AUTHORITIES
(continued)

		<u>Page</u>
1		
2		
3	<i>Humanitarian Law Project v. U.S. Treasury Dep't</i>	
4	578 F.3d 1133 (9th Cir. 2009)	23
5	<i>Hunt v. City of Los Angeles</i>	
6	638 F.3d 703 (2011)	15, 24
7	<i>IDK v. Clark County</i>	
8	836 F.2d 1185 (9th Cir. 1988)	14, 23, 24
9	<i>In re Nat'l Sec. Letter</i>	
10	33 F.4th 1058 (9th Cir. 2022)	19, 22
11	<i>In re Three Nat'l Security Letters</i>	
12	35 F.4th 1181 (9th Cir. 2022)	21
13	<i>Int'l Franchise Ass'n v. City of Seattle</i>	
14	803 F.3d 389 (9th Cir. 2015)	11, 12
15	<i>Interstate Cir., Inc. v. City of Dallas</i>	
16	390 U.S. 676 (1968)	14
17	<i>Jacobs v. Clark County Sch. Dist.</i>	
18	526 F.3d 419 (9th Cir. 2008)	18, 19
19	<i>Jones v. Google LLC</i>	
20	56 F.4th 735 (9th Cir. 2022)	27, 28, 29
21	<i>Litton Indus. Inc. v. FTC</i>	
22	676 F.2d 364 (9th Cir. 1982)	15
23	<i>Lone Star Sec. & Video, Inc. v. City of Los Angeles</i>	
24	827 F.3d 1192 (9th Cir. 2016)	16
25	<i>Long Beach Area Peace Network v. City of Long Beach</i>	
26	574 F.3d 1011 (9th Cir. 2009)	13
27	<i>Marquez-Reyes v. Garland</i>	
28	36 F.4th 1195 (9th Cir. 2022)	15, 22, 23
	<i>Maryland v. King</i>	
	567 U.S. 1301 (2012) (Roberts, C.J., in chambers)	30
	<i>Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue</i>	
	460 U.S. 575 (1983)	11

TABLE OF AUTHORITIES
(continued)

		<u>Page</u>
1		
2		
3	<i>Murphy v. NCAA</i>	
4	138 S. Ct. 1461 (2018).....	27
5	<i>Nat’l Endowment for the Arts v. Finley</i>	
6	524 U.S. 569 (1998).....	12
7	<i>Nat’l Fed’n of the Blind v. Target Corp.</i>	
8	452 F. Supp. 2d 946 (N.D. Cal. 2006)	26
9	<i>New Energy Co. of Ind. v. Limbach</i>	
10	486 U.S. 269 (1988).....	25
11	<i>New York v. Ferber</i>	
12	458 U.S. 747 (1982).....	27
13	<i>Nken v. Holder</i>	
14	556 U.S. 418 (2009).....	30
15	<i>Perry v. L.A. Police Dept.</i>	
16	121 F.3d 1365 (9th Cir. 1997).....	18
17	<i>Pharm. Rsch. & Mfrs. of Am. v. Walsh</i>	
18	538 U.S. 644 (2003).....	25
19	<i>Pike v. Bruce Church, Inc.</i>	
20	397 U.S. 137 (1970).....	26, 27
21	<i>Prince v. Massachusetts</i>	
22	321 U.S. 158 (1944).....	21
23	<i>Publius v. Boyer-Vine</i>	
24	237 F. Supp. 3d 997 (E.D. Cal. 2017).....	26
25	<i>Recycle for Change v. City of Oakland</i>	
26	856 F.3d 666 (9th Cir. 2017).....	18
27	<i>Reno v. ACLU</i>	
28	521 U.S. 844 (1997).....	21
	<i>Roulette v. City of Seattle</i>	
	97 F.3d 300 (9th Cir. 1996).....	11
	<i>Rumsfeld v. Forum for Acad. & Institutional Rts., Inc. (FAIR)</i>	
	547 U.S. 476 (2006).....	12, 18

TABLE OF AUTHORITIES
(continued)

		<u>Page</u>
1		
2		
3	<i>Sable Commc'ns of Cal., Inc. v. F.C.C.</i>	
4	492 U.S. 115 (1989).....	20
5	<i>Se. Promotions, Ltd v. Conrad</i>	
6	420 U.S. 546 (1975).....	13
7	<i>Sorrell v. IMS Health Inc.</i>	
8	564 U.S. 552 (2011).....	11, 12
9	<i>Spirit of Aloha Temple v. Cnty. of Maui</i>	
10	49 F.4th 1180 (9th Cir. 2022).....	13
11	<i>Thomas v. Chi. Park Dist.</i>	
12	534 U.S. 316 (2002).....	14
13	<i>Turner Broad. Sys., Inc. v. FCC</i>	
14	512 U.S. 622 (1994).....	12, 17, 18, 19
15	<i>Twitter Inc. v. Garland</i>	
16	61 F.4th 686 (9th Cir. 2023).....	17, 21, 22
17	<i>U.S. v. O'Brien</i>	
18	391 U.S. 367 (1968).....	19
19	<i>U.S. v. Playboy Ent. Grp., Inc.</i>	
20	529 U.S. 803 (2000).....	20, 21
21	<i>U.S. v. Williams</i>	
22	553 U.S. 285 (2008).....	22, 23
23	<i>United Haulers Ass'n v. Oneida-Herkimer Solid Waste Mgmt. Auth.</i>	
24	550 U.S. 330 (2007).....	25
25	<i>Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.</i>	
26	455 U.S. 489 (1982).....	23
27	<i>Village of Schaumburg v. Citizens for a Better Env't</i>	
28	444 U.S. 620 (1980).....	13
	<i>Virginia v. Hicks</i>	
	539 U.S. 113 (2003).....	22
	<i>Willams v. Gerber Prods., Co.</i>	
	552 F.3d 934 (9th Cir. 2008).....	14

TABLE OF AUTHORITIES
(continued)

	<u>Page</u>
<i>Williams-Yulee v. Fla. Bar</i> 575 U.S. 433 (2015).....	20
<i>Winter v. Nat. Res. Def. Council, Inc.</i> 555 U.S. 7 (2008).....	10, 30
 STATUTES	
United States Code, Title 12 § 5365(i)(2).....	13
United States Code, Title 15 §§ 6501–6506	4, 28
§ 6502(d)	28
United States Code, Title 26 § 501(r)(3)	13
United States Code, Title 47 § 230.....	14, 29, 30
§ 230(c)(1).....	29
§ 230 (e)(3).....	29
California Business & Professions Code § 17500.....	15
§ 22575.....	14
§ 22580.....	4
§ 22581.....	4

TABLE OF AUTHORITIES
(continued)

		<u>Page</u>
3	California Civil Code	
4	§ 1798.99.29	6
5	§ 1798.99.29(b)	17
6	§ 1798.99.30(a)	6, 26
7	§ 1798.99.30(b)(1)	26
8	§ 1798.99.30(b)(4)	6, 7
9	§ 1798.99.30(j)	26
10	§ 1798.99.31	30
11	§ 1798.99.31(a)	6, 26
12	§ 1798.99.31(a)(1)–(4)	13
13	§ 1798.99.31(a)(1)(A)–(B)	7, 8
14	§ 1798.99.31(a)(1)(B)	14
15	§ 1798.99.31(a)(3)–(4)	13
16	§ 1798.99.31(a)(5)	15, 16
17	§ 1798.99.31(a)(9)	14
18	§ 1798.99.31(b)	6
19	§ 1798.99.31(b)(1)	8, 16, 24, 28
20	§ 1798.99.31(b)(4)	9
21	§ 1798.99.31(b)(7)	24
22	§ 1798.99.31(b)(8)	9, 16
23	§ 1798.99.31(d)	9
24	§ 1798.99.32	9
25	§ 1798.99.32(d)	25
26	§ 1798.99.32(d)(3)	16
27	§ 1798.99.32(e)	16
28	§ 1798.99.33	9
	§ 1798.99.35	25
	§ 1798.99.35(a)	9
	§ 1798.99.35(c)	14
	§ 1798.99.35(e)	10
	§ 1798.99.40	7
	§ 1798.100	2
	§ 1798.120(a)	2
	§ 1798.120(c)	4
	§ 1798.140(i)	26
	§ 1798.140(v)	2
	§ 1798.140(b)(4)	24
	§ 1798.140(d)	6, 26
	§ 1798.140(l)	9, 24
	§ 1798.145	8

TABLE OF AUTHORITIES

(continued)

Page**CONSTITUTIONAL PROVISIONS**

United States Constitution

First Amendment *passim*

Fourth Amendment 10

Fourteenth Amendment..... 10

United States Constitution Article I

§ 8, Clause 3 25

OTHER AUTHORITIES

Code of Federal Regulations, Rule 16

§§ 312.1–312.13 28

§ 312.2..... 4

INTRODUCTION

The California Age-Appropriate Design Code Act allows children to explore the internet while reducing threats to their privacy and safety. The Act operates well within constitutional parameters. The regulation of businesses—including online businesses—and protection of children are well-recognized government responsibilities. The Act, which regulates those businesses that trade in consumers’ personal information and offer products, services, and features likely to be accessed by children, requires certain actions that proactively protect that information and prohibits certain actions that involve the collection and use of that information. Plaintiff’s members do not have a First Amendment right to children’s personal information. Nothing in the Act restricts the content that businesses can provide to minors, and any incidental effect the Act may have on businesses’ speech is justified by the State’s compelling interest in children’s welfare. The Act’s clear and specific requirements and prohibitions, as well as its procedural protections and scienter requirements, ensure that businesses’ rights remain protected. Compliance does not trigger concerns under the dormant Commerce Clause. Nor is the Act inconsistent with existing federal law. This Court should deny Plaintiff’s motion.

BACKGROUND

I. EXISTING PRACTICES & REGULATION

A. Online Businesses’ Collection and Use of Personal Information

The collection, sharing, selling, and other use of personal information provides substantial revenue for online businesses. Egelman Decl. ¶¶ 11–12. Internet companies constantly collect data from individuals online and offline. *Id.* ¶ 13. This data includes what services people use, how they use them, and from where they use them. Businesses are able to link this data to unique individuals through persistent identifiers, like the device an individual uses to access the internet, which tend not to change over time. *Id.* ¶ 14. Once data is linked to unique individuals, businesses are able to create thorough individual profiles using information drawn directly from the collected data, and to make predictions and inferences based on that data. *Id.* ¶¶ 13–14. With this data, businesses can learn, predict, or infer things like user’s interests, preferences, and behaviors as well as more personal details such as religion, health conditions, sexual orientation, or

socioeconomic status. *Id.* Highly personal individual information can be predicted or inferred from minimal data. *Id.* Geolocation information is a highly valuable piece of data that is widely available through databases that map Internet Protocol (IP) addresses—which are transmitted with every internet connection—to physical locations. *Id.* ¶¶ 13, 31, 55. From this information alone, a business may be able to accurately predict details about a user’s religion or sexual orientation. *Id.* ¶¶ 13–14. Once a business has compiled a profile, those profiles can be used or sold to third parties to create targeted advertising and learn more about consumer behavior to maximize profit, among other things. *Id.* ¶¶ 11–14; Radesky Decl. ¶¶ 66, 68, 78, 89.

Because this mass collection of data raises significant privacy concerns, California regulates the collection and use of consumer data. Existing statutes cover consumer’s “personal information,” which is defined as information that “identifies, relates to, describes,” or is reasonably capable of association with, or linking to, a particular consumer or household. Cal. Civ. Code §1798.140(v) (all statutory references are to the Cal. Civ. Code unless otherwise noted). Personal information includes names, addresses, email addresses, IP addresses, commercial information, browsing history, search history, geolocation data, and information regarding a consumer’s interaction with an internet website. *Id.* It also includes profiles or inferences made from this information. *Id.* Businesses must notify consumers that their data is being collected and consumers have the right to direct businesses not to sell or share that information. §1798.100; §1798.120(a). In short, California law intends to empower its residents to control their data. However, practically speaking, businesses do not always provide internet users with the necessary tools to do so. Egelman Decl. ¶¶ 24–34.

B. User Tools for Limiting Collection and Use of Personal Information

Privacy Settings: Privacy settings allow users to limit data collection by preventing businesses from storing data, called “cookies,” in the user’s web browser. Egelman Decl. ¶ 29. However, default settings are usually the least restrictive and changing the settings is not always user-friendly. *Id.* ¶ 19. Even if a user is able to successfully block cookies, businesses now track by other means that are not user-controlled, like “fingerprints”—the aggregating of several data points that are automatically collected, such as personal computer settings and location data, and

1 used to identify the user. *Id.* ¶¶ 30–31. Users can do little to stop collection of this data. *Id.*

2 **Terms of Service, Privacy Policies, and Community Standards:** Although terms of
3 service and the like are supposed to allow users to make informed decisions about how and
4 whether to engage with a business, numerous studies have shown that terms of service and
5 privacy policies often prove indecipherable, if a user can even find them, and often do not
6 accurately describe the service’s behavior. Egelman Decl. ¶¶ 24–28; Radesky Decl. ¶ 93. These
7 policies typically allow businesses maximum flexibility in using the personal information they
8 collect. *See* Egelman Decl. ¶¶ 13–14, 28. Also, community standards are intended to inform
9 consumers about how the business moderates its own platform, but it is extremely difficult for
10 users to hold businesses accountable for enforcing these policies, and businesses’ own
11 enforcement is typically, at best, reactive. Radesky Decl. ¶¶ 72, 95.

12 **Consumer Reporting:** Most online businesses purport to provide a way for users to
13 contact the business to ask questions or report concerns. But in practice, there is no method for
14 parents or youth seeking to provide feedback (other than blocking/reporting content) or report a
15 recurrent problem with specific platforms. Radesky Decl. ¶ 94. Parents whose children have died
16 after cyberbullying or taking part in social media challenges have reported trying to get in touch
17 with social media companies, but being ignored. *Id.* If a business fails to take adequate action or
18 respond at all to a reported concern, there is little a user can do. *Id.* ¶¶ 94–95.

19 **II. CHILDREN ON THE INTERNET**

20 Children are especially vulnerable to the risks businesses’ data collection practices pose.
21 Radesky Decl. ¶¶ 39, 45–72. Yet, despite their awareness that children use their services and the
22 existence of technological capabilities to provide a safer experience for children, businesses often
23 fail to take steps to provide that safer experience. *Id.* ¶¶ 30–44; Egelman ¶¶ 35–45.

24 **A. Children’s Internet Use**

25 Children’s internet use has expanded rapidly in the last decade, with children using digital
26 technologies for an average of 0:49 hours per day for children under 2, 2:30 for 2–4 year olds,
27 3:05 for 5–8 year olds, 5:33 for 6–12 year olds, and 8:39 for 13–17 year olds. Radesky Decl. ¶¶
28 21–25. During the COVID-19 pandemic, children’s access to digital technology and time online

1 increased approximately 52%. *Id.* ¶¶ 26–28. Children use the internet for both educational and
 2 entertainment purposes. *Id.* ¶¶ 26–29. Unplugging is not a viable option. *Id.* ¶ 29.

3 **B. Laws Regulating Children’s Online Experience**

4 Despite the ubiquitous presence of the internet in children’s lives, specific legal protections
 5 for children in the US are limited. At the federal level, the Children’s Online Privacy Protection
 6 Act (COPPA) requires that online businesses protect the personal information of children, but
 7 only where the platform is “directed towards” children under 13. 15 U.S.C. §§6501–6506.
 8 However, unless the website self-identifies as one that “target[s] children as its primary
 9 audience[,]” all a website must do is “prevent the disclosure of personal information from visitors
 10 who identify themselves as under age 13” without parental consent. 16 C.F.R. §312.2. At the state
 11 level, California has passed laws specifically designed to protect minors from particular products,
 12 like alcohol, and affords minors special rights, like the ability to have their posts removed by
 13 request. Cal. Bus. & Prof. §§22580, 22581. Although generally businesses may not sell or share
 14 the personal information of a user if they have actual knowledge the user under 16, §1798.120(c),
 15 there is no comprehensive law protecting the collection and use of children’s data.

16 AB 2273 is modeled on the United Kingdom’s Age Appropriate Design Code, commonly
 17 referred to as the “Children’s Code.” This Code requires that all websites likely to be accessed by
 18 children provide privacy protections by default. Keaney (ICO) Decl. ¶¶ 16–25, 32–34 & Ex. A.
 19 As a result, businesses, including some that are represented in this lawsuit, have undertaken
 20 positive changes that have resulted in a safer internet for children. *Id.* ¶¶ 65–67; Radesky ¶ 84.

21 **C. Businesses’ Interaction with Children Online**

22 Existing privacy regulations have inadvertently created a culture of agnosticism about
 23 whether and when children use services intended for adults. Radesky Decl. ¶¶ 30–39; Egelman
 24 Decl. ¶¶ 44–45. Businesses are disincentivized from identifying their services as “child-directed”
 25 because doing so limits the businesses’ ability to monetize their products by collecting and selling
 26 user data and showing targeted advertisements. Radesky Decl. ¶ 39; Egelman Decl. ¶¶ 44–45. As
 27 a result, it is fairly common for apps that were almost certainly intended for children, such as
 28 those that appear in the Google Play “5 and under” app store, to avoid these restrictions by

1 claiming that they were intended for users over 13. Radesky Decl. ¶¶ 31, 36; Egelman Decl. ¶ 45.
 2 This leads not only to the over-collection of children’s data, but to using this data to lead children
 3 to inappropriate ads and other content. Radesky Decl. ¶¶ 31–39. It is only if and when unintended
 4 consequences are discovered that these problems are addressed at all. *Id.* ¶¶ 40–42. Essentially,
 5 despite federal regulation, businesses have, at best, taken a reactive, rather than proactive,
 6 approach towards protecting children’s data. *Id.*

7 **D. Unique Vulnerabilities of Children Online**

8 Children have more curiosity, less impulse inhibition, less critical thinking and abstract
 9 reasoning about complicated concepts (like data collection), more responsivity to parasocial and
 10 peer relationships, and more attraction to novelty and rewards than adults. Radesky Decl. ¶¶ 45–
 11 47. These characteristics are developmentally adaptive and help children learn and build social
 12 relationships in non-digital spaces, but can be taken advantage of through digital design. *Id.* ¶ 46.

13 Businesses design their services to optimize revenue generation by using tactics that
 14 children are more susceptible to, like maximizing time spent using the product, bringing more
 15 people to the product, and increasing interactions and content generation. *Id.* ¶¶ 48–71; Egelman
 16 Decl. ¶¶ 12, 48. For example, multiple interview studies show that children and teens feel like
 17 they spend too much time online, feel pressure to engage, and find it hard to stop using platforms.
 18 Radesky Decl. ¶ 51. Manipulative dark patterns that work through parasocial relationship
 19 pressure, fabricated time pressure, and navigation constraints commonly appear in apps and
 20 platforms used by children. *Id.* ¶ 55; Egelman Decl. ¶ 51. One study showed that these features
 21 occurred in 80% of apps and were more common in apps played by children from lower-income
 22 and lower-education households. Radesky Decl. ¶ 55. Because design features promote content
 23 creation and integrate metrics for popularity, children may take part in extreme content generation
 24 (e.g., challenges) to receive validation online or engage in other harmful activity, such as
 25 disordered eating, self-harm, or gambling, based on what they are seeing online. *Id.* ¶¶ 61–71.

26 These outcomes are features, not bugs, of current platform designs. *Id.* ¶¶ 64–67. And
 27 children, because of their extensive time online and curiosity, and the “pester power” to spend
 28 money, are not unintended victims; they are targets. *Id.* ¶¶ 39, 64–67.

1 **III. THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT**

2 AB 2273 was passed unanimously by the Legislature. Its findings document statewide,
 3 national, and international support for increasing children’s online privacy protections and safety.
 4 In the Act, the Legislature declares and finds that “children should be afforded protections not
 5 only by online products and services specifically directed at them but by all online products and
 6 services they are likely to access[,]” regulated businesses “should consider the best interest of
 7 children when designing, developing and providing” services, and “[i]f a conflict arises between
 8 commercial interests and best interests of children, companies should prioritize the privacy,
 9 safety, and well-being of children over commercial interests.” §1798.99.29.

10 **A. Regulated Businesses**

11 The Act only applies to large companies that trade in personal information. Regulated
 12 businesses are either (1) for-profit entities operating in California that collect consumers’ personal
 13 information or has it collected on their behalf, determine the purposes and means of processing
 14 that information, and have an annual gross revenue of more than \$25,000,000; buy, sell, or share
 15 the personal information of 100,000 or more consumers annually; or derive 50% or more of their
 16 annual revenues from selling or sharing that information; (2) entities that control or are controlled
 17 by and share common branding and consumers’ personal information with businesses described
 18 above; or (3) certain joint ventures or partnerships. §1798.99.30(a); §1798.140(d).

19 Within that group of businesses, the Act regulates only those that provide an online service,
 20 product, or feature (collectively “service”) likely to be accessed by children. §1798.99.31(a), (b).
 21 “Likely to be accessed by children” means that the business’s offering: (1) is directed to children,
 22 as defined by COPPA; (2) is determined, based on competent and reliable evidence regarding
 23 audience composition, to be routinely accessed by a significant number of children, or is
 24 substantially similar or the same as a service for which such a determination has been made; (3)
 25 contains advertisements marketed to children; (4) has design elements that are known to be of
 26 interest to children, including games, cartoons, music, and celebrities that appeal to children; or
 27 (5) is determined, based on internal company research, to have children as a significant amount of
 28 its audience. §1798.99.30(b)(4). Broadband internet access, telecommunications services,

1 delivery and use of a physical product, and certain medical information is excluded from
2 regulation. *Id.* at (b)(5); §1798.99.40.

3 **B. Requirements for Regulated Businesses**

4 **1. Proactive Steps to Protect Children’s Privacy**

5 For each service or similar group of services likely to be accessed by children, businesses
6 must identify the service’s purpose, “how it uses children’s personal information, and the risks of
7 material detriment to children that arise from” the business’s data management practice in a Data
8 Protection Impact Assessment (“DPIA”). §1798.99.31(a)(1)(A)–(B); *Id.* at (c)(2). A DPIA
9 completed for compliance with any other similar law, such as the UK Children’s Code, is deemed
10 compliant with the Act. *Id.* at (c)(1). A DPIA must address, to the extent applicable, whether the
11 design of the service could (i) harm children, including by exposing children to harmful or
12 potentially harmful content; (ii) lead to children experiencing or being targeted by harmful or
13 potentially harmful contacts; (iii) permit children to witness, participate in, or be subject to
14 harmful or potentially harmful conduct, or (iv) allow children to be party to or exploited by
15 harmful or potentially harmful contacts. *Id.* at (a)(1)(B). The DPIA must also address whether any
16 algorithms and targeted advertising systems used could harm children; whether and how the
17 service uses system design features to increase, sustain, or extend children’s use of the service,
18 including the automatic playing of media, rewards for time spent, and notifications; and whether,
19 how, and for what purpose the service collects and processes children’s sensitive personal
20 information. *Id.* Regulated businesses must document any risk of material detriment that arises
21 from their data management practices in the DPIA and create a timed plan to mitigate or
22 eliminate these risks before the service is accessed by children. *Id.* at (a)(2).

23 The DPIA is intended to be the business’s internal document. It is “protected as confidential
24 and shall be exempt from public disclosure.” *Id.* at (a)(4)(B). Regulated businesses must
25 biennially review all DPIAs, provide the Attorney General with a list of all DPIAs within three
26 days of receiving a written request to do so, and make any specific DPIA available to the
27 Attorney General within 5 days of a written request to do so. *Id.* at (a)(1)(A), (a)(3)–(4). DPIAs
28 retain any legal privilege even if disclosed to the Attorney General. *Id.* at (a)(4)(C).

1 In addition to DPIAs, regulated businesses must also: (1) estimate the age of a child user
 2 with a reasonable level of certainty appropriate to the risks that arise from the business's data
 3 management practices, or apply the privacy and data protection afforded to children to all
 4 consumers; (2) configure all default privacy settings provided to children to offer a high level of
 5 privacy unless the business can demonstrate a compelling reason that a different setting is in the
 6 best interest of children; (3) provide any privacy information, terms of service, policies, and
 7 community standards concisely, prominently, and using clear language suited to the age of
 8 children likely to access the service; (4) if applicable, provide an obvious signal to the child while
 9 the child is being monitored or tracked by a guardian or other consumer; (5) enforce published
 10 terms, policies, and community standards established by the business, including but not limited to
 11 privacy policies and those concerning children; and (6) provide prominent, accessible and
 12 responsive tools to help children or their guardians exercise their privacy rights and report
 13 concerns. *Id.* at (a)(5)–(10).

14 **2. Prohibitions**

15 Regulated businesses are prohibited from engaging in certain business practices that use
 16 children's personal information. First, regulated businesses cannot use any child's personal
 17 information in a way that the business knows or has reason to know is materially detrimental to
 18 the physical health, mental health, or well-being of the child. §1798.99.31(b)(1). Second,
 19 regulated businesses are prohibited from profiling a child by default except where the business
 20 can demonstrate it has appropriate safeguards in place to protect children and profiling is either
 21 necessary to provide the requested service and limited to the aspects of the service with which the
 22 child is actively and knowingly engaged, or where the business can demonstrate a compelling
 23 reason profiling is in the best interest of children. *Id.* at (b)(2). Third, regulated businesses cannot
 24 collect, sell, share, or retain any personal information not necessary to provide a service with
 25 which a child is actively or knowingly engaged absent a demonstrated compelling reason that the
 26 practice is in the best interest of children likely to access the service. *Id.* at (b)(3). Businesses may
 27 engage in these practices as needed to comply with existing laws. *Id.*; §1798.145. Fourth, if the
 28 end user is a child, regulated businesses cannot use personal information for any reason other than

the reason for which it was collected absent a demonstrated compelling reason it is in the best interest of children. §1798.99.31(b)(4). Fifth, regulated businesses cannot collect, sell, or share any child’s precise geolocation information by default unless that is strictly necessary to provide the requested service and then only for the limited time necessary to provide the service and businesses cannot collect this information without providing an obvious sign to the child while the information is being collection. *Id.* at (b)(5)–(6). Seventh, regulated businesses cannot use dark patterns—interfaces designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice—to lead or encourage children to provide personal information beyond what is reasonably expected to provide the service, to forgo privacy protections, or to take any action that the business knows or has reason to know is materially detrimental to the child’s physical health, mental health, or well-being. *Id.* at (b)(7); §1798.140(l). And, any information businesses collect to estimate age may be used for that purpose only, and may not be retained by businesses longer than needed to make the estimate. Age assurance shall be proportionate to the risks and data practice of a service. §1798.99.31(b)(8).

C. Enforcement & Guidance

Regulated businesses must comply with the above requirements, including completing DPIAs, by July 1, 2024. §1798.99.31(d); §1798.99.33. Violators face injunctions and civil penalties up to \$2,500 per affected child for each negligent violation and up to \$7,500 per affected child for each intentional violation. §1798.99.35(a). Penalties are assessed and recovered via a civil suit brought by the Attorney General. *Id.* Businesses in substantial compliance with the DPIA requirements will receive written notice from the Attorney General of any alleged violations before the Attorney General initiates a suit. *Id.* at (c)(1). A business will not be liable for civil penalties for any violations cured within 90 days of the notice if it provides written notice of curing and sufficient measures to prevent future violations. *Id.* at (c)(2).

The Act creates the California Children’s Data Protection Working Group, which will issue a publicly available report containing best practices for implementation of the Act by January 1, 2024 (six months before the compliance date) and every two years thereafter. §1798.99.32. Regulated businesses “may look to guidance and innovation in response to” the UK Children’s

Code when developing services likely to be accessed by children. AB 2273, §1(d). Additionally, the Attorney General may adopt regulations related to the Act. §1798.99.35(e).

IV. PLAINTIFF’S CHALLENGE TO AB 2273

Plaintiff is NetChoice, a membership group composed of 35 large tech companies including Google, Meta, Amazon, Twitter, and TikTok. It filed this suit on December 14, 2022, alleging that the Act violated the First, Fourth, and Fourteenth Amendments, and the dormant Commerce Clause, and is preempted by federal law. It filed this Motion on February 17, 2023.

LEGAL STANDARD

“A preliminary injunction is an extraordinary remedy never awarded as of right.” *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008); *Dymo Indus., Inc. v. Tapeprinter, Inc.*, 326 F.2d 141, 143 (9th Cir. 1964) (per curiam). Plaintiff must prove that it is likely to succeed on the merits of its claims, it is likely to suffer irreparable harm without preliminary relief, that the balance of equities tips in its favor, and that an injunction is in the public interest. *Winter*, 555 U.S. at 20; *Alliance for Wild Rockies v. Cottrell*, 632 F.3d 1127, 1135 (9th Cir. 2011).

ARGUMENT

I. PLAINTIFF IS NOT LIKELY TO SUCCEED ON THE MERITS

A. AB 2273 Does Not Violate the First Amendment

Plaintiff’s members have no right to children’s personal information. Thus, AB 2273 does not violate, or even implicate, Plaintiff’s members’ First Amendment rights. The Act imposes no prior restraints because it does not regulate content, mandate government approval before businesses can act, or restrict what content businesses make accessible to consumers. It is a facially neutral business regulation and thus not subject to any heightened scrutiny. However, even if the Act triggered heightened scrutiny, it could withstand such scrutiny because it serves compelling interests in protecting children from intrusive, privacy-violating practices all too common on the internet today. Far from being overbroad, the Act is carefully tailored to addressing the most substantial threats to child online privacy.

1. AB 2273 does not regulate speech or expressive conduct

Businesses have no First Amendment right to collect and use children’s personal

1 information and “[a] facial freedom of speech attack must fail unless, at minimum, the challenged
 2 statute is directed narrowly and specifically at expression or conduct commonly associated with
 3 expression.” *Roulette v. City of Seattle*, 97 F.3d 300, 305 (9th Cir. 1996) (unless otherwise noted,
 4 all internal quotation marks and citations have been omitted throughout). The collection and use
 5 of data under the Act is neither speech nor conduct with a significant expressive element. Further,
 6 often, children are not even willingly sharing this data. *See* Radesky Decl. ¶¶ 32–33. It can be
 7 collected from them, and all consumers, without their knowledge or consent. Egelman Decl. ¶¶
 8 30–31. This is not a case where two parties wish to share information and the State is standing in
 9 the way. *See Sorrell v. IMS Health Inc.*, 564 U.S. 552, 654–65 (2011) (First Amendment protects
 10 two private parties willingly sharing information).

11 The Act regulates business practices—those related to the collection and use of children’s
 12 personal information—which are not typically considered conduct with a significant expressive
 13 element. *Int’l Franchise Ass’n v. City of Seattle*, 803 F.3d 389, 408 (9th Cir. 2015). An entity
 14 cannot claim a First Amendment violation simply because it is subject to government regulation.
 15 *Am. Soc’y of Journalists & Authors v. Bonta* (“ASJA”), 15 F.4th 954, 961 (9th Cir. 2021).
 16 “[R]estrictions on protected expression are distinct from restrictions on economic activity or,
 17 more generally, on nonexpressive conduct. While the former is entitled to protection, the First
 18 Amendment does not prevent restrictions directed at commerce or conduct from imposing
 19 incidental burdens on speech.” *HomeAway.com v. City of Santa Monica*, 918 F.3d 676, 685 (9th
 20 Cir. 2019) (no First Amendment scrutiny for ordinance regulating online booking transactions)
 21 (quoting *Sorrell*, 564 U.S. at 567); *see also Minneapolis Star & Tribune Co. v. Minn. Comm’r of*
 22 *Revenue*, 460 U.S. 575, 581 (1983) (newspapers can be subject to “generally applicable economic
 23 regulations without causing constitutional problems”) “To determine whether the First
 24 Amendment applies, we must first ask the threshold question [of] whether conduct with a
 25 significant expressive element drew the legal remedy or the ordinance has the inevitable effect of
 26 singling out those engaged in expressive activity.” *Homeaway.com*, 918 F.3d at 685 (quoting *Int’l*
 27 *Franchise*, 803 F.3d at 408). “A court may consider the inevitable effect of a statute on its face, as
 28 well as a statute’s stated purpose.” *Id.* (quoting *Sorrell*, 564 U.S. at 565).

Plaintiff argues that businesses use children’s personal information to make specialized recommendations to them, such as for books, movies, and videos to watch, and thus businesses’ ability to collect and use children’s data implicates businesses’ First Amendment rights. Pl. Br. 3, 15. This is simply incorrect. The Supreme Court explicitly “reject[s] the view that conduct can be labeled speech whenever the person engaging in the conduct intends to thereby express an idea.” *Rumsfeld v. Forum for Acad. & Institutional Rts., Inc. (FAIR)*, 547 U.S. 47, 65–66 (2006) (citing cases). Further, businesses can continue to make recommendations to child users, even including recommendations for content the business knows or has reason to know will harm the child; they just may not use the child’s personal information to do so. *See Nat’l Endowment for the Arts v. Finley*, 524 U.S. 569, 573 (1998) (rejecting claim where law does not “inherently interfere[] with First Amendment rights”). Recommendations based on anything other than the child’s personal information are unrestricted. *See Denver Area Telecomm. Consortium, Inc., v. FCC*, 518 U.S. 727, 746 (1996) (regulation to protect children permissible where cable operators could comply through rearranging broadcast times); *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 647 (1994) (rule that cable operators must carry broadcast channels permissible given operators controlled every other channel in their package).

The Act’s stated purpose further supports that it “was not motivated by a desire to suppress speech[.]” *Int’l Franchise*, 803 F.3d at 409. Rather, the “inevitable effect of the [Act] on its face is to regulate nonexpressive conduct”—the collection and use of children’s personal information. *Homeaway.com*, 918 F.3d at 685 (quoting *Sorrell*, 564 U.S. at 565). The Act is generally applicable because limitations apply equally to all regulated businesses. Some organizations, like non-profits and governmental entities, are excluded because they lack the profit motive of the regulated businesses. “[S]uch distinctions do not typically implicate the First Amendment[.]” and the existence of “different, or even broader, carve outs” does not “render[] [a law] generally inapplicable.” *ASJA*, 15 F.4th at 964. Nor does the Act deprive businesses of information or the ability to use it in a manner that discriminates between users. *See Sorrell*, 564 U.S. at 577 (invalidating prohibition on sharing information with only certain parties).

2. None of the challenged provisions impose a prior restraint

1 “The relevant question” in determining whether a prior restraint exists “is whether the
 2 challenged regulation *authorizes* suppression of speech in advance of its expression[.]” *Long*
 3 *Beach Area Peace Network v. City of Long Beach*, 574 F.3d 1011, 1023 (9th Cir. 2009) (quoting
 4 *Ward v. Rock Against Racism*, 491 U.S. 781, 795 n.5 (1989)). The regulation must specifically
 5 target, rather than incidentally affect, expression protected by the First Amendment. *Spirit of*
 6 *Aloha Temple v. Cnty. of Maui*, 49 F.4th 1180, 1191 (9th Cir. 2022). “[C]ontent-neutral
 7 injunctions that do not bar all avenues of expression are not treated as prior restraints.” *Greater*
 8 *L.A. Agency on Deafness, Inc. v. Cable News Network, Inc.*, 742 F.3d 414, 431 (9th Cir. 2014).

9 **DPIA Requirement:** This provision requires businesses to internally assess, and prepare
 10 confidential reports to the government about their data collection and use practices.
 11 §1798.99.31(a)(1)–(4); *see also* ICO Decl. Exs. B1–B3 (UK DPIA samples). Such reporting
 12 requirements are well-within the bounds of appropriate government regulation. *See Hotel Emps.*
 13 *& Rest. Emps. Int’l Union v. Nev. Gaming Comm’n*, 984 F.2d 1507, 1518 (9th Cir. 1993); *Village*
 14 *of Schaumburg v. Citizens for a Better Env’t*, 444 U.S. 620, 637–38 n.12 (1980) (requirement to
 15 “report certain information” on routine basis is permissible); *see also, e.g.* 12 U.S.C. §5365(i)(2)
 16 (certain financial institutions must run annual or semiannual internal stress tests); 26 U.S.C.
 17 §501(r)(3) (non-profit hospitals must conduct community health needs assessment every three
 18 years and adopt implementation strategy to meet identified needs). The DPIA is not subject to
 19 public disclosure and need not be approved—or even seen—by the Attorney General before a
 20 business can begin offering a service. §1798.99.31(a)(3)–(4).

21 Contrary to what Plaintiff suggests, Pl. Br. 9–10, the Act does not authorize penalization
 22 based on substance communicated in the DPIA. *See Nev. Gaming*, 984 F.2d at 1518 (no prior
 23 restraint where “there is no attempt to control the content of any speech or the nature of any
 24 organizational activity”); *compare* §1798.99.31(a)(3)–(4) *to Bantam Books v. Sullivan*, 372 U.S.
 25 58, 68 (1963) (law “directly and designedly stopped the circulation of publications”). The AG’s
 26 only role is to determine if a DPIA addresses all the required points. *Compare* §1798.99.31(a)(3)–
 27 (4) *to Se. Promotions, Ltd v. Conrad*, 420 U.S. 546, 554 n.7 (1975) (“approval of an application
 28 required some judgment as to the content and quality of the [theater] production”). It is only if the

1 business does not cure or makes no effort to complete the DPIA that the Attorney General can
 2 even attempt to seek penalties through a civil suit. *Compare* §1798.99.35(c) to *Bantam Books*,
 3 372 U.S. at 71 (procedures were “radically deficient”).

4 Unlike the laws in the cases Plaintiff cites, the DPIA must address a “reasonably specific
 5 and objective” list of subjects; compliance determinations are not left “to the whim of the
 6 administrator.” *Thomas v. Chi. Park Dist.*, 534 U.S. 316, 324 (2002); *compare*
 7 §1798.99.31(a)(1)(B) to *Interstate Cir., Inc. v. City of Dallas*, 390 U.S. 676, 689–90 (1968)
 8 (standards did not provide sufficient guidance), and *Bantam Books*, 372 U.S. at 71 (“statutory
 9 mandate is vague and uninformative”). That a business may decide to discontinue or never launch
 10 a service rather than complete a DPIA does not effect a prior restraint. *See IDK v. Clark County*,
 11 836 F.2d 1185, 1196–97 (9th Cir. 1988) (license requirement “does not operate as a prior restraint
 12 on expression”).

13 **Policy Enforcement Provision:** The Policy Enforcement Provision, §1798.99.31(a)(9),
 14 permissibly holds online businesses accountable for doing what they say they are going to do.
 15 *Barnes v. Yahoo, Inc.*, 570 F.3d 1096, 1109 (9th Cir. 2009) (promissory estoppel contract claim
 16 not precluded by Section 230); Cal. Bus. & Prof. Code §22575 (online businesses must abide by
 17 posted privacy policies). The government has no control over any content and businesses remain
 18 free to create whatever policies they want. They need not commit to taking actions that they do
 19 not intend take to or are morally opposed to. *See Williams v. Gerber Prods., Co.*, 552 F.3d 934,
 20 939 n.3 (9th Cir. 2008) (“It is not difficult [for businesses] to choose statements, designs, and
 21 devices which will not deceive.”). The policies Plaintiff submitted demonstrate the flexibility
 22 businesses give themselves in determining how to respond to violations of their policies; most
 23 include explicit language reserving final decisions about content exclusively to the website or its
 24 moderators. *See e.g.*, Docs. 29-4, 29-6; 29-7, 29-24; 29-26, 29-27. The Act does not permit the
 25 Attorney General to rewrite or ignore these terms. Contrary to what Plaintiff suggests, Pl. Br. 10–
 26 11, if a business, consistent with its publicly posted policies, has decided to remove or allow
 27 content, there is nothing the Attorney General can do.

28 Further, for a business to publish policies and not abide by them is deceptive and

misleading and thus renders the policy itself unprotected speech. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 563 (1980); *Litton Indus. Inc. v. FTC*, 676 F.2d 364, 373 (9th Cir. 1982); Cal. Bus. & Prof. Code §17500 (prohibiting false or misleading advertising). Indeed, “[i]t is an open question whether the prior restraint doctrine even applies to commercial speech.” *Hunt v. City of Los Angeles*, 638 F.3d 703, 718 n.7 (2011) (citing cases). Even if it does, requiring businesses to comply with their own posted policies does not authorize the suppression of any protected speech or compel speech.

Age Estimation & Data Protection Provision: Requiring businesses to protect children’s privacy and data implicates neither protected speech nor expressive conduct. This provision sets forth the level of protections businesses must provide to children. §1798.99.31(a)(5). Businesses that estimate the age of child users need only provide child users the data and privacy protections appropriate to the risks that arise from the businesses’ data management practices. *Id.* Businesses that do not estimate the age of child users must apply child-appropriate data and privacy protections to all consumers. *Id.* The provision says nothing about content and does not require businesses to block any content for users of any age.

Plaintiff’s challenge is based on mischaracterizations. Pl. Br. 12–13. The Act does not require “age verification” or even age estimation; businesses can opt out of age estimation entirely and instead provide the same data and privacy protections to everyone. Plaintiff contends that either option will affect its member’s bottom line: they will either have to cover the costs of age estimation or lose whatever revenue they obtain through providing lesser data and privacy protection to all users. But the financial costs of complying with government regulation cannot alone be the basis of a First Amendment claim. *ASJA*, 15 F.4th at 962.

Plaintiff’s inappropriate attempt to raise the third-party claims of children by arguing that age estimation will force children to either comply with invasive age-verification requirements or be deprived access to regulated businesses presents a false choice. *See Marquez-Reyes v. Garland*, 36 F.4th 1195, 1201 (9th Cir. 2022) (explaining limitations on raising third-party rights) (quoting *L.A. Police Dep’t v. United Reporting Publ’g Corp.*, 528 U.S. 32, 38 (1999)). Further, if businesses choose to engage in age estimation, nothing in the Act requires use of the most

1 invasive age-estimation tools imaginable. To the contrary, businesses are instructed to use
 2 “minimally invasive” tools, §1798.99.32(d)(3), and the estimation only need be appropriate to the
 3 level of risk that their data management practices present, §1798.99.31(a)(5). Defendant has
 4 provided multiple examples of such tools, Egelman Decl. ¶¶ 53–54; Radesky Decl. ¶ 96; ICO
 5 Decl. ¶¶ 37–39, some of which are already being tested by NetChoice members, ICO Decl. ¶ 65,
 6 and best practices for implementation will be available six months before businesses are required
 7 to comply, §1798.99.32(e). *See Lone Star Sec. & Video, Inc. v. City of Los Angeles*, 827 F.3d
 8 1192, 1199 (9th Cir. 2016) (in a facial challenge courts must consider government’s
 9 “authoritative constructions, including . . . implementation and interpretation”).

10 Even if Plaintiff could raise claims based on children’s right to access information,
 11 restricting businesses’ use of children’s data does not require barring children’s access to any
 12 content. Unlike the broad content-based laws in cases Plaintiff cites, Pl. Br. 13, the Act does not
 13 penalize providing any particular content. *Compare e.g.* §1798.99.31(b)(1) *to Butler v. Michigan*,
 14 352 U.S. 380, 382–83 (1957) (law criminalized making certain books available to the public).
 15 Children can have, and businesses can provide, access to any information the child seeks. *See*
 16 *Greater L.A.*, 742 F.3d at 431 (“[C]ontent-neutral injunctions that do not bar all avenues of
 17 expression are not treated as prior restraints.”). Rather, the Act prevents businesses from
 18 attempting to increase their profits by using children’s data to deliver them things they do not
 19 want and have not asked for, such as ads for weight loss supplements and content promoting
 20 violence and self-harm. Radesky Decl. ¶¶ 48, 62–68. Further, Plaintiff misplaces its reliance on
 21 cases challenging content-based criminal statutes, like laws prohibiting child sexual exploitation,
 22 where age verification of the minor involved could serve as either an affirmative defense to or
 23 lack thereof as an element of the crime. *See* Pl. Br. 13–14 (citing cases). Age estimation plays a
 24 completely different role here. And, the Act protects children’s anonymity by prohibiting
 25 information used for age estimation from being used for any other purpose. §1798.99.31(b)(8).

26 **3. AB 2273 is facially neutral**

27 Even if AB 2273 does implicate First Amendment concerns, it is not subject to heightened
 28 scrutiny because it is content, viewpoint, and speaker neutral. “[A] regulation that serves purposes

unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some . . . messages but not others.” *Doe v. Harris*, 772 F.3d 563, 575 (9th Cir. 2014) (quoting *Ward*, 491 U.S. at 791). Such a law is content neutral if it is “*justified* without reference to the content of the regulated speech.” *Id.* at 574. On the other hand, a regulation is “facially content based” if it “targets speech based on its communicative content,” “prohibit[s] public discussion of an entire topic, or single[s] out specific subject matter for differential treatment.” *Twitter Inc. v. Garland*, 61 F.4th 686, 697 (9th Cir. 2023) (citing cases).

To determine whether the Act’s “overriding objective” is content-neutral, the court reviews “the Act and its various findings[.]” *Turner*, 512 U.S. at 646. In *Turner*, cable operators challenged a federal rule requiring them to carry broadcast channels as part of their cable packages. *Id.* at 631–32. In concluding that the “overriding Congressional purpose is unrelated to the content of [operator’s] expression[.]” the Court cited Congress’s findings that the rule’s purpose was to preserve access to free television programming—a “substantial and important” government interest—which would be endangered if cable operators refused to carry broadcast stations for economic reasons. *Id.* at 646–47. Though cable operators lost some discretion, “the design and operation” of the rule did not have any of the markers of content-based regulation, such as requiring or prohibiting particular ideas or points of view, penalizing operators because of the content of their programming, compelling operators to affirm points of view with which they disagree, or producing a net decrease in the amount of available speech. *Id.* at 647. In short, because operators were free to carry whatever programming they wished on all stations not subject to the must-carry rule, the rule was deemed content neutral. *Id.* at 646–47.

The same logic applies here. The Legislature clearly explained the Act’s purpose: to “prioritize the privacy, safety, and well-being of children over commercial interests.” §1798.99.29(b). Currently, businesses have an economic incentive to collect, use, buy, and sell children’s data. Egelman Decl. ¶¶ 11–13; Radesky Decl. ¶¶ 33, 39, 64, 78, 101. It is these profit-driven business practices, not any particular message, that AB 2273 restricts. The Act does not carry any markers of content-based regulation. As long as businesses do not use children’s data, they can continue to offer, provide access to, and recommend any content they want.

Plaintiff’s assertion that the Act is “inherently content-based” because it prioritizes the health and safety of minors, Pl. Br. 19, does not make it so. That some limitations on the use of children’s personal information require businesses to consider knowledge they have about how their actions affect children does not make the Act content-based. Those limitations are consistent with the Act’s content-neutral purpose: to prioritize children’s safety and well-being over profit. Plaintiff’s “ability to hypothesize a content-based purpose” that “rests on little more than speculation” “does not cast doubt upon the [Act’s] content-neutral character.” *Turner*, 512 U.S. at 652. Nor should Plaintiff’s highly speculative claims that the DPIA and Policy Enforcement provisions are content-based or compel speech cast any doubt. As described above, Arg. I.A.2, these provisions are common forms of acceptable government regulation. The Act does not affect businesses’ speech, require “inherently expressive” conduct, or otherwise “sufficiently interfere with any message” of businesses. *See FAIR*, 547 U.S. at 64–65. Any impact on speech is merely incidental to the Act’s regulation of conduct. *Id.* at 62.

Here, the court must ask whether the conduct the law restricts—using children’s personal information—is expressive or communicative. *Recycle for Change v. City of Oakland*, 856 F.3d 666, 672 (9th Cir. 2017). It is not. And because it is not, creating exceptions to general bans on such use (like allowing it where it is in the best interest of the child), even ones that refer to content, do not present a constitutional problem. *See Jacobs v. Clark County Sch. Dist.*, 526 F.3d 419, 433 (9th Cir. 2008) (exception to uniform policy did not render policy content-based); *Perry v. L.A. Police Dept.*, 121 F.3d 1365, 1369 (9th Cir. 1997) (neutral ban with exception that refers to content is content neutral). Even if the law incidentally burdens businesses’ speech, the Act is content neutral because, for all the reasons already explained, it is “*justified* without reference to the content of the [allegedly] regulated speech.” *Harris*, 772 F.3d at 575.

For all of the reasons above, the Act is content neutral. For the same reasons that AB 2273 is generally applicable, it is not speaker-based. Plaintiff does not allege that it is viewpoint-based. Thus, the Act is not subject to heightened scrutiny.

4. AB 2273 withstands any level of First Amendment scrutiny

a. At most, intermediate scrutiny applies

1 If the Court determines the Act restricts speech and higher scrutiny is warranted, it should
2 apply, at most, intermediate scrutiny.

3 “[T]he Supreme Court has repeatedly held that a law restricting speech on a viewpoint and
4 content neutral basis is constitutional as long as it withstands intermediate scrutiny[.]” *Jacobs*,
5 526 F.3d at 434 (citing *Turner*, 512 U.S. at 661–62). The same is true of laws that have incidental
6 effects on expressive conduct. *Id.* (citing *U.S. v. O’Brien*, 391 U.S. 367, 376–77 (1968)). And
7 here, any speech the Act may implicate is commercial speech, which is also subject to
8 intermediate scrutiny. *Cent. Hudson*, 447 U.S. at 566. For example, businesses’ publicly posted
9 policies are supposed to aid consumers in deciding whether to engage with their products.
10 Egelman Decl. ¶ 24; Radesky Decl. ¶ 72. When consumers do engage with those products, the
11 business gains revenue. Egelman Decl. ¶¶ 11–13; Radesky Decl. ¶¶ 49, 55, 100. Indeed,
12 Plaintiff’s declarants’ objections and their alleged injury are based on the impact the Act will
13 have on their revenue. Pl. Br. 12–13, 30. Thus, there can be no doubt that regulated businesses
14 have “an economic motive for engaging in the [alleged] speech” with regard to the specific
15 products—services likely to be accessed by children—that the Act regulates. *Am. Acad. of Pain*
16 *Mgmt. v. Joseph*, 353 F.3d 1099, 1106 (9th Cir. 2004) (listing conditions for commercial speech)
17 (citing *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66–67 (1983)).

18 AB 2273 easily survives intermediate scrutiny. As described further below, Plaintiff’s
19 members’ business practices pose “real” risks to children, and the Act “in fact alleviates th[ose
20 risks] to a material degree” by reducing the use of those business practices. *Edenfield v. Fane*,
21 507 U.S. 761, 770–71 (1993); *see also Coyote Publ’g v. Miller*, 598 F.3d 592, 611 (9th Cir. 2010)
22 (“a reasonable fit between ends and means” meets intermediate scrutiny).

23 **b. AB 2273 withstands strict scrutiny**

24 A content-based speech regulation must survive strict scrutiny and, if it is the type of
25 restriction for which procedural safeguards are required, it must provide those safeguards. *In re*
26 *Nat’l Sec. Letter*, 33 F.4th 1058, 1071 (9th Cir. 2022). “Under strict scrutiny, restrictions may be
27 justified only if the government proves that they are narrowly tailored to serve compelling state
28 interests.” *Id.* at 1070. AB 2273 is not content based, but can withstand this scrutiny.

1 “It is evident beyond the need for elaboration that a State’s interest in safeguarding the
 2 physical and psychological well-being of a minor is compelling.” *Ferris v. Santa Clara County*,
 3 891 F.2d 715, 717 (9th Cir. 1989) (quoting *Globe Newspaper Co. v. Superior Court*, 457 U.S.
 4 596, 607 (1982)). Accordingly, courts “have sustained legislation aimed at protecting the physical
 5 and emotional well-being of youth even when the laws have operated in the sensitive area of
 6 constitutionally protected rights.” *Id.*; accord *Sable Commc’ns of Cal., Inc. v. F.C.C.*, 492 U.S.
 7 115, 126 (1989). Indeed, “the Supreme Court[] [has] repeated[ly] recogni[zed] that children
 8 deserve special solicitude in the First Amendment balance because they lack the ability to access
 9 and analyze fully the information presented through commercial media.” *Anheuser-Busch, Inc. v.*
 10 *Schmoke*, 101 F.3d 325, 329–30 (4th Cir. 1996) (collecting cases).

11 Under strict scrutiny, speech restrictions can be justified by “history, consensus, and simple
 12 common sense[.]” *Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 628 (1995). Where, as here, the
 13 interest is “intuitive[.]” *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 445 (2015), or evident from “an
 14 impressive historical pedigree” of “public disapproval” of the prohibited conduct, *Coyote Publ’g*,
 15 598 F.3d at 604, little, if any, evidence is required. That children face significant barriers to
 16 protecting their personal information online and face serious harms as a result is part of the
 17 legislative findings and affirmed by Defendant’s experts’ testimony. *See* AB 2273, §1; Radesky
 18 Decl. ¶¶ 21–72; Egelman Decl. ¶¶ 11–30, 49–51. Here, “an actual problem has been proved[.]”
 19 *U.S. v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 822 (2000).

20 And the Act is narrowly tailored. Even if the Act did restrict content, it is well established
 21 that the government can regulate mediums that—like the internet—are “accessible to children[.]”
 22 are “likely” to have children as an audience, and that “have established a uniquely pervasive
 23 presence in the lives of all Americans[.]” *Denver Area*, 518 U.S. at 744–45. Under these
 24 circumstances, a “permissive” approach that may restrict content, but does not ban it all together,
 25 are “appropriate as a means of achieving the underlying purpose of protecting children.” *Id.* at
 26 746. The Act regulates only those businesses that trade in personal information and are likely to
 27 be accessed by children. It requires or prohibits specific actions that directly involve the
 28 collection and use of children’s personal information. The Act need not advance its interest “in

1 the least restrictive and least intrusive way[.]” *G.K. Ltd. Travel v. City of Lake Oswego*, 436 F.3d
 2 1064, 1073–74 (9th Cir. 2006), and, here, the State’s interest would undoubtedly be “achieved
 3 less effectively absent” the Act. *Colacurcio v. City of Kent*, 163 F.3d 545, 553 (9th Cir. 1998).

4 “[P]erfect tailoring” is not required and courts should avoid “wad[ing] into the swamp of
 5 calibrating the individual mechanisms of a restriction” when applying strict scrutiny. *In re Three*
 6 *Nat’l Security Letters*, 35 F.4th 1181, 1186 (9th Cir. 2022). In any case, Plaintiff’s proposed
 7 alternatives are in no way “as effective in achieving the legitimate purpose” of this Act. *Id.*
 8 Plaintiff’s parental-oversight alternative is a thinly veiled attempt to escape all regulation. Unlike
 9 in cases Plaintiff cites, Pl. Br. 21–22, parents cannot simply block children from accessing any
 10 online business that collects or uses their children’s personal information, Egelman Decl. ¶ 24–
 11 31, 34 (user-based attempts to protect privacy are “futile”); Radesky Decl. ¶ 95 (“maintaining
 12 digital privacy is a near impossible task” for parents). *See Playboy*, 529 U.S. at 816 (requiring
 13 less restrictive alternative be “plausible”). Even if they could, such action would not be consistent
 14 with the Act’s goals: to allow children to use the internet safely, not prevent them from using it
 15 all. Indeed, “[i]t is the interest of youth itself, and of the whole community, that children be both
 16 safeguarded from abuses and given opportunities for growth[.]” *Prince v. Massachusetts*, 321
 17 U.S. 158, 165 (1944). Further, “[w]hile the supervision of children” on the internet “may best be
 18 left to their parents, the knowledge that parental control or guidance cannot always be provided
 19 and society’s transcendent interest in protecting the welfare of children justify reasonable
 20 regulation[.]” *Ginsberg v. New York*, 390 U.S. 629, 640 (1968). In any case, relying on parental
 21 involvement alone would leave vast swaths of children completely unprotected, thus undermining
 22 “the State’s independent interest in the well-being of its youth[.]” *Reno v. ACLU*, 521 U.S. 844,
 23 865 (1997); *accord e.g., Ginsberg*, 390 U.S. at 640–41. Plaintiff’s suggestion that COPPA
 24 accomplishes the Act’s purpose fares no better. COPPA does not protect all children under 18 nor
 25 apply to all businesses likely to be accessed by children.

26 Finally, the Act is not required to have the procedural safeguards necessary for “traditional
 27 censorship regimes,” *Twitter*, 61 F.4th at 707, because those “are not required in the context of
 28 government restrictions on the disclosure of information transmitted confidentially as part of a

legitimate government process,” *id.*, and may not apply where the challenged law “neither requires a speaker to submit proposed speech for review and approval” nor “require[s] a speaker to obtain a license before engaging in business[.]” *Nat’l Sec. Letter*, 33 F.4th at 1077. The Act includes significant procedural safeguards, a cure period and court review, that are “sensitive to the need to prevent First Amendment harms.” *Twitter*, 61 F.4th at 705.

5. AB 2273 is not overbroad

“Invalidation for overbreadth is strong medicine that is not to be casually employed.” *U.S. v. Williams*, 553 U.S. 285, 292 (2008). Plaintiff “bears the burden of demonstrating, from the text of [the law] and from actual fact, that substantial overbreadth exists.” *Gospel Missions of Am. v. City of Los Angeles*, 419 F.3d 1042, 1050 (9th Cir. 2005) (citing *Virginia v. Hicks*, 539 U.S. 113, 122 (2003)); *see also Marquez-Reyes*, 36 F.4th at 1202 (“it is impossible to determine whether a statute reaches too far without first knowing what the statute covers.”). That the Act regulates conduct, not speech, makes the bar even higher as “the overbreadth doctrine’s concern with chilling protected speech attenuates as the otherwise unprotected behavior that it forbids the state to sanction moves from pure speech towards conduct.” *Hicks*, 539 U.S. at 124. “[W]here conduct and not merely speech is involved. . . the overbreadth of a statute must not only be real, but substantial as well, judged in relation to the statutes plainly legitimate speech.” *Gospel Mission*, 419 F.3d at 1050 (citing *Broadrick v. Oklahoma*, 413 U.S. 601, 615 (1973)). Here, it is neither.

Plaintiff has failed to show why any of the conduct required or prohibited by the Act “cannot constitutionally be subject to some regulation.” *Gospel Mission*, 419 F.3d at 1050. Plaintiff relies on speculative arguments about children’s inability to access content, but, as discussed above, nothing in the Act bars children from seeking, or businesses from providing access to, any content. “The mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge.” *Williams*, 553 U.S. at 303.

Plaintiff has not shown that the Act violates the First Amendment in any—let alone a “substantial” number of—potential applications. *Gospel Mission*, 419 F.3d at 1050. Even if the Act might reach some protected speech through its regulation of the use of children’s personal

information, “it is not substantially overbroad relative to its legitimate sweep.” *Id.* “Whether a statute’s chilling effect on legitimate speech is substantial should be judged in relation to what the statute clearly proscribes.” *Cal. Teachers Ass’n v. State Bd. of Educ.*, 271 F.3d 1141, 1151 (9th Cir. 2001). For the same reasons the Act is narrowly tailored, it is not overbroad. The Act prohibits certain businesses from using children’s personal information for specified reasons, “the vast majority” of applications “raises no constitutional problems whatever.” *Williams*, 553 U.S. at 303. Further, “the overbreadth doctrine does not apply to commercial speech.” *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 496–97 (1982). Even if Plaintiff identifies one particular set of circumstances where the First Amendment might protect businesses’ use of children’s personal information, that would justify an as-applied challenge, not pre-enforcement facial invalidation. *Marquez-Reyes*, 36 F.4th at 1207.

B. AB 2273 Is Not Unconstitutionally Vague

The Act is not void for vagueness. A law is not vague where it “give[s] adequate notice of what conduct is prohibited and sufficient guidelines to prevent arbitrary and discriminatory enforcement.” *IDK*, 836 F.2d at 1197–98. Because the “absence of a significant First Amendment interest is . . . fatal to a facial challenge of a business regulation” unless “[it] is vague in all possible applications[.]” *id.* at 1198, and laws should not be facially invalidated based on the possibility of potential edge cases, *Cal. Teachers*, 271 F.3d at 1155, Plaintiff’s challenge must fail. Although laws that “clearly implicate free speech rights” will “survive a facial challenge so long as it is clear what the statute proscribes in the vast majority of its intended applications[.]” *Humanitarian Law Project v. U.S. Treasury Dep’t (“HLP”)*, 578 F.3d 1133, 1146–47 (9th Cir. 2009), that Plaintiff can hypothesize a way the law might be applied to speech does not mean that the law is subject to a higher standard, *Williams*, 553 U.S. at 305–06. *HLP*, 578 F.3d at 1146–47 (applying all-applications test despite First Amendment claims); *see also Flipside*, 455 U.S. at 495 (same). In any case, “perfect clarity and precise guidance have never been required even of regulations that restrict expressive activity.” *Williams*, 553 U.S. at 307. “The touchstone of a facial vagueness challenge in the First Amendment context, . . ., is not whether *some* amount of legitimate speech will be chilled; it is whether a *substantial* amount of legitimate speech will be

1 chilled.” *Cal. Teachers*, 271 F.3d at 1152. The Act meets that standard.

2 It is well-established that modifiers such as “materially detrimental[,]” “a significant
3 number[,]” or “substantial effect” do not render a statute facially vague. *See Cal. Teachers*, 271
4 F.3d 1152–53 (“overwhelmingly” and “nearly all” are not vague) (citing cases). “Although the[se
5 terms] are not readily translated into a mathematical percentage, the First Amendment does not
6 require them to be.” *Id.* at 1152. Likewise, the “best interest of the child” standard appears in over
7 one hundred California statutes and dozens of federal statutes. It is not suddenly rendered vague
8 here. Nor is “likely to be accessed by children[,]” which is defined by statute, §1798.140(b)(4).
9 *See IDK*, 836 F.2d at 1198 (“terms are narrowly defined in the regulation” so are not vague).
10 Finally, “dark patterns” is a term defined by statute, §1798.140(l), is already regulated by
11 California law, and is commonly used in the tech field. Egelman Decl. ¶ 51; Radesky Decl ¶¶ 53–
12 56, 97. These are “words of common understanding, to which no [regulated party] is a
13 stranger[,]” and thus are not unconstitutionally vague. *Cal. Teachers*, 271 F.3d at 1151–52.

14 Moreover, the dark patterns provision and several other challenged terms are modified by
15 scienter requirements. *See e.g.*, §1798.99.31(b)(1), (7). The Act’s terms must be “read in context
16 with the entire provision[,]” *Hunt*, 638 F.3d at 714, and “[t]he Court has recognized that a scienter
17 requirement may mitigate a law’s vagueness, especially with respect to the adequacy of notice to
18 the complainant that [the] conduct is proscribed.” *Cal. Teachers*, 271 F.3d at 1154 (citing cases).
19 For this reason, Plaintiff’s stated fear that businesses will be unfairly penalized for an unknowing
20 violation of the Act is a red herring. For example, regardless of the child user’s age, if the
21 business did not know or did not have reason to know that its use of children’s data would harm
22 children, then the business is not liable. §1798.99.31(b)(1).

23 As explained above, businesses are not required to estimate children’s ages. They can
24 instead apply the same privacy and data protections to all users. And the concept of regulating
25 based on a consumer’s age is not novel. State, federal, and international law already provide data
26 privacy protections based on age. Similarly, Plaintiff’s argument that they do not understand what
27 makes certain practices “risky” is undermined by their own statements and common sense. As
28 Plaintiff’s declarants’ statements show, some businesses’ policies are more privacy protective

than others and some businesses' data collection practices are more expansive than others. *Compare* Cairella Decl. ¶ 20 with Paolucci Decl. ¶ 3 and Masnick Decl ¶ 10. It is common sense that less protective privacy policies and expansive collection of personal information are more risky, and more protective privacy policies and minimized data collection are less risky. *See Cal. Teachers*, 271 F.3d at 1151 n.8 (considering purpose of statute and common sense); *Holder v. Humanitarian Law Project*, 561 U.S. 1, 32 n.6 (considering common sense and evidence).

Finally, “[f]acial invalidation is, manifestly, strong medicine that has been employed by the Court sparingly and only as a last resort[.]” *Cal. Teachers*, 271 F.3d at 1155, and several other factors here weigh against it. Most of Plaintiff’s members already are or should be in compliance with the provisions challenged here because they are substantially similar to UK law. ICO Decl. ¶¶ 18–23, 65. Guidance from the UK is readily available. *Id.* ¶¶ 35–52. Guidance in the form of best practices and recommendations is forthcoming. §1798.99.32(d). Even after enforcement begins, the Act provides for notice and a cure period, and no penalties can be assessed unless and until a state court finds that a business violated the Act. §1798.99.35. Given the Act’s clear terms and significant protections, Plaintiff’s facial vagueness challenge must fail.

C. AB 2273 Does Not Violate the Dormant Commerce Clause

The Commerce Clause grants Congress the power to regulate commerce among the several States. U.S. Const. art. I, § 8, cl. 3. It has long been interpreted to include “an implicit restraint on state authority[.]” *United Haulers Ass’n v. Oneida-Herkimer Solid Waste Mgmt. Auth.*, 550 U.S. 330, 338 (2007). This “dormant” Commerce Clause “prohibits economic protectionism—that is, regulatory measures designed to benefit in-state economic interests by burdening out-of-state competitors.” *New Energy Co. of Ind. v. Limbach*, 486 U.S. 269, 273 (1988). Here, rather than claiming a discriminatory purpose, Plaintiff alleges only that AB 2273 regulates extraterritorially and that the law’s burden on interstate commerce outweighs its benefits.

1. AB 2273 does not regulate extraterritorially

The dormant Commerce Clause’s prohibition against extraterritorial legislation is narrow. *See, e.g., Pharm. Rsch. & Mfrs. of Am. v. Walsh*, 538 U.S. 644, 669 (2003) (rejecting extraterritoriality challenge where law regulating in-state sales allegedly affected out-of-state

1 transactions). Plaintiff alleges that AB 2273 “applies to *all* operations of a provider that does
 2 business in California,” including out-of-state operations. Pl. Br. 23 (citing cases). Not so. The
 3 Act does not control a provider’s out-of-state operations. It regulates only a “business” that does
 4 business in California, §1798.99.30(a), §1798.140(d), that provides an online service “likely to be
 5 accessed by children,” §1798.99.31(a), who are residents of California §1798.99.30(b)(1),
 6 §1798.99.30(a), (j), §1798.140(i). AB 2273 is thus distinguishable from the California statute
 7 challenged in *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997 (E.D. Cal. 2017), that “d[id] not limit
 8 its application to California,” and as a result, had the effect of controlling conduct occurring
 9 “anywhere in the country.” *Id.* at 1025.

10 In addition—and contrary to Plaintiff’s outdated view of internet technology—“internet
 11 content providers can identify the geographic location of their users and target content based on
 12 the location of the users.” *Nat’l Fed’n of the Blind v. Target Corp.*, 452 F. Supp. 2d 946, 961
 13 (N.D. Cal. 2006). Modern geolocation technology allows a business to tailor its website to
 14 comply with AB 2273’s requirements—and indeed, has been widely-used by businesses to
 15 comply with other California laws for users in California. Egelman Decl. ¶¶ 55–62.

16 Accordingly, the Ninth Circuit rejected a similar dormant Commerce Clause challenge. In
 17 *Greater Los Angeles*, 742 F.3d 414, the Court held that a California law requiring closed
 18 captioning on websites did not regulate extraterritorially because the law “applie[d] only to [the
 19 business’s] videos as they [we]re accessed by California viewers, [and] d[id] not have the
 20 practical effect of directly regulating conduct wholly outside of California.” *Id.* at 433. Because
 21 that law required CNN to modify its website only for California visitors, “leav[ing] the remainder
 22 [of its website] unchanged,” CNN could “avoid the potential for extraterritorial application” of
 23 the law. *Id.* (citing *Nat’l Fed’n of the Blind*, 452 F. Supp. 2d at 961 (rejecting Target’s
 24 extraterritoriality claim because it could make a version of its website for California users)). This
 25 holding applies with equal force here. Plaintiff’s extraterritoriality claim should be rejected.

26 **2. AB 2273 satisfies *Pike* balancing**

27 Under the *Pike* balancing test, laws that “regulate[] even-handedly to effectuate a legitimate
 28 local public interest” will be upheld unless the plaintiff establishes a cognizable burden on

interstate commerce that “is clearly excessive in relation to the putative local benefits.” *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970). Plaintiff alleges that AB 2273 “poses a substantial obstacle to interstate commerce” because it regulates subjects that purportedly require a uniform system of regulation. Pl. Br. 24. The Ninth Circuit rejected that theory in *Greater Los Angeles*, observing that CNN “already serves different versions of its home page depending on the visitor’s country,” and it “provide[d] no explanation for why it could not do the same for California residents.” 742 F.3d at 733. Thus, the supposed “conflicts,” Pl. Br. 24–25, between AB 2273 and other states’ laws do not pose a cognizable burden; any provider’s choice to “self-censor content in all fifty states[,]” *id.* 25, to avoid regulation is not an inevitable consequence of AB 2273. Indeed, if this argument were accepted, few, if any, of the dozens of state laws Plaintiffs identify would survive scrutiny under *Pike*.

Plaintiff also disregards AB 2273’s substantial local benefits. As described above, Arg. I.A.4.b, it is undisputed that “safeguarding physical and psychological well-being of a minor is compelling.” *Ferber*, 458 U.S. at 756–57; *see also* Radesky Decl. ¶¶ 45–85.

None of the burdens Plaintiff alleges clearly exceed these established benefits.

D. AB 2273 Is Not Preempted by Federal Law

The Supremacy Clause “specifies that federal law is supreme in case of a conflict with state law.” *Murphy v. NCAA*, 138 S. Ct. 1461, 1479 (2018). There are “three different types of preemption—conflict, express, and field—but all of them work in the same way: Congress enacts a law that imposes restrictions or confers rights on private actors; a state law confers rights or imposes restrictions that conflict with the federal law; and therefore . . . the state law is preempted.” *Id.* at 1480. Here, Plaintiffs rely on express and conflict preemption theories. “Although express and conflict preemption are analytically distinct inquiries, they effectively collapse into one when”—as here—“the preemption clause uses the term inconsistent.” *Jones v. Google LLC*, 56 F.4th 735, 741 (9th Cir. 2022).

1. COPPA

COPPA sets minimum requirements for businesses that offer online services directed toward children under 13, including requirements to obtain parental consent before collecting,

1 using, or disclosing children’s personal information; provide notice of their privacy policies; and
 2 give parents the ability to review and change their children’s personal information collected by
 3 the operator. 15 U.S.C. §§6501–6506, 16 C.F.R. §§312.1–312.13. Plaintiff contends that because
 4 AB 2273 provides protections that are more expansive than COPPA’s, AB 2273 replaces the
 5 parental control conferred by COPPA with “a host of new and different state-imposed obligations
 6 on services.” Pl. Br. 26.

7 This theory fails. AB 2273 does not—and cannot—replace any of COPPA’s requirements,
 8 which would be in effect regardless of whether the California Legislature had enacted AB 2273.
 9 And, COPPA’s preemption clause only prohibits states from imposing liability that is
 10 “inconsistent with the treatment of those activities or actions under this section.” 15 U.S.C.
 11 §6502(d). “[I]nconsistent” “refers to contradictory state law requirements, or to requirements that
 12 stand as obstacles to federal objectives.” *Jones*, 56 F.4th at 740. “[S]tate laws that supplement, or
 13 require the same thing, as federal law, do not stand[] as an obstacle, to Congress’s objectives, and
 14 so are not inconsistent.” *Id.* at 740–41. COPPA sets minimum requirements for obtaining parental
 15 consent for collection, use, or disclosure of personal information from children under 13, and AB
 16 2273 supplements this by placing additional restrictions on the collection and use of children’s
 17 personal information. *See, e.g.*, §1798.99.31(b)(1). These criteria can apply simultaneously. As
 18 confirmed by the Ninth Circuit, COPPA leaves room for states to enact laws that regulate in a
 19 manner that is consistent with COPPA. *Jones*, 56 F.4th at 741–42. Because AB 2273
 20 compliments, instead of contradicts COPPA, AB 2273 does not fall within the COPPA
 21 preemption clause.

22 Plaintiff also argues that AB 2273 is preempted by COPPA because AB 2273 regulates
 23 platforms likely to be accessed by children under 18, whereas COPPA regulates platforms
 24 directed to children under 13, Pl. Br. 27. This argument assumes that COPPA’s regulation of
 25 platforms directed to a subset of children invalidates state regulation of platforms directed to a
 26 broader set of children, and appears to be based on a field preemption theory. To win on field
 27 preemption claim, Plaintiff must show that “a framework of regulation [is] so pervasive . . . that
 28 Congress left no room for the States to supplement it or [] there is a federal interest . . . so

1 dominant that the federal system will be assumed to preclude enforcement of state laws on the
 2 same subject.” *Arizona v. United States*, 567 U.S. 387, 399 (2012). Plaintiff has cited no case law
 3 establishing that COPPA occupies the field in this manner. To the extent AB 2273 regulates more
 4 platforms or an additional subset of children, it merely supplements—and is not “inconsistent
 5 with”—COPPA. *Jones*, 56 F.4th at 740.

6 **2. Section 230 of the Communications Decency Act**

7 Section 230 of the Communications Decency Act prohibits a “provider or user of an
 8 interactive computer service” from being “treated as the publisher or speaker of any information
 9 provided by another information content provider.” 47 U.S.C. §230(c)(1). It permits enforcement
 10 of “any State law that is consistent with [Section 230]” and prohibits bringing a cause of action or
 11 imposing liability that is “inconsistent[.]” 47 U.S.C. §230 (e)(3). Plaintiff’s preemption theory
 12 here is that AB 2273’s requirements that businesses enforce their own published terms, policies,
 13 and community standards, and AB 2273’s restrictions on the use of minors’ personal information,
 14 are inconsistent with Section 230. Pl. Br. at 28–29. Neither of these theories has any merit.

15 Nothing in Section 230 prevents a State from holding businesses accountable for doing
 16 what they say they are going to do, or preempts the numerous state laws regulating false
 17 advertising or unfair business practices. And binding precedent explicitly holds that Section 230
 18 does not prevent online businesses from being held liable for their own conduct. *See, e.g.*,
 19 *HomeAway.com*, 918 F.3d 676 (rejecting Section 230 immunity for processing rental bookings
 20 posted by others on website); *Fair Hous. Council of San Fernando Valley v. Roommates.com*,
 21 *LLC*, 521 F.3d 1157 (9th Cir. 2008) (rejecting Section 230 immunity for designing website that
 22 facilitates discrimination); *Barnes*, 570 F.3d 1096 (promissory estoppel claim not preempted
 23 given company’s promise to remove fake profiles); *cf. Doe v. Internet Brands, Inc.*, 824 F.3d 846,
 24 852 (9th Cir. 2016) (Section 230 “does not declare a general immunity from liability deriving
 25 from third-party content.”).

26 Likewise, AB 2273’s restrictions on the collection and use of children’s personal
 27 information does not conflict with Section 230. As explained above, Arg.I.A.2, businesses can
 28 continue to publish and provide children access to the content they search for. AB 2273 simply

prevents businesses from using children’s personal information in specified ways. The fact that Plaintiff’s members wish to use that information in connection with decisions about publishing third-party content does not immunize the collection of children’s personal information from any regulation by the States. It is well-established in this circuit that the government can restrict how businesses collect and use consumer data without running afoul of Section 230. *See Roommates.com*, 521 F.3d at 1171 (rejecting Section 230 immunity where “website is designed to force subscribers to divulge” certain personal information). Indeed, COPPA itself places limitations on the collection and use of children’s data; it is implausible that Congress intended for Section 230 to preempt state-law data restrictions similar to those that Congress has itself imposed. AB 2273 is not preempted by Section 230.

II. OTHER INJUNCTION FACTORS WEIGH AGAINST RELIEF

A plaintiff must establish that it will likely suffer irreparable harm if the injunction is not granted. *Winter*, 555 U.S. at 22. As discussed above, Plaintiff has not been deprived of any constitutional right. Because AB 2273 goes into effect on July 1, 2024, any allegation of imminent enforcement fails. §1798.99.31. Plaintiff’s vague and speculative allegations of financial injury are insufficient to support a finding of irreparable harm, *Goldie’s Bookstore, Inc. v. Sup. Ct. of Cal.*, 739 F.2d 466, 472 (9th Cir. 1984), especially given that many of Plaintiff’s members must already comply with a substantially similar UK law, ICO Decl. ¶¶ 18–23, 65.

The balance of equities and the public interest also militate against issuing an injunction. *Nken v. Holder*, 556 U.S. 418, 435 (2009) (factors merge when government is party). It is in the public interest to advance the safety and protection of minors. *See e.g., Ferris*, 891 F.2d at 717; *see generally* Radesky Decl. ¶¶ 45–85 (children’s vulnerability and risks online), ¶¶ 86–103 (efficacy of AB 2273); Egelman Decl. ¶¶ 35–52 (children’s privacy and AB 2273). Further, an injunction would inflict irreparable harm upon California by preventing enforcement of a statute enacted by representatives of the people. *Maryland v. King*, 567 U.S. 1301, 1303 (2012) (Roberts, C.J., in chambers). The balancing weighs sharply against granting the motion.

CONCLUSION

Plaintiff’s motion should be denied.

1 Dated: April 21, 2023

Respectfully submitted,

2 ROB BONTA
3 Attorney General of California
4 ANYA M. BINSACCA
5 Supervising Deputy Attorney General
6 NICOLE KAU
7 Deputy Attorney General

8 /s/ Elizabeth K. Watson
9 ELIZABETH K. WATSON
10 Deputy Attorney General
11 *Attorneys for Defendant*
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

Case Name: *NetChoice, LLC v. Rob Bonta*

Case No. **5:22-cv-08861-BLF**

I hereby certify that on April 21, 2023, I electronically filed the following documents with the Clerk of the Court by using the CM/ECF system:

- **DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION**
- **DECLARATION OF SERGE EGELMAN, PH.D. IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION with Exhibit A**
- **DECLARATION OF EMILY KEANEY, DEPUTY COMMISSIONER OF REGULATORY POLICY FOR THE INFORMATION COMMISSIONER'S OFFICE IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION with Exhibits A to C**
- **DECLARATION OF JENNY S. RADESKY, MD IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION with Exhibit A**

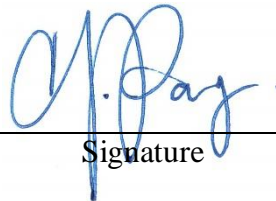
I certify that **all** participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

I declare under penalty of perjury under the laws of the State of California and the United States of America the foregoing is true and correct and that this declaration was executed on April 21, 2023, at San Francisco, California.

G. Pang

Declarant

SA2022305631/43662549.docx



Signature