No. 25-2366

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NETCHOICE, LLC, D/B/A NETCHOICE,

Plaintiff-Appellee,

v.

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

Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California
No. 5:22-cv-08861-BLF
The Honorable Beth Labson Freeman

PLAINTIFF-APPELLEE NETCHOICE'S RESPONSE BRIEF

Adam S. Sieff
DAVIS WRIGHT TREMAINE LLP
350 South Grand Avenue
27th Floor
Los Angeles, CA 90071
(213) 633-6800
adamsieff@dwt.com

Ambika Kumar
Bianca G. Chamusco
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue
Suite 3300
Seattle, WA 98104
(206) 757-8030
ambikakumar@dwt.com
biancachamusco@dwt.com

David M. Gossett
Meenakshi Krishnan
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW
Suite 500 East
Washington, DC 20005
(202) 973-4200
davidgossett@dwt.com
meenakshikrishnan@dwt.com

Robert Corn-Revere
FOUNDATION FOR INDIVIDUAL RIGHTS AND EXPRESSION
700 Pennsylvania Avenue SE
Suite 340
Washington, D.C. 20003
(215) 717-3423 Ext. 209
bob.corn-revere@thefire.org

Attorneys for Plaintiff-Appellee NetChoice, LLC

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Plaintiff-Appellee NetChoice, LLC (NetChoice) states that it has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

Page

CORPORATE DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES v

INTRODUCTION 1

JURISDICTIONAL STATEMENT 3

STATEMENT OF ISSUES 3

STATUTORY AUTHORITIES 4

STATEMENT OF THE CASE 4

A. The internet provides a vibrant forum for speech. 4

B. Preexisting laws protect California children's privacy online. 6

C. California enacts the Age-Appropriate Design Code Act. 8

D. This court affirmed injunction of the DPIA requirements. 12

E. The district court enjoins the rest of the Act. 14

SUMMARY OF ARGUMENT 16

ARGUMENT 18

I. The District Court Correctly Enjoined The Act Under The First Amendment Based On Its Content-Based Coverage Definition. 18

A. The Act burdens speech based on content in every case. 19

B. The State's arguments that the coverage definition does not regulate speech, much less on the basis of content, are baseless. 22

C. No application of the Act survives strict scrutiny. 29

D. The overbreadth standard is satisfied. 36

II. The District Court Correctly Held That The Already Invalidated DPIA Provisions Are Not Severable From The Remainder Of The Act 40

III. The District Court Correctly Enjoined Several Individual Provisions For Independent Reasons. 47

A. The age-estimation mandate violates the First Amendment on its face 47

B. The information-use restrictions are unconstitutionally vague. 53

C. The "dark pattern" restriction is unconstitutionally vague. 58

IV. The Court May Also Affirm On Alternative Grounds. 60

A. The information-use and "dark pattern" restrictions violate the First Amendment to the extent NetChoice challenges them 60

1. Information-use provisions 63

2. "Dark pattern" restriction 66

B. The Act violates the Commerce Clause. 68

C. COPPA preempts the Act 69

D. Section 230 preempts the Act's provisions that regulate how services moderate third-party content. 70

CONCLUSION 71

CIRCUIT RULE 28-2.6 STATEMENT OF RELATED CASES 73

FORM 8. CERTIFICATE OF COMPLIANCE FOR BRIEFS 74

CERTIFICATE OF SERVICE 75

STATUTORY ADDENDUM 76

TABLE OF AUTHORITIES

Page(s)

Cases

Abbott Lab'ys v. Franchise Tax Bd.,
175 Cal. App. 4th 1346 (2009) 43, 45

ACLU v. Mukasey,
534 F.3d 181 (3d Cir. 2008) 54

Acosta v. City of Costa Mesa,
718 F.3d 800 (9th Cir. 2013) 43

Americans for Prosperity Found. v. Bonta,
594 U.S. 595 (2021) ..... *passim*

Arizona Attorneys for Criminal Justice v. Mayes,
127 F.4th 105 (9th Cir. 2025) 62

Ashcroft v. Free Speech Coal.,
535 U.S. 234 (2002) 35

Barlow v. Davis,
72 Cal. App. 4th 1258 (1999) 46

Barnes v. Yahoo!, Inc.,
570 F.3d 1096 (9th Cir. 2009) 71

Barr v. Am. Ass'n of Pol. Consultants,
591 U.S. 610 (2020) 21, 22, 26, 29

Bates v. Pakseresht,
--- F.4th ---, 2025 WL 2079875
(9th Cir. July 24, 2025) ..... *passim*

Bd. of Osteopathic Exam'rs v. Bd. of Med. Exam'rs,
53 Cal. App. 3d 78 (1975) 43, 44

Boos v. Barry,
485 U.S. 312 (1988) 26, 29, 50

Brockett v. Spokane Arcades, Inc.,
472 U.S. 491 (1985) 62, 63

Brown v. Ent. Merchants Ass'n,
564 U.S. at 800 ..... *passim*

Butcher v. Knudsen,
38 F.4th 1163 (9th Cir. 2022) 53

Butler v. Michigan,
352 U.S. 380 (1957) 17, 18, 50

Cal. Redev. Ass'n v. Matosantos,
53 Cal. 4th 231 (2011) 42, 43

Cal. Tchrs. Ass'n v. San Diego Cmty. Coll. Dist.,
28 Cal. 3d 692 (1981) 44

CCIA v. Paxton,
747 F. Supp. 3d 1011 (W.D. Tex. 2024) 20, 71

Child.'s Health Def. v. Meta Platforms, Inc.,
112 F.4th 742 (9th Cir. 2024) 66, 67

Church of Lukumi Babalu Aye, Inc. v. City of Hialeah,
508 U.S. 520 (1993) 48

Citizens United v. FEC,
558 U.S. 310 (2010) 61

City of Austin v. Reagan Nat'l Advertising of Austin, LLC,
596 U.S. 61 (2022) 25

Counterman v. Colorado,
600 U.S. 66 (2023) 54

County of Sonoma v. Super. Ct.,
173 Cal. App. 4th 322 (2009) 40, 41, 43, 45

Doe v. Grindr Inc.,
128 F.4th 1148 (9th Cir. 2025) 70

Flynt v. Bonta,
131 F.4th 918 (9th Cir. 2025) 68

Foti v. City of Menlo Park,
146 F.3d 629 (9th Cir. 1998) 54

Free Speech Coal., Inc. v. Paxton,
145 S. Ct. 2291 (2025) ..... *passim*

Free Speech Coal. v. Reno,
198 F.3d 1083 (9th Cir. 1999), *aff'd*, 535 U.S. 234 (2002) 54

H.K. v. Google LLC,
595 F. Supp. 3d 702 (C.D. Ill. 2022) 69

Herceg v. Hustler Mag., Inc.,
565 F. Supp. 802 (S.D. Tex. 1983) 26

Hill v. Colorado,
530 U.S. 703 (2000) 58

Holder v. Humanitarian L. Project,
561 U.S. 1 (2010) 53

Hubbard v. City of San Diego,
139 F.4th 843 (9th Cir. 2025) 21, 22

In re Matthew B.,
232 Cal. App. 3d 1239 (1991) 57

Int'l Franchise Ass'n, Inc. v. City of Seattle,
803 F.3d 389 (9th Cir. 2015) 24

Isaacson v. Horne,
716 F.3d 1213 (9th Cir. 2013) 61, 71

Jevne v. Super. Ct.,
35 Cal. 4th 935 (2005) 41

John Doe No. 1 v. Reed,
561 U.S. 186 (2010) 61, 63

Jones v. Google LLC,
73 F.4th 636 (9th Cir. 2023) 69, 70

Junior Sports Mags., Inc. v. Bonta,
2025 WL 1863184 (9th Cir. July 7, 2025) 65

Kasler v. Lungren,
72 Cal. Rptr. 2d 260 (Ct. App. 1998),
rev'd on other grounds, 23 Cal. 4th 472 (2000) 40

Kennedy v. Bremerton Sch. Dist.,
597 U.S. 507 (2022) 30, 31

Mahanoy Area Sch. Dist. v. B.L.,
594 U.S. 180 (2021) 33

Make UC a Good Neighbor v. Regents of Univ. of Cal.,
16 Cal. 5th 43 (2024) 44

Matsumoto v. Labrador,
122 F.4th 787 (9th Cir. 2024) 39

McCormack v. Herzog,
788 F.3d 1017 (9th Cir. 2015) 55

McCoy v. Alphabet, Inc.,
2021 WL 405816 (N.D. Cal. Feb. 2, 2021) 7

Mendoza v. California,
149 Cal. App. 4th 1034 (2007) 42

Metromedia, Inc. v. City of San Diego,
32 Cal. 3d 180 (1982) 46

Minneapolis Star & Trib. Co. v. Minn. Comm'r of Rev.,
460 U.S. 575 (1983) 50

Moody v. NetChoice, LLC,
603 U.S. 707 (2024) ..... *passim*

NAACP v. Button,
371 U.S. 415 (1963) 55

Nat'l Pork Producers Council v. Ross,
598 U.S. 356 (2023) 68

NetChoice, LLC v. Bonta,
113 F.4th 1101 (9th Cir. 2024) ..... *passim*

NetChoice, LLC v. Bonta,
--- F. Supp. 3d ---, 2025 WL 1918742
(N.D. Cal. July 11, 2025) 71

NetChoice, LLC v. Bonta,
692 F. Supp. 3d 924 (N.D. Cal. 2023) 12

NetChoice, LLC v. Carr,
2025 WL 1768621 (N.D. Ga. June 26, 2025) 20, 71

NetChoice, LLC v. Fitch,
134 F.4th 799 (5th Cir. 2025) 37

NetChoice, LLC v. Fitch,
2025 WL 1709668 (S.D. Miss. June 18, 2025) 20

NetChoice, LLC v. Griffin,
2025 WL 978607 (W.D. Ark. Mar. 31, 2025) 20

NetChoice, LLC v. Reyes,
748 F. Supp. 3d 1105 (D. Utah 2024) 20

NetChoice, LLC v. Yost,
778 F. Supp. 3d 923 (S.D. Ohio 2025) 20

New Mexico ex rel. Balderas v. Tiny Lab Prods.,
457 F. Supp. 3d 1103 (D.N.M. 2020) 69

O'Kane v. Catuira,
212 Cal. App. 2d 131 (1963) 44

Packingham v. North Carolina,
582 U.S. 98 (2017) 4, 5

People v. Nguyen,
222 Cal. App. 4th 1168 (2014) 40, 43, 46

PETA, Inc. v. N.C. Farm Bureau Fed'n,
60 F.4th 815 (4th Cir. 2023) 63

Planned Parenthood of Cent. N.J. v. Farmer,
220 F.3d 127 (3d Cir. 2000) 57, 58, 59

Porter v. Martinez,
68 F.4th 429 (9th Cir. 2023) 25

Project Veritas Action Fund v. Rollins,
982 F.3d 813 (1st Cir. 2020) 63

Project Veritas v. Schmidt,
125 F.4th 929 (9th Cir. 2025) 25, 26

Quintano v. Mercury Casualty Co.,
11 Cal. 4th 1049 (1995) 45

Reed v. Town of Gilbert,
576 U.S. 155 (2015) ..... *passim*

Reno v. ACLU,
521 U.S. 844 (1997) 4, 52

Riley v. Nat'l Fed'n of the Blind of N.C, Inc.,
487 U.S. 781 (1988) 35

Rubin v. Coors Brewing Co.,
514 U.S. 476 (1995) 32

Sam Francis Found. v. Christies, Inc.,
784 F.3d 1320 (9th Cir. 2015) 68

SEAT v. Paxton,
765 F. Supp. 3d 575 (W.D. Tex. 2025) 20

Smith v. Butterworth,
866 F.2d 1318 (11th Cir. 1989), *aff'd*, 494 U.S. 624 (1990) 63

Snyder v. Phelps,
562 U.S. 443 (2011) 33

Sorrell v. IMS Health Inc.,
564 U.S. 552 (2011) 33, 65

Stahl v. City of St. Louis,
687 F.3d 1038 (8th Cir. 2012) 58, 60

Tschida v. Motl,
924 F.3d 1297 (9th Cir. 2019) 28

Turner Broad. Sys., Inc. v. FCC,
512 U.S. 622 (1994) 29, 38, 39, 51

United States v. Eichman,
496 U.S. 310 (1990) 67

United States v. Grace,
461 U.S. 171 (1983) 63

United States v. Hall,
912 F.3d 1224 (9th Cir. 2019) 55

United States v. O'Brien,
391 U.S. 367 (1968) 24

United States v. Playboy Ent. Grp., Inc.,
529 U.S. 803 (2000) ..... *passim*

United States v. Supreme Ct. of N.M.,
839 F.3d 888 (10th Cir. 2016) 61, 62

United States v. Williams,
553 U.S. 285 (2008) 53

Video Software Dealers Ass'n v. Schwarzenegger,
556 F.3d 950 (9th Cir. 2009), *aff'd*, 564 U.S. 786 (2011) 31, 32

Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.,
455 U.S. 489 (1982) 57

Ward v. Rock Against Racism,
491 U.S. 781 (1989) 29

X Corp. v. Bonta,
116 F.4th 888 (9th Cir. 2024) 31, 39

Yim v. City of Seattle,
63 F.4th 783 (9th Cir. 2023) 32, 34, 52

Constitutional Provisions

United States Constitution

Amend. I ..... *passim*
Art. I, sec. 8 ..... *passim*

California State Constitution

Art. I, § 1 7

Statutes

Children's Online Privacy Protection Act (COPPA),
15 U.S.C. §§ 6501–06 ..... *passim*

§ 6501(4)(B) 7
§ 6502(a)(1) 70
§ 6502(b)(1)(A)(ii) 7
§ 6502(d) 7

Section 230 of the Communications Decency Act,
47 U.S.C. § 230 ..... *passim*

§ 230(a)(1) 5
§ 230(a)(4) 5
§ 230(c)(1) 71

Age Appropriate Design Code Act, AB 2273,
codified at Cal. Civ. Code § 1798.99.28–40 ..... *passim*

§ 1798.99.29 70
§ 1798.99.30 ..... *passim*
§ 1798.99.31(a) ..... *passim*
§ 1798.99.31(b) ..... *passim*
§ 1798.99.32 14
§ 1798.99.35(a) 12
§ 1798.99.35(c) 12
§ 1798.99.40 8

AB 2273, Findings & Decls.

§ 1(a)(7) 10
§ 1(a)(8) 21, 27
§ 1(d) 21, 27, 41
§ 1(e) 21, 27, 41

California Consumer Privacy Act of 2018 (CCPA),
as amended by California Privacy Rights Act of
2020 (CPRA), Cal. Civ. Code § 1798.100 *et seq.* ..... *passim*

§ 1798.100(a)(2) 7
§ 1798.100(b) 7
§ 1798.120(b) 7
§ 1798.120(c) 7
§ 1798.120(d) 7
§ 1798.140(d) 8, 19, 20
§ 1798.140(*l*) 59
§ 1798.140(v)(1) 10
§ 1798.145(a)(7) 68

Regulations

16 C.F.R. § 312.3 7

Other Authorities

Kevin Collier and Angela Yang, *Hackers leak 13,000 user photos and IDs from the Tea app, designed as a women's safe space,* NBC News (July 25, 2025), https://www.nbcnews.com/tech/social-media/tea-app-hacked-13000-photos-leaked-4chan-call-action-rcna221139 51

INTRODUCTION

However well-intentioned it may be, California's Age Appropriate Design Code Act, AB 2273, provides the State with extraordinary power to censor speech on the internet. This Court has already recognized that once—holding that the Act's central Data Protection Impact Assessment (DPIA) mandate "deputizes covered businesses into serving as censors for the State." *NetChoice, LLC v. Bonta*, 113 F.4th 1101, 1109, 1118, 1121 (9th Cir. 2024).[1] Although the Court noted that most of the Act's remaining provisions "do not necessarily impact protected speech in all or even most applications," it rejected the State's primary argument that the Act regulates only "data management practices," not content, and remanded for the district court to perform an assessment under the newly decided *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024). NetChoice amended its claims, and the district court again concluded that the rest of the Act is impermissible. This Court should affirm.

First, as the district court held, application of the Act's substantive provisions hinges on the content that businesses publish, rendering it

[1] The State calls this decision "*NetChoice II*." Br. 11. NetChoice does the same.

subject to strict scrutiny that it does not satisfy. The Act covers only those services "likely to be accessed" by children, a phrase defined by whether children will find content appealing. The State responds that the coverage definition does not regulate speech—but ignores that the definition determines what services are regulated *based on* their speech. Consequently, any application of the Act's subordinate regulatory provisions is subject to strict scrutiny. Under strict scrutiny, those provisions are invalid—and indeed, the State does not even try to satisfy this standard. 1-ER-27.

Second—as the district court also held—the Act's DPIA mandate, which this Court held invalid, is not severable from the remaining substantive provisions. 1-ER-46–51. The Act's text and legislative history show the State would not have adopted the Act without the DPIA provisions, which permit businesses to avoid liability by curing any alleged violations that the Attorney General identifies by removing "harmful" material.

Third, the district court correctly enjoined several specific provisions on independent grounds. The State does not even challenge the court's conclusion that the content policy enforcement mandate

"would burden the business's right to exercise its editorial judgment" and violates the First Amendment. 1-ER-32. The court also held that the age-estimation mandate violates the First Amendment because it restricts access to protected speech, 1-ER-36–39, and that the Act's information-use and "dark pattern" restrictions are invalid because they are unconstitutionally vague, turning on undefined terms including "material detriment," "best interests," and "well-being." 1-ER-41–45; *see NetChoice II*, 113 F.4th at 1120. The State's insistence that these are "clear" establishes anything but.

Finally, the Court may affirm on grounds the district court rejected.

JURISDICTIONAL STATEMENT

NetChoice agrees with the State's jurisdictional statement.

STATEMENT OF ISSUES

1. Whether the district court correctly enjoined all regulatory provisions of the Act collectively because their application hinges on the content that businesses publish and because they fail to satisfy strict scrutiny.

2. Whether the district court correctly held that the already invalidated DPIA provisions are not severable from the remainder of the

Act.

3. Whether the district court correctly enjoined the Act's age-estimation mandate, information-use restrictions, and "dark pattern" restriction on additional First Amendment and vagueness grounds.

4. Whether the Court should affirm the preliminary injunction on the alternative grounds NetChoice raised below.

STATUTORY AUTHORITIES

The State omitted the following statutes from its addendum, which are contained in the addendum to this brief: Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–06; Section 230 of the Communications Decency Act, 47 U.S.C. § 230; and California Consumer Privacy Act of 2018 (CCPA), *as amended by* California Privacy Rights Act of 2020 (CPRA), Cal. Civ. Code § 1798.100 *et seq*. (selected sections).

STATEMENT OF THE CASE

A. The internet provides a vibrant forum for speech.

The internet is a medium "as diverse as human thought[,]" *Reno v. ACLU*, 521 U.S. 844, 870 (1997), which in the brief span of a generation has become indispensable to the exchange of information. "[W]ebsites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard[,]" *Packingham v. North Carolina*,

582 U.S. 98, 107 (2017), allowing individuals to "relate to family and friends, as well as to businesses, civic organizations, and governments." *Moody*, 603 U.S. at 716. This "extraordinary advance in the availability of educational and informational resources" has "flourished, to the benefit of all Americans, with a minimum of government regulation." 47 U.S.C. § 230(a)(1), (4).

Given the "staggering amount of content" on the internet, online services necessarily must "organize uploaded posts in a variety of ways." *Moody*, 603 U.S. at 719. One way of doing so is by tailoring content to users. Suggesting a book or film based on a user's browsing, reading, or listening, for example, creates value to users by personalizing the service and to content creators by connecting them with an audience. *See, e.g.*, 2-SER-492–93 ¶¶ 2–6; 2-SER-507–08 ¶ 8; 2-SER-511 ¶ 20; 2-SER-533–34 ¶ 13.

Online providers interact with users in myriad ways. Most have areas where all users can view content without creating an account. *See, e.g.*, 2-SER-507 ¶ 7; 2-SER-474 ¶ 5; 2-SER-493–94 ¶¶ 7–9. Many have features available only to users who create an account. *See, e.g.*, 2-SER-507–08 ¶ 8; 2-SER-474 ¶ 6; 2-SER-492–93 ¶¶ 7–9; 2-SER-482 ¶ 5. Some

require users to pay subscription fees for extra services. *See, e.g.*, 2-SER-506–07 ¶ 4; 2-SER-482 ¶ 5. Others provide services and content without charge, relying on advertisements to support the content and services they provide. *See, e.g.*, 2-SER-506–07 ¶¶ 4, 7; 2-SER-511 ¶ 21; 2-SER-475 ¶ 9; 2-SER-493–94 ¶¶ 7, 9, 10. As California has conceded, "today's internet would not exist without the digital advertising revenue that, as a practical matter, funds its creation and expansion." Compl. ¶ 1, *United States v. Google LLC*, No. 23-108 (E.D. Va. Jan. 24, 2023), Dkt. No. 1 (complaint filed by California and others).

B. Preexisting laws protect California children's privacy online.

Preexisting federal and state laws regulate the collection and use of minors' personal information online.

At the federal level, COPPA requires websites "directed to children" under 13, or that have "actual knowledge" that a user is a minor, to disclose their information collection, use, and disclosure practices, and to obtain parental consent "for the collection, use, or disclosure of personal

information from children." 15 U.S.C. §§ 6501(4)(B), 6502(b)(1)(A)(ii).[2] COPPA preempts inconsistent child-focused state privacy rules. *Id.* § 6502(d).

California also has a comprehensive state data privacy regime, the 2018 CCPA, which "give[s] consumers of all ages 'an effective way to control their personal information.'" *NetChoice II*, 113 F.4th at 1109 (quotation omitted). As amended in 2020, the CCPA provides users extensive rights to control the data collected about them, and parents the ability to control the data collected from their children. *See* Cal. Civ. Code § 1798.100 *et seq.*[3] The State Constitution and common law also protect children's privacy. Cal. Const. art. I, § 1; *e.g., McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *7–8 (N.D. Cal. Feb. 2, 2021).

---

[2] Websites also must provide parents "reasonable means" to review and refuse consent to the use of a child's personal information, and cannot condition participation in certain activities on excessive disclosure of personal information. 16 C.F.R. § 312.3(a)–(d).

[3] Online services must "inform consumers as to the categories of" and "purposes for which" personal information is being collected, *id.* § 1798.100(b); not collect more information absent notice, *id.* § 1798.100(a)(2); provide notice of any sale or sharing of information, *id.* § 1798.120(b); honor requests not to do so, *id.* § 1798.120(d); and not sell or share the information of a consumer the service knows is younger than 16, absent authorization from that user (or if the user is under 13, their parent or guardian), *id.* § 1798.120(c).

C. California enacts the Age-Appropriate Design Code Act.

California passed the Act in 2022. The Act, "modeled after" the United Kingdom's Age-Appropriate Design Code, 1-SER-229, imposes obligations on certain "business[es]"[4] that "provide[] an online service, product, or feature likely to be accessed" by anyone under age 18. §§ 31(a), (b), 30(b)(1). The law uses content to decide whether a service is "likely to be accessed by children"—focusing on whether the service is "directed to children," § 30(b)(4)(A); offers "advertisements marketed to children," § 30(b)(4)(C); has "design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children," § 30(b)(4)(E); or has an "audience" routinely or largely composed of children (as indicated by specific sources), § 30(b)(4)(B), (F).

The Legislature made the Act's central purpose of regulating content plain through its now-enjoined requirement (not defended here)

[4] A "business" is any for-profit entity that meets certain criteria, including earning more than $25M in gross annual revenue or sharing at least 100,000 customers' information annually. *Id.* § 1798.140(d). The Act exempts non-profits, government entities, medical providers, and online services that provide the "delivery or use of a physical product." *Id.* §§ 30(b)(5)(C), 1798.99.40, 1798.140(d).

that covered businesses prepare DPIAs and mitigate purported harms identified in those DPIAs. Appellant Attorney General Bonta praised the Act for "protect[ing] children from … harmful material" and "dangerous online content." 1-SER-256–58. Likewise, Governor Newsom lauded the law for "protect[ing] kids" from harmful "content." 1-SER-259–60. Further, the State's expert used the word "content" more than 70 times in her declaration to justify the statute, deriding existing laws because they "only" cover data management. 4-ER-592–629. *See NetChoice II*, 113 F.4th (DPIA provisions "chief among [the Act's] mandates").

The Act would have required online businesses to assess and document whether their services "could harm" minors by exposing them to "potentially harmful" content, contacts, or communications; permitting them to "witness" any "potentially harmful conduct"; or using "algorithms" or "automatic" processing to deliver "targeted" content and ads that "could harm" them. § 31(a)(1)(B)(i)–(vii). It also would have required the provider to "create a timed plan to mitigate or eliminate" those risks "before" minors access the service, § 31(a)(2), and to submit DPIAs to the Attorney General on demand, § 31(a)(3).

Despite referring to "data management," these requirements have little to do with protection of data or privacy. *See NetChoice II*, 113 F.4th at 1118 (interpreting Act's references to "data management" and data protection as "proxies for content"). Instead, they proceed from the premise that online services must redesign their *content* to be "appropriate for children." AB 2273, Findings & Decls. § 1(a)(7).

Other subordinate mandates and prohibitions implement this overarching purpose:

Policy-Enforcement Mandate: § 31(a)(9). Services must "enforce" policies, including content policies, to the State's satisfaction.

Information-Use Restrictions: § 31(b)(1)–(4). The Act restricts services' use of minors' "personal information"—defined broadly to include any information "reasonably capable of being associated with, or [that] could reasonably be linked, directly or indirectly, with a particular consumer or household," Cal. Civ. Code § 1798.140(v)(1)—to organize or deliver content:

- Delivering Content: § 31(b)(1). The Act prohibits covered providers from using a minor's personal information (including an IP address and browsing history) to deliver content the provider "knows, or has reason to know, is materially detrimental" to the minor's "well-being."

- Automated Processing of Personal Information (so-called "Profiling"): § 31(b)(2). The Act essentially ends content personalization for minors by restricting services from "analyzing or predicting" the user's "personal preferences [or] interests" using "automated processing." §§ 30(b)(6), 31(b)(2).

- Sharing or Retaining Personal Information: § 31(b)(3). The Act prohibits services from sharing or retaining "personal information" unless "necessary" to provide the service "with which a child is actively and knowingly engaged" or there is a "compelling reason" that doing so "is in the best interests of" minors likely to access the service. § 31(b)(3).

- Use of Personal Information for Additional Reasons: § 31(b)(4). The Act forbids providers from using a minor's "personal information" for "any reason other than a reason for which [it] was collected" unless providers present a "compelling reason" the use is in children's "best interests." § 31(b)(4). Parents are not permitted to opt out of this restriction.

"Dark Pattern" Restriction: § 31(b)(7). The Act prohibits covered providers from using so-called "dark patterns" to "lead or encourage" minors to provide more information than "reasonably expected" or "take any action" the provider should know "is materially detrimental" to the minor's "physical health, mental health, or well-being." § 31(b)(7). The State interprets the term to reach commonplace publishing features that simplify and improve users' ability to access content, such as newsfeed functions that recommend personalized content. 4-ER-610–12 ¶¶ 49, 55; *see NetChoice II*, 113 F.4th at 1123 n.8

("dark patterns may include the 'infinite scroll' feature on X (formerly Twitter)" and "'streaks' on Snapchat").

Age-Estimation Mandate: § 31(a)(5). Online services must estimate the age of ***all*** their users with "a reasonable level of certainty appropriate to the risks" that could arise from their services, or else apply the "protections afforded to children to all consumers." § 31(a)(5). Adults may not opt themselves or their children out of these restrictions. *Id.*

Enforcement: The Act authorizes the Attorney General to obtain penalties of up to $7,500 per "affected child," and injunctive relief. *Id.* § 1798.99.35(a). As enacted, the Attorney General could not have sought penalties without first providing services an opportunity to cure noncompliance. *Id.* § 1798.99.35(c). But that process is not available because it was preliminarily enjoined as a result of the constitutional infirmities in the DPIA requirements, *NetChoice II*, 113 F.4th at 1124.

D. This court affirmed injunction of the DPIA requirements.

The district court granted NetChoice's first motion for a preliminary injunction in September 2023. *NetChoice, LLC v. Bonta*, 692 F. Supp. 3d 924 (N.D. Cal. 2023). This Court affirmed as to the DPIA requirements, holding they "deputiz[ed]" online services into acting as

"censors for the State." The Court reasoned that the DPIA requirement compelled non-commercial speech and was content-based and subject to strict scrutiny in all applications, which the State fell "well short of satisfying." *NetChoice II*, 113 F.4th at 1108, 1113, 1116–22.

This Court remanded the remaining provisions for review under the standard for facial challenges articulated in *Moody*, 603 U.S. 707, which the Supreme Court issued shortly before oral argument. *NetChoice II*, 113 F.4th at 1125–26. *Moody* directed lower courts considering First Amendment facial challenges to assess "[w]hat activities, by what actors" the challenged laws regulate, and whether "a substantial number of [the law's] applications are unconstitutional, judged in relation to [any] plainly legitimate sweep." 603 U.S. at 716–25 (citations omitted).

This Court did not disturb the district court's reasoning that specific applications of the challenged provisions are likely unconstitutional, nor did it reach NetChoice's other claims under Section 230, COPPA, and the Commerce Clause, U.S. Const., Art. I, sec. 8. *NetChoice II*, 113 F.4th at 1126 n.9. It also concluded that it was premature to consider whether the DPIA requirements were severable before completing the *Moody* analysis. *Id.* at 1124–25.

E. The district court enjoins the rest of the Act.

NetChoice filed an Amended Complaint clarifying the scope of its challenges and the specific relief sought. 1-SER-167–69 ¶¶ 84–90; 1-SER-175–77 ¶¶ 1–13. NetChoice challenged on a facial basis all the regulatory provisions in § 31(a)–(b) because the Act's content-based coverage definition renders the requirements unconstitutional in every application. 1-SER-175 ¶ 2. NetChoice also brought facial challenges to the individual provisions listed on pages 10-12, *supra*, as well as the already-enjoined DPIA provisions (§ 31(a)(1)–(4)), for violating the First Amendment—and in the alternative, as-applied challenges for NetChoice's members. 1-SER-176 ¶¶ 3–8. Finally, NetChoice sought facial relief from § 31(a)–(b) on the ground that they are not severable from the already-enjoined DPIA provisions, 1-SER-176 ¶ 9; and facial and as-applied relief under the Commerce Clause, COPPA, and Section 230, 1-SER-177 ¶¶ 10–12.[5]

NetChoice then filed a second motion for a preliminary injunction, 3-ER-527–66, which the district court granted, 1-ER-2–57. The court held that because the Act only covers "[b]usinesses that provide online

[5] NetChoice did not challenge the working group provisions in § 32.

services, products, or features 'likely to be accessed by children'" it is a content-based regulation subject to strict scrutiny. 1-ER-13–16; 1-ER-21. Applying strict scrutiny, the court found the State failed to meet its burden of proving that § 31(a)–(b) serve a compelling state interest and are narrowly tailored in any application. 1-ER-24–27.

The district court also considered NetChoice's challenges to individual provisions. The court held that the age-estimation mandate, § 31(a)(5), "impose[s] the same barriers to speech on all covered businesses and their audiences" in every case and "has no legitimate sweep," and thus is facially invalid. 1-ER-39. It enjoined the information-use, § 31(b)(1)–(4), and "dark pattern," § 31(b)(7), provisions on vagueness grounds—noting that both turn on "terms [that] have no established meaning." 1-ER-41–45. And it held that the policy-enforcement mandate, § 31(a)(9), violates the First Amendment on its face to the extent it compels covered businesses to moderate user-generated content in ways that satisfy the government, 1-ER-31–33. The district court also concluded that the enjoined central reporting DPIA provisions are not volitionally severable from the remainder of the Act.

1-ER-51. The district court declined to enjoin the Act on COPPA, Section 230, or Dormant Commerce Clause grounds. 1-ER-52–55.

This appeal followed. 4-ER-630–32. The State does not renew its defense of the Act's DPIA requirements or associated notice-and-cure provision; does not challenge the district court's injunction of § 31(a)(9)'s policy enforcement mandate; and does not address any *Winters* factor except likelihood of success. *See* 1-ER-10 ("State effectively concede[d] the other three *Winter* factors" below).

SUMMARY OF ARGUMENT

The Court should affirm the preliminary injunction of the Act's regulatory provisions, § 31(a)–(b).

I. The district court correctly enjoined these provisions based on the Act's content-based coverage definition. Because the Act defines who is regulated based on whether they publish subject matter likely to interest children, the Act's regulatory provisions burden speech based on its content in the same way, in every application, and are subject to strict scrutiny. The State cannot show that any of these provisions satisfies strict scrutiny, and thus the district court correctly held them overbroad and facially invalid.

II. The district court also correctly enjoined § 31(a)–(b) as facially invalid because these regulatory provisions are not severable from the Act's central, already-enjoined DPIA provisions. The DPIA provisions would have allowed businesses to avoid liability by self-identifying and removing or deprioritizing content that might later be deemed "harmful" to kids, and by obeying orders from the Attorney General to "cure" any purported violations of the Act. The text and legislative history show the State would not have adopted the Act without these provisions. And these mechanisms, albeit unconstitutional, were integral to the Act's standards- and compliance-oriented approach, which would have permitted covered businesses to avoid crippling penalties arising from surprise enforcement.

III. The district court's injunction of several individual regulatory provisions on alternative bases were also appropriate. As the court held, the age-estimation mandate, § 31(a)(5), is independently invalid on its face because forcing adults and minors to verify their ages to access fully protected speech, or else requiring services to self-censor fully protected speech to meet government-imposed age-appropriateness standards, triggers and fails strict scrutiny in every instance. *See Butler v.*

Michigan, 352 U.S. 380, 383 (1957) (state cannot "reduce the adult population … to reading only what is fit for children"). And the information-use restrictions, § 31(b)(1)–(4), and "dark pattern" restriction, § 31(b)(7), are facially invalid because they rest upon vague, undefined terms like "material detriment," "best interests," and "well-being" that invite arbitrary and subjective censorship.

IV. The Court may also affirm the district court's injunction because the information-use and "dark pattern" restrictions facially violate the First Amendment in specific applications to protected publishing activities; the Act violates the Commerce Clause; and the Act is preempted by COPPA and in part by Section 230.

ARGUMENT

I. The District Court Correctly Enjoined The Act Under The First Amendment Based On Its Content-Based Coverage Definition.

As the district court correctly held, the Act is subject to strict scrutiny because, due to the coverage definition, it applies only to businesses that publish certain content. Where—as here—a law regulates speech or its dissemination because of its content, the law is "presumptively unconstitutional." *Reed v. Town of Gilbert*, 576 U.S. 155,

163, 169 (2015). The government "bears the burden of proving" the law is necessary to serve a compelling interest and is the least restrictive means of serving that interest. *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 816 (2000). The State cannot meet that burden.

The State disputes that the Act's coverage definition regulates speech at all, Br. 19–24; claims that if it does, that definition is not content-based and thus does not trigger strict scrutiny, Br. 24–33; and argues that even if strict scrutiny applies, the Act survives such scrutiny, Br. 33–38. None of these arguments has merit.

A. The Act burdens speech based on content in every case.

The district court correctly held that the regulatory requirements are all subject to strict scrutiny because the Act—by virtue of its content-based coverage definition—burdens speech based on content in *every* application. 1-ER-12–28.

Under this coverage definition, if an online service publishes information "directed to" minors—such as "games," "cartoons," "music," "celebrities," "advertisements," or "design elements" that "appeal to" minors—that service must comply with the Act. § 30(b)(4)(A)–(F); Cal. Civ. Code § 1798.140(d). If the service has a significant audience of, or

"audience composition" comprised of, minors—which will turn in significant measure on the service's content—it too is regulated. *Id.* By contrast, if a service publishes content that has no appeal to minors or caters to an "audience" that does not include a significant number of minors, it is not subject to regulation.

The Act's coverage definition runs headlong into the rule that the government "has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *Reed*, 576 U.S. at 163 (citation omitted). Because the Act "defin[es] regulated speech by particular subject matter," and thus "singles out specific subject matter for differential treatment," *id.* at 163, 169, its every application is subject to strict scrutiny, 1-ER-14–21.[6]

The Act is analogous to the sign ordinance in *Reed*, which was content-based and subject to strict scrutiny because it differentiated

[6] The decision joins seven other courts' holdings that similar coverage definitions require strict scrutiny. *See NetChoice, LLC v. Carr*, 2025 WL 1768621, at *12 (N.D. Ga. June 26, 2025); *NetChoice, LLC v. Fitch*, 2025 WL 1709668, at *8 (S.D. Miss. June 18, 2025); *NetChoice, LLC v. Yost*, 778 F. Supp. 3d 923, 953–54 (S.D. Ohio 2025); *SEAT v. Paxton*, 765 F. Supp. 3d 575, 594 (W.D. Tex. 2025); *NetChoice, LLC v. Griffin*, 2025 WL 978607, at *9–10 (W.D. Ark. Mar. 31, 2025); *CCIA v. Paxton*, 747 F. Supp. 3d 1011, 1032–34 (W.D. Tex. 2024); *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105, 1121–24 (D. Utah 2024).

based on whether a sign's subject matter was political, ideological, or directional. 576 U.S. at 165–71. It is also akin to the content-based law that restricted automated robocalls unless the subject matter of a robocall involved the collection of a government debt. *See Barr v. Am. Ass'n of Pol. Consultants*, 591 U.S. 610, 618–21 (2020) (plurality op.). And it is comparable to a law that "permits the teaching of subjects such as tai chi and Shakespeare at shoreline parks and beaches," but restricts "the teaching of yoga." *Hubbard v. City of San Diego*, 139 F.4th 843, 851 (9th Cir. 2025).

It does not matter if—as the State maintains—"[t]he word 'content' nowhere appears in the definitional provision," Br. 32, because online businesses are regulated or not based on the type of subject matter they publish. And even if the Act's coverage were not defined explicitly by content-based criteria, its "purpose" confirms that it is content-based. *Reed*, 576 U.S. at 165 (quotation omitted). Censorship is the Act's avowed and obvious objective, AB 2273, Findings & Decls. § 1(a)(8), (d), (e); 1-SER-31–58; 1-SER-227; 1-SER-229; 1-SER-248–49; 1-SER-258; 1-SER-260, and that unconstitutional aim is built into the Act's applicability.

B. The State's arguments that the coverage definition does not regulate speech, much less on the basis of content, are baseless.

The State's arguments to evade strict scrutiny are makeweight.

First, the State argues that the coverage definition "does not regulate anything" by itself and does not "implicat[e] protected expression." Br. 19–23 (citation omitted). But the Act imposes the substantive obligations in § 31(a)–(b) *based on* whether a service publishes certain subject matter under § 30(b)(4), so the coverage definition renders each of those obligations content-based. The law in *Barr* worked the same way: The statute, which regulated robocalling, excluded calls "made solely to collect a debt owed to … the United States." 591 U.S. at 616. That coverage definition did not "regulate anything," Br. 20, either—but, like the Act, defined what activities, by what actors, were subject to regulation. Accordingly, it rendered the law's regulation content-based. *Barr*, 591 U.S. at 618–21; *see Hubbard*, 139 F.4th at 851.

The State also contends the coverage definition does not "inevitably single[] out entities engaged in expressive activity," since minors "are capable of using ride sharing service[s]," "electronic ticketing services," "financial transaction services," fitness apps, "health-related services,"

and "gambling website[s]" that do not predominantly engage in expression. Br. 20–22. But the Act does not ask whether minors "are capable of using" some service. It asks whether the service is "likely to be accessed" by minors pursuant to content-based indicia defined by the law. This is indisputable as to most all of those indicia—such as whether the services are "directed" to children, § 30(b)(4)(A); "marketed to children," § 30(b)(4)(C); or publish content that "appeal to" minors like "games," "cartoons," "music," and "celebrities." § 30(b)(4)(E). And the remaining criteria focus on online services that have an "*audience*," § 30(b)(4)(B), (F) (emphasis added)— a term not ordinarily used for services like Uber or Venmo that do not publish content.

This makes sense, as the services the State speculates minors "could use" have nothing to do with California's asserted interest in protecting minors from allegedly harmful online content: No one has ever suggested that young people suffer from depression, eating disorders, or sleep deprivation because they might use Venmo, Lyft, or StubHub. Thus, while some minors might occasionally *use* such services, they are

not services "likely to be accessed by children" within the meaning of the Act.[7]

The State's example of a hypothetical "gambling website that uses characters from children's cartoons," Br. 22, backfires. The Act would apply to such a website under § 30(b)(4)(E) because of the presence of those cartoons, so it is not the gambling but *the cartoons*—speech with a particular subject matter—that "dr[aws] the legal remedy." *Int'l Franchise Ass'n, Inc. v. City of Seattle*, 803 F.3d 389, 408 (9th Cir. 2015) (Br. 20, 22). That is a regulation of speech based on its content. *Cf. United States v. O'Brien*, 391 U.S. 367, 376–77 (1968) (law against burning draft cards was content neutral as it was destruction of government property, not the expressive significance of that act, that drew legal remedy).

Second, the State claims that even if the coverage definition implicates expressive activity, the Act's definitions are not content-based and do not subject the entire Act to strict scrutiny. Br. 24–33. This misreads the governing case law, is inconsistent with the language and intent of the Act, and ignores the State's own evidence.

[7] Even if such services somehow fell within the coverage definition, that inclusion would do nothing to change the content-based focus of the Act's coverage definition.

Starting with the law: As the district court concluded, *City of Austin v. Reagan National Advertising of Austin, LLC*, 596 U.S. 61 (2022), and *Porter v. Martinez*, 68 F.4th 429 (9th Cir. 2023), demonstrate that the coverage definition is content-based. *See* 1-ER-16–18; *contra* Br. 24, 27–28. *City of Austin* involved an ordinance regulating advertisements differently depending on whether the goods were sold "on-premises." 596 U.S. at 73–74. The ordinance discriminated based on *where* the goods were sold, *not* "the topic discussed or the idea or message expressed," rendering strict scrutiny inapplicable. *Id.* Similarly in *Porter*, the application of a law regulating honking hinged on "traffic circumstances," not "the 'content' of the honk." 68 F.4th at 441–42. Both cases, however, confirmed that laws "singl[ing] out specific subject matter for differential treatment"—like the sign ordinance in *Reed* and the Act here—demand strict scrutiny. *City of Austin*, 596 U.S. at 69; *Porter*, 68 F.4th at 442–43.

Likewise, *Project Veritas v. Schmidt*, 125 F.4th 929 (9th Cir. 2025), Br. 25, 28, does not help the State. That case held only that a statute prohibiting secret recordings of conversations was content-neutral even though it exempted the *open* recording of conversations involving police officers. *Id.* at 937. Since the statute still prohibited *secret* recordings of

police, it did not exempt recording police as a subject matter and thus did not regulate on the basis of content. 1-ER-17. No part of that holding would have allowed the state to escape strict scrutiny if it passed a law prohibiting recordings only about "cartoons," "celebrities," or "topics likely to interest children." *See Barr*, 591 U.S. at 618–21.

Turning to the language of the Act: The State focuses on the fact that the Act describes its coverage scheme in terms of the *audience* a business serves, instead of the content it publishes. Br. 25–26. In fact, the Act's focus on "audience," § 30(b)(4)(B), underscores its content basis because a regulation based on "concern for [speech's] effect" on a particular audience is "the essence of content-based regulation." *Playboy*, 529 U.S. at 811–12; *see also Boos v. Barry,* 485 U.S. 312, 321 (1988) (laws "focus[ed] on the direct impact of speech on its audience" are content based); 1-ER-18 (same). The State's example of an attractive nuisance, Br. 29, makes this plain: What makes an online business "attractive" to children and thus regulable under the Act is *the information* it carries. "No court has held that the written word is … an attractive nuisance." *Herceg v. Hustler Mag., Inc.*, 565 F. Supp. 802, 803 (S.D. Tex. 1983).

That tracks because the language of the Act demonstrates that content regulation "is a central and assertedly imperative feature" of it. *Bates v. Pakseresht*, --- F.4th ---, 2025 WL 2079875, at *7, *9, *11 (9th Cir. July 24, 2025) (enjoining law that also required speakers to prioritize "speech that promotes the state's conceptions" of a "child's best interest," while restricting "speech that contradicts the state's views"). The Act's stated intent is to prevent services from "offer[ing] detrimental material," AB 2273, Findings & Decls. § 1(a)(8); and the "data management practices" it regulates, § 31(a)(1)(B)(i)–(vii), are content-based. *See supra* page 10. Statements of the law's purpose by the Act's sponsor, the Governor, and the Attorney General confirm this content focus, 1-SER-227; 1-SER-229; 1-SER-248–49; 1-SER-258; 1-SER-260; as does this Court's conclusion that the State's asserted privacy interests are "proxies for content." *NetChoice II*, 113 F.4th at 1118, 1121.[8]

[8] It is also apparent from the Act's incorporation of mandatory guidance from the materially identical British law—unrestrained by the First Amendment—that overtly regulates on the basis of content. *See* AB 2273, Findings & Decls. § 1(d), (e); 1-SER-31–58.

Finally, the State's own evidence: The State and its witnesses focus exclusively on types of content the State views as harmful,[9] highlighting that the Act's coverage definition is a threshold inquiry designed to restrict children's access to such content. The State thus undermines its legal argument by asserting that "the Act is about protecting children" and their "privacy" from online harms, Br. 33, 53—as those harms amount to concern that the *ideas and information* available online are too interesting, *id.* at 4–6, that kids will spend too much time engaging with them, 3-ER-489–95 ¶¶ 80–101; 4-ER-610–11 ¶¶ 49–52, and that this "exposure" is not in their best interests, Br. 6–7.

Laws "justified by a concern that stems from the direct communicative impact of speech" are content-based and subject to strict scrutiny. *Tschida v. Motl*, 924 F.3d 1297, 1303 (9th Cir. 2019) (quotation

[9] *See* 4-ER 599 ¶ 22; 4-ER-603–05 ¶¶ 34–41; 4-ER-609–10 ¶¶ 48, 50; 4-ER-613-18 ¶¶ 60–62, 65, 67, 69–72; 4-ER-624–26 ¶¶ 96, 98 (invoking protection from specified content as justification); 3-ER-467–67 ¶¶ 3, 5 (Act targets harms from "media use," "educational content/interactive design," "advertising," "games," "video-sharing platforms like YouTube," and "interactive media"); 3-ER-471–74 ¶¶ 24–26, 29–31; 3-ER-478 ¶ 43; 3-ER-485–87 ¶¶ 70–75 (Act targets speech involving "hate and discrimination," "violation of dignity," "problematic/excessive social media use," "bullying/harassment," "negative social media content," "offensive name-calling," "false rumors," "negative things," "explicit images," and age-inappropriate "advertisements"); *see* Br. 4–6.

omitted); *see Playboy*, 529 U.S. at 811–12; *Boos*, 485 U.S. at 321. As in *Bates*, this "regulation of speech cannot be described as incidental[,]" since it is clear that "it is the regulation of speech that predominates." 2025 WL 2079875, at *11. That the Act's coverage definition *also* draws facial content-based distinctions only makes it worse. *Reed*, 576 U.S. at 166–67 (distinguishing *Ward v. Rock Against Racism*, 491 U.S. 781 (1989)).

In sum, the Act's coverage scheme triggers regulation based on dissemination of subject matter that bears indicia of attracting minors, so it follows that any application of the Act's substantive regulations burdens services based on the content they carry. *Barr*, 591 U.S. at 619. The Act's definitional core is therefore constitutionally tainted, and that poisoned root infects the entire regulatory scheme. *See Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994) (strict scrutiny applies "to regulations that suppress, disadvantage, or impose differential burdens upon speech because of its content").

C. No application of the Act survives strict scrutiny.

The State's claim (Br. 33–38) that the Act's regulatory provisions, § 31(a)–(b), can withstand strict scrutiny is unpersuasive.

Laws subject to strict scrutiny are "presumptively invalid." *Playboy*, 529 U.S. at 817. Because strict scrutiny "enforce[s] 'the fundamental principle that governments have no power to restrict expression because of its message, its ideas, its subject matter, or its content,'" it "is fatal in fact absent truly extraordinary circumstances." *Free Speech Coal., Inc. v. Paxton*, 145 S. Ct. 2291, 2310 (2025) (citation omitted). To satisfy strict scrutiny, the government must show that a law "furthers a compelling governmental interest and is narrowly tailored to that end." *Reed*, 576 U.S. at 171. "If a less restrictive alternative would serve the [g]overnment's purpose, the legislature must use that alternative." *Playboy*, 529 U.S. at 813.

The State makes no effort to show that any application of the Act's substantive provisions satisfies any level of First Amendment review. It argues the district court could not possibly apply strict scrutiny adequately without evaluating each substantive regulation, Br. 34–35, but ignores that it was *the State's burden* to mount such individualized defenses. *See Kennedy v. Bremerton Sch. Dist.*, 597 U.S. 507, 524, 532 (2022) (once a plaintiff demonstrates an abridgement of speech, "the focus then shifts to the defendant to show that its actions were nonetheless

justified and tailored consistent with the demands of our case law"); *Playboy*, 529 U.S. at 817. It never did. 1-ER-24 ("The State does not even attempt to satisfy strict scrutiny."). The district court granted the injunction on the basis of that failure, *id.* and this Court can and should affirm on the same basis. *See X Corp. v. Bonta*, 116 F.4th 888, 903 (9th Cir. 2024) (remanding to enter injunction because of state's failure to address strict scrutiny).

The district court also—in the alternative and "[f]or the sake of completeness"—performed the strict scrutiny analysis anyway, and held that the regulations failed it collectively or individually. 1-ER-24–28. That determination, too, was correct.

No compelling interest. "[W]hen the government seeks to restrict speech" to protect minors, "it must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way." *Video Software Dealers Ass'n v. Schwarzenegger*, 556 F.3d 950, 962 (9th Cir. 2009), *aff'd*, 564 U.S. 786 (2011). Here, the State has not shown the maladies it seeks to address with § 31(a)–(b)'s substantive provisions—such as depression, anxiety, disrupted sleep, poor academic performance, sedentary habits,

and hurt feelings, 3-ER-471–73 ¶¶ 23–27, 29–30; 3-ER-478 ¶ 43—are caused by online services, much less those online services "likely to be accessed by children," § 30(b)(4). *See* 1-SER-130–42 ¶¶ 10–40; 1-SER-10–19 ¶¶ 22–47.[10]

The State also does not show how any of the substantive regulations in § 31(a)–(b)—collectively or individually—"will in fact alleviate" any targeted harm. *Video Software Dealers Ass'n*, 556 F.3d at 962. To the contrary, NetChoice's expert presented research demonstrating that these provisions will more likely have the *opposite* effect: violating young people's privacy, damaging their mental health, and harming their well-being. 1-SER-10–19 ¶¶ 22–47; 1-SER-22–26 ¶¶ 55–69; 1-SER-28 ¶¶ 80–81. A law that undercuts its stated aims cannot survive any level of First Amendment review. *Yim v. City of Seattle*, 63 F.4th 783, 794 (9th Cir. 2023) (citing *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 489 (1995)).

[10] As before, Dr. Radesky's testimony also "do[es] not prove" that online speech "cause[s]" these harms, but "at best" shows "some correlation" between "exposure" and small "effects." *Brown,* 564 U.S. at 800–01; 4-ER-610 ¶ 50. And while Dr. Radesky claimed (3-ER-480 ¶ 52; 3-ER-494 ¶ 96) to have discovered the requisite "causal link," *Brown*, 564 U.S. at 800, to poorer mental health on remand, the new studies are correlational, 3-ER-480 ¶ 52 nn.51–52, and methodologically flawed, 1-SER-7–10 ¶¶ 10–21; 1-SER-25–26 ¶¶ 65–69.

Without evidence connecting § 31(a)–(b) to any potentially compelling interests, simply preventing teens from spending too much time engaging with information and expression online is not a legitimate government interest. Minors have First Amendment rights to engage in speech that is not obscene for them. *Brown*, 564 U.S. at 794–95. "That the State finds expression too persuasive," or "catchy," for young people "does not permit it to quiet the speech or to burden its messengers." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 578 (2011); *see Brown*, 564 U.S. at 798 (speech not less protected because it is engaging).

Nor may the State abridge minors' access to protected speech believing it may distress some audiences. *See Mahanoy Area Sch. Dist. v. B.L.*, 594 U.S. 180, 185, 190–91 (2021) (profane criticism protected despite upsetting classmates); *Snyder v. Phelps*, 562 U.S. 443, 450–51, 458 (2011). The government's "general conception of [a] child's best interest does not create a force field against the valid operation of other constitutional rights," or automatically justify any policy enacted "to promote children's safety and wellbeing." *Bates*, 2025 WL 2079875, at *7, *9. These are decisions for families to make, not the government.

No narrow tailoring. The State also has not shown that any of the Act's regulations are the least speech-restrictive alternative. *Playboy*, 529 U.S. at 813; *Yim*, 63 F.4th at 793–94.

First, the regulations in § 31(a)–(b) are not limited to speech unprotected by the First Amendment, such as child sexual abuse material (CSAM), speech promoting illegal drugs and gambling, or deceptive advertising. *Cf.* 3-ER-483–87 ¶¶ 63–67, 69, 71–75; 3-ER-497–98 ¶¶ 106–107(a)–(c). Rather, these provisions regulate any "materially detrimental" information that is not "in the best interests of children." § 31(a), (b); *see* 1-ER-26. According to the State, this includes any speech that extends minors' time online, 3-ER-472 ¶¶ 25–27; 3-ER-478–80 ¶¶ 43–52; 3-ER-488–96 ¶¶ 78–101; 3-ER-497-99 ¶ 107(d); promotes "negative social comparison" and "content," 3-ER-472 ¶¶ 25–26; 3-ER-473 ¶ 29; 3-ER-480–81 ¶ 53; involves "name-calling," "negative things," or "risky, shocking, or attention-grabbing posts," 3-ER-473–74 ¶¶ 30–31 ; 3-ER-484 ¶ 64; or exposes minors to "marketing" and "advertising" that is not "age-appropriate," 3-ER-477–78 ¶ 42; 3-ER-485 ¶ 70; 3-ER-4878 ¶ 75. Such speech is constitutionally protected. *Brown*, 564 U.S. at 794. And the State's alternate argument that fully protected speech may be

regulated to shield minors from illegal conduct like "sexual exploitation" or "grooming," 3-ER-474–75 ¶¶ 32–36; 3-ER-484 ¶ 63, "turns the First Amendment upside down." *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 255 (2002).

Second, the State could accomplish its goals by enforcing existing laws, including COPPA, the CPRA, and laws governing CSAM, sexual abuse, deceptive advertising, and gambling. Although the State asserts these laws are not adequately enforced, 2-SER-367–68 ¶¶ 37–40; 4-ER-601–05 ¶¶ 30–39; 3-ER-477–78 ¶ 42, a law is not tailored when "the State may vigorously enforce" less-restrictive rules. *Riley v. Nat'l Fed'n of the Blind of N.C, Inc.*, 487 U.S. 781, 800 (1988); *see NetChoice II*, 113 F.4th at 1121 (DPIA requirement invalid partially because State could have "rel[ied] on existing criminal laws that prohibit related unlawful conduct").

Third, the law's substantive regulations are not the least restrictive means to address even the Act's real but illegitimate purpose. The Act applies a one-size-fits-all instead of a "household-by-household" approach. *Playboy*, 529 U.S. at 816, 818, 823. Dr. Radesky admits many services provide parents tools to limit access to "age-appropriate video

content." 4-ER-624–26 ¶ 96(d). The State does not explain why it did not "employ[] less restrictive means," such as by "incentivizing companies to offer voluntary content filters or application blockers" or "educating children and parents" on such tools. *See NetChoice II*, 113 F.4th at 1121.

D. The overbreadth standard is satisfied.

The State also defends against NetChoice's coverage-definition challenge on the ground that, as a result of *Moody*, facial relief is unavailable unless NetChoice identifies every single website, feature, and function burdened by the Act. Br. 33–38. This misreads *Moody*.

First Amendment facial challenges are subject to a "less demanding" standard to "provide breathing room for free expression." *Moody*, 603 U.S. at 723. A speech regulation is facially invalid if even "a substantial number of [its] applications are unconstitutional, judged in relation to [its] plainly legitimate sweep." *Id.* (citation omitted).

Moody described this longstanding test as a two-step process. Courts first determine a challenged law's "full range of applications" (i.e., does it regulate speech in some, most, or all cases). *Id.* at 726. They next decide which of the laws' applications to speech "violate the First Amendment," and compare the constitutional and unconstitutional

applications. *Id.* at 725. When the pertinent facts "are the same across the board" and the substantial effect of a law is to regulate protected speech without constitutional justification, the law is facially invalid. *Americans for Prosperity Found. v. Bonta*, 594 U.S. 595, 618–19 (2021).

Facial relief is the natural remedy here, and the district court properly applied *Moody* to hold that, because of the coverage definition, the regulatory provisions in § 31(a)–(b) are facially invalid. Unlike the district court in *NetChoice, LLC v. Fitch*, 134 F.4th 799, 809 (5th Cir. 2025) (Br. 36–38)—which released its decision only hours after the Supreme Court decided *Moody*, and "understandably" had not applied a full *Moody*-informed analysis—the decision below canvassed the Act's applications to covered businesses; determined that the Act's coverage definition meant "*all* applications" of the Act's regulatory provisions necessarily regulate speech on a content-basis; concluded the provisions were thus subject to strict scrutiny; and held that the State failed to carry its burden to show that any of the regulations had any "constitutionally permissible application" satisfying that standard. 1-ER-24; 1-ER-27. Since the Act's "every application to a covered business" thus violated the

First Amendment, 1-ER-27 (citation omitted), the court held the regulations in § 31(a)–(b) invalid on their face.

That analysis is correct. At *Moody*'s first step, regulating a business because it publishes a certain type of content garnering a certain audience inherently regulates those businesses' speech. *See Playboy*, 529 U.S. at 811–12. Sections 31(a)–(b) do so because of the coverage definition. Thus, unlike the statutes in *Moody*—where the evidence did not show that every potentially covered entity actually engaged in protected editorial activity that could be unconstitutionally restricted in the first place, 603 U.S. at 726—the Act's provisions apply by definition to services engaged in specific publishing activity, and therefore regulate speech "in every case." *Americans for Prosperity*, 594 U.S. at 618.

The question at step two is which applications are unconstitutional, which are constitutional, and how those compare. *Every* application of the Act's regulatory provisions is unconstitutional. Under any level of First Amendment review, and in any application to protected speech, the State must show that these provisions materially advance a solution to a real problem. *See Brown*, 564 U.S. at 799–800; *Turner*, 512 U.S. at 662–64. The State has provided no evidence that carries its burden. Likewise,

whether under intermediate or strict scrutiny, the State must show that these requirements are sufficiently tailored. *Playboy*, 529 U.S. at 813, 816–17; *Turner*, 512 U.S. at 662–64. The State cannot satisfy that obligation, either, since the Act indisputably regulates more protected speech than necessary to protect minors from the kinds of illegal exploitation and unprotected obscenity the State is permitted to regulate.

NetChoice need not identify every single website, feature, and function burdened by the Act. Br. 35–38. First Amendment facial challenges have never required such a granular census. *See Matsumoto v. Labrador*, 122 F.4th 787, 814–15 (9th Cir. 2024) (finding it "not difficult to conclude" that a law was overbroad under *Moody* when a handful of examples showed it could "realistically be applied to … a substantial amount of protected speech"). Facial relief is available whenever challenged "provisions raise the same First Amendment issues for every covered" website. *X Corp.*, 116 F.4th at 899.

This Court thus enjoined the Act's central DPIA requirement because "in every application to a covered business, [it] raises the same First Amendment issues." *NetChoice II*, 113 F.4th at 1116. So too here: All the Act's regulatory provisions are subject to strict scrutiny because

the coverage definition selectively burdens online businesses based on the content they publish. Because strict scrutiny applies in every case, and because the State has not carried *its burden* to prove that any of the Act's regulations survive that scrutiny, the Act flunks the same First Amendment analysis in every case.

II. The District Court Correctly Held That The Already Invalidated DPIA Provisions Are Not Severable From The Remainder Of The Act.

Sections 31(a)–(b) are also invalid because they cannot survive without the DPIA provisions. Under California law, invalid language can be excised under the "volitional severability" test only if the party seeking severance can show that the remaining provisions "would have been adopted by the legislative body had [it] foreseen" the statute's partial invalidation. *People v. Nguyen*, 222 Cal. App. 4th 1168, 1192 (2014) (citation omitted). The State's effort to make this showing, Br. 53–56, founders on the Act's text and legislative history.

Start with the text. AB 2273 contains no severability clause—an omission that raises a "presumption of inseverability" under California law. *Kasler v. Lungren*, 72 Cal. Rptr. 2d 260, 273 (Ct. App. 1998), *rev'd on other grounds*, 23 Cal. 4th 472 (2000); *see also County of Sonoma v.*

Super. Ct., 173 Cal. App. 4th 322, 352 (2009) (absence of a severability clause is indicia of legislative intent).

Two more features of the text strengthen that presumption. First, the Legislature imported the Act's architecture and terminology from the U.K. Age-Appropriate Design Code, and thus the Act should operate similarly to that *unitary* code, of which the DPIA notice-and-cure process is a key aspect. 2-SER-415. Second, the statutory mandate that California regulators consult U.K. guidance in construing the Act demonstrates the centrality of the DPIA safe harbor. *See* AB 2273, Findings & Decls., § 1(d)–(e). Guidance from the U.K.'s Information Commissioner's Office emphasizes compliance and remediation over sanctions. *See* 2-SER-387 ¶¶ 27, 30; 2-SER-401 ¶ 67; 2-SER-415 (describing U.K. enforcement approach). But absent the Act's 90-day cure period, covered businesses have no opportunity to reach compliance before incurring immediate financial penalties. That departs from the statute the Legislature enacted—underscoring the "overriding importance" of the DPIA safe harbor to the Act's intended operation. *Jevne v. Super. Ct.*, 35 Cal. 4th 935, 961 (2005).

Legislative history confirms that the Legislature would not have enacted the Act without the invalid DPIA provisions, including the 90-day cure period. The Legislature shelved the June 30, 2022, version of the Act, which lacked notice-and-cure provisions, in a "suspense file" where legislation dies without a vote. *See* 2-ER-61 ¶ 6; 2-ER-63. The bill was amended on August 11, 2022, to add (among other things) a 45-day cure period. But it was only after the Legislature revised the bill *again* on August 22, 2022, to enlarge the cure period to 90 days that the Act garnered the votes to pass. *See* 2-ER-61 ¶¶ 9–11; 2-ER-63. That the Legislature *considered*—but *did not* adopt—the bill without the 90-day cure demonstrates that it *would not* have adopted those versions. *See Mendoza v. California*, 149 Cal. App. 4th 1034, 1064 (2007) (provisions not severable where legislature considered but declined to adopt alternative version of bill); 1-ER-50–51.

As it did below, the State claims that adding the safe harbor establishes only that the Legislature preferred a version of the Act with a cure provision to one without. Br. 55. But "what the Legislature actually *did*" is the best evidence of what it "would have" done. *Cal.*

Redev. Ass'n v. Matosantos, 53 Cal. 4th 231, 273 (2011). The Legislature *could* have enacted a law without the safe harbor. It declined.

The State contends the district court nevertheless erred in concluding the Act is not volitionally severable because NetChoice cannot show that adding the safe harbor was the "*reason* the bill left the suspense file." Br. 54. But that reverses the burden of proof. The onus is not on *NetChoice* to show that the Legislature passed the Act *because of* the DPIA provisions. It is on the *State* to show that the Legislature would have passed the Act *without* them. *See Nguyen*, 222 Cal. App. 4th at 1192–93 (burden falls on the government to show severability). And the Court must conclude "with confidence" that the Legislature would have enacted the Act in constitutional form. *Acosta v. City of Costa Mesa*, 718 F.3d 800, 817–18 (9th Cir. 2013). Without certainty, severance is impermissible. *See id.* at 818; *Sonoma*, 173 Cal. App. 4th at 352; *Abbott Lab'ys v. Franchise Tax Bd.*, 175 Cal. App. 4th 1346, 1361 (2009).

The State's own briefing is thus fatal to its argument. It admits it is "possible"—even "equally possible"—that the addition of the notice-and-cure provision "led to the bill's passage." Br. 54. But "[s]everance is not proper … 'where the legislative intent is doubtful.'" *Bd. of Osteopathic*

Exam'rs v. Bd. of Med. Exam'rs, 53 Cal. App. 3d 78, 85 (1975) (citation omitted). Even odds fall well short of the "confidence" the law demands. *See O'Kane v. Catuira*, 212 Cal. App. 2d 131, 141 (1963) (trial court "clearly correct" to strike entire act where it was "impossible to say" what Legislature would have done had it foreseen partial invalidation).

The State also faults the district court for relying on floor statements by the bill's co-author calling attention to the safe harbor, arguing they warrant little attention. Br. 54–55. Rejecting that very argument as "without merit," the California Supreme Court has repeatedly held that statements by a bill's author are salient evidence of legislative purpose in a severability analysis when they are reflected in committee materials and communicated to the Legislature. *Make UC a Good Neighbor v. Regents of Univ. of Cal.*, 16 Cal. 5th 43, 60 & n.19 (2024). "A legislator's statement is entitled to consideration … when it is a reiteration of legislative discussion and events leading to adoption of proposed amendments rather than merely an expression of personal opinion." *Cal. Tchrs. Ass'n v. San Diego Cmty. Coll. Dist.*, 28 Cal. 3d 692, 700 (1981).

Assemblymember Wicks' floor statements meet that standard. When presenting the final version of the bill for a vote, she emphasized—on the record—that the newly expanded safe harbor would "ensure businesses in substantial compliance with the [Act] have an opportunity to remedy violations prior to being subject to civil penalties." 3-ER-575. Courts have held similar evidence sufficient to defeat severability. *See Sonoma*, 173 Cal. App. 4th at 352 (declining to sever where Senate bill analysis referred "specifically to [the invalid provision] under the 'arguments in support' of the legislation").

Nor does *Quintano v. Mercury Casualty Co.*, 11 Cal. 4th 1049 (1995) (Br. 54–55), help the State. That case downplayed the relevance of an individual legislator's statements "in construing a statute." *Id.* at 1062. But volitional severability does not turn on what the statute *means*; it turns on what the Legislature *would have done*. Legislative debate bears directly on that counterfactual inquiry. *See, e.g.*, *Abbott Lab'ys*, 175 Cal. App. 4th at 1361 (relying on post-enactment statement of single legislator in assessing severability).

The State's appeal to broad policy goals, Br. 56, fares no better. By its reckoning, the Legislature was "so committed" to protecting children's

privacy that it would have enacted virtually *any* version of the Act, no matter how punitive, incomplete, or divorced from its original design. *Id.* But if the strength of a general policy objective were enough to salvage a gutted statute, then every statute enacted in service of a popular cause would be severable. That is not the law. *See Barlow v. Davis*, 72 Cal. App. 4th 1258, 1267 (1999) ("intended function of a particular statutory scheme" is what counts, "not more conceptual policy matters").

It is thus the State—not NetChoice—that has attempted to answer "the wrong question." Br. 55 (citation & internal quotation marks omitted). The question is not whether the Legislature was broadly concerned for the "privacy and safety of child users." Br. 56. It is whether the Legislature would have enacted *this* truncated version of AB 2273—a punitive, strict-liability regime "inconsistent with the language and original intent" of the Act and "less effective in achieving [the Legislature's] goals[.]" *Metromedia, Inc. v. City of San Diego*, 32 Cal. 3d 180, 191 (1982); *see Nguyen*, 222 Cal. App. 4th at 1193 (law inseverable where remainder's penalty scheme "would go beyond" original intent). The answer to that question is "no."

III. The District Court Correctly Enjoined Several Individual Provisions For Independent Reasons.

In addition to enjoining all the regulatory provisions because of the Act's tainted coverage definition and severability defects, the district court also found that NetChoice was likely to prevail on its individual facial First Amendment challenges to the age-estimation mandate, § 31(a)(5), information-use restrictions, § 31(b)(1)–(4), and "dark pattern" restriction, § 31(b)(7). The Court need not reach these arguments if it affirms on either of the first two grounds, but here too the district court was correct.

A. The age-estimation mandate violates the First Amendment on its face.

The district court correctly enjoined the age-estimation mandate as facially invalid under the First Amendment. 1-ER-36–39; *contra* Br. 39–44. This mandate requires covered services to "[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers."

§ 31(a)(5). It is unconstitutional in every application and therefore facially invalid under *Moody*.[11]

Critically—and unlike the age-verification mandate in *Free Speech Coalition*, which only restricted "access [to] content that is obscene to minors"—the Act's age-estimation mandate restricts access to "fully protected speech" for both minors and adults. 145 S. Ct. at 2309–11. This is because regulated services provide access to information, § 30(b)(4), (5), almost all of which is constitutionally protected. The "narrowly limited classes of speech" that fall outside the First Amendment's protection, *Brown*, 564 U.S. at 790–91, comprise a tiny fraction of the speech communicated online—*less than 1%* of the content on some of the largest services. 1-SER-66–88. By forcing covered services to either "estimate age for the purpose of determining what content is appropriate for that age," or censor content to "comport with the highest risk level,

[11] The argument that the age-estimation mandate does not regulate speech but only "triggers the Act's other substantive provisions," Br. 39–40, does not disturb this holding. Courts do not decide whether a component of a regulatory regime "could survive constitutional scrutiny if it existed separately." *Church of Lukumi Babalu Aye, Inc. v. City of Hialeah*, 508 U.S. 520, 540 (1993). If a component "functions, with the rest of the enactments in question, to suppress" First Amendment rights, "it must be invalidated." *Id.*

presumably, the youngest children," 1-ER-37, any application of the Act burdens access to or alters the content of "*fully protected speech*." *Free Speech Coal.*, 145 S. Ct. at 2314–15, 2315 n.12 (agreeing that strict scrutiny applies to such laws).

Neither of the State's arguments for lesser scrutiny is persuasive. *First*, the State argues that the "act of estimating a user's age is *conduct,*" and thus the mandate does not trigger the First Amendment at all. Br. 39–40 (emphasis added). Nonsense. *Free Speech Coalition* rejected that very argument, holding that online age-screens are always subject to at least *some level* of First Amendment scrutiny because "age verification necessarily" burdens the "First Amendment right to access speech." 145 S. Ct. at 2316. There is no dispute that § 31(a)(5) requires covered services to age-screen before providing access to *all* content, or else alter *all* content to be age-appropriate for the youngest viewers. *See NetChoice II*, 113 F.4th at 1110, 1118 (adjusting "data protections," as used in § 31(a)(5), requires addressing "risks that arise from the data management practices" of a covered service, which in turn "require[s] consideration of content or proxies for content"); *accord* 1-ER-38. Because

nothing limits that mandate to unprotected speech, First Amendment scrutiny applies.

Second, the State contends that even if the First Amendment applies, the age-estimation mandate is subject to intermediate scrutiny because it restrains access to *all* speech neutrally, not just speech with particular content. Br. 40. But either compliance option triggers strict scrutiny. Compelling providers to collect some form of age-identification "as a condition of engaging in protected activity … impose[s] a form of prior restraint" because it burdens access to fully protected speech before it can occur and without adjudication. *Minneapolis Star & Trib. Co. v. Minn. Comm'r of Rev.*, 460 U.S. 575, 588 n.9 (1983). Alternatively, applying the Act's restrictions to all users would "reduce the adult population … to reading only what is fit for children." *Butler*, 352 U.S. at 383. Strict scrutiny applies to laws that force intermediaries either to restrain access to fully protected speech, *Free Speech Coal.*, 145 S. Ct. at 2309, 2311, or "alter" their "own editorial choices," *Moody*, 603 U.S. at 734.[12]

[12] That the State justifies the age-estimation mandate as "necessary to effectuate the Act's purpose of protecting child users," Br. 44, underscores its content basis. *See Boos*, 485 U.S. at 321; *Playboy*, 529 U.S. at 811–12.

In any event, the mandate fails any level of First Amendment review. The State has not shown that mandatory age-estimation or content-sanitation will in fact advance an interest in children's well-being in a direct and material way. *See Turner*, 512 U.S. at 662–64 (standard for intermediate scrutiny). Instead, access to online services is neither the cause of nor even correlated with the teen mental health problems the State seeks to prevent, and restricting teenagers' access to fully protected speech will on balance harm, not help, many of them. *See* 1-SER-7–19 ¶¶ 10–47; 1-SER-22–26 ¶¶ 55–69; 1-SER-28 ¶¶ 80–81; 1-SER-130–43 ¶¶ 10–43.

Furthermore, to the extent the State's interest is children's privacy, forcing services to extract personal information from users will *imperil* that aim. *See* 2-SER-469–70 ¶¶ 7–10; 1-SER-123 ¶ 7; 1-SER-117 ¶ 6; 2-SER-457–58; *accord* 1-ER-37–39.[13] The risk to privacy is not mitigated (*cf.* Br. 41) by the Act's limitations on how data collected for age

[13] Just last month, hackers gained access to thousands of verification photos and government IDs from an app that requires identity verification. *See* Kevin Collier and Angela Yang, *Hackers leak 13,000 user photos and IDs from the Tea app, designed as a women's safe space*, NBC News (July 25, 2025), https://www.nbcnews.com/tech/social-media/tea-app-hacked-13000-photos-leaked-4chan-call-action-rcna221139.

estimation may be handled. That provision, § 31(b)(8), does not eliminate the privacy-intrusive collection and processing of information in the first place; nor does it restrict the third-party vendors on which the State's own witness encourages services to rely. 3-ER-442 ¶ 64. A law at odds with itself fails even intermediate scrutiny. *Yim*, 63 F.4th at 794.

The mandate is also not narrowly tailored. If the State wished to protect minors from content that it can constitutionally preclude them from accessing under the First Amendment, it could have passed a law requiring age-estimation for such material. *See Free Speech Coal.*, 145 S. Ct. at 2317. But the Act does not just limit teenagers' access to "explicit portrayals of nudity or sex acts that predominantly appeal to the prurient interest," which states may restrict. *Id.* at 2308–09 & n.7. It limits their access to a wide range of content constitutionally protected as to them. *Id.* at 2311–12 & n.9. As the Supreme Court stressed in *Reno,* the State may not "torch a large segment of the Internet"—fully protected for both adults and minors alike, *Brown*, 564 U.S. at 794–95—just to prevent potential discrete risks to some children. 521 U.S. at 882.

This choice between unconstitutional limitations on speech mars almost *any* application of § 31(a)(5), which thus is unconstitutional "in every case." *Americans for Prosperity*, 594 U.S. at 618.

B. The information-use restrictions are unconstitutionally vague.

The district court also correctly enjoined the information-use restrictions, § 31(b)(1)–(4), as unconstitutionally vague. 1-ER-41–43; *contra* Br. 44–49.

A law is unconstitutionally vague if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *United States v. Williams*, 553 U.S. 285, 304 (2008). Laws regulating expression face an even "more stringent" test, *Holder v. Humanitarian L. Project*, 561 U.S. 1, 19 (2010), because they cause speakers "to steer far wider of the unlawful zone," *Butcher v. Knudsen*, 38 F.4th 1163, 1169 (9th Cir. 2022) (citation omitted). Such laws must be invalidated if not drawn with precision. *Id.*

The information-use restrictions turn on the undefined terms "material detriment," "best interests," and "well-being," which are especially subjective because they apply to any single minor. *See* § 31

(applying standards to "a child"). This Court previously noted the problematic vagueness of the phrase "material detriment." *NetChoice II*, 113 F.4th at 1120. And the district court held these terms "have no established meaning," and that the Act "provides no guidance." 1-ER-42.

Reasonable minds can disagree as to what types of information and ideas are "detrimental" to a young person's "best interests" or "well-being," and those judgments belong to individual families according to their values. *See Brown*, 564 U.S. at 794–95. Bestowing them on the government invites haphazard, discriminatory "*ad hoc*" enforcement, *Foti v. City of Menlo Park*, 146 F.3d 629, 638–39 (9th Cir. 1998), leaving covered services no way to ensure compliance. *See ACLU v. Mukasey*, 534 F.3d 181, 205 (3d Cir. 2008) (services "forced to guess" what "harmful to minors" means); *Free Speech Coal. v. Reno*, 198 F.3d 1083, 1095 (9th Cir. 1999) (similar), *aff'd*, 535 U.S. 234 (2002). Unrebutted evidence illustrates the "predictable tendency" for such uncertainty to chill speech. *Counterman v. Colorado*, 600 U.S. 66, 77–78 (2023); *see* 2-SER-494–96 ¶¶ 11–17; 2-SER-510–11 ¶¶ 18–19; 2-SER-477 ¶ 15; 2-SER-487–90 ¶¶ 16–19; 2-SER-531–32 ¶¶ 6–7.

The State insists these terms are "clear," but its brief raises more questions than answers. Br. 45–46. It argues the meanings of "material detriment" and "well-being" are obvious from dictionary definitions, for example, because who could doubt that connecting a child to a criminal, or suggesting a 14-year old buy alcohol, is detrimental to their well-being? *Id.* at 46. But hypothesizing a couple of extreme cases does nothing to cabin the law's expansive terms (especially given that these terms apply to children across a wide range of ages). And the ability to cherry-pick plausible examples is not the test of vague laws, nor what makes them pernicious to free expression. Specificity is required to avoid regulations, like this one, that "lack precise definition," *McCormack v. Herzog,* 788 F.3d 1017, 1031 (9th Cir. 2015), and are "susceptible to many different interpretations" that tread upon protected speech. *United States v. Hall*, 912 F.3d 1224, 1227 (9th Cir. 2019). The test is not whether a term has applications everyone can agree make sense, but whether it is so standardless that it permits selective application based on subjective judgments of an enforcer. *See NAACP v. Button*, 371 U.S. 415, 433, 435 (1963).

This Act does so in spades. Take the State's interpretation of actions "materially detrimental" to a child's health or well-being—any activity that "causes meaningful harm to a child's physical state, mental state, or overall condition of health and happiness." Br. 45. What does that include? Sleep loss? Distraction? Hurt feelings? Dr. Radesky appears to think so. 4-ER-606–11 ¶¶ 46, 48–53; 4-ER-619–20 ¶ 79. But what if the sleep loss is from staying up late reading something interesting on Wikipedia, or learning a skill on YouTube? What if the distraction is caused by discovering inspiring literature on Goodreads? And what if the hurt feelings are from defending an unpopular political opinion on social media, or being exposed to important but distressing world events like war, or famine in the *New York Times*? The Act gives no guidance, and has no guardrails, to ensure these terms could not restrict protected speech.

The Act's invocation of the "best interests of children" suffers similar defects. 1-ER-43. Although the State contends the term is used in family law, Br. 49, its application in that specialized context is confined to finite custodial options, a fixed record, and judicial criteria that do not require moral judgments about speech. *Cf. Bates*, 2025 WL 2079875, at

*12 (standard does not permit government to "decide that certain political views were most conducive to the best interests of children and then reject prospective adoptive parents who refused to impart those views"). Even in that limited context, the term is an "elusive guideline that belies rigid definition." *In re Matthew B.*, 232 Cal. App. 3d 1239, 1263 (1991).

These terms' vagueness is not ameliorated by any scienter requirements. *Cf.* Br. 46–47. Although such a requirement "may mitigate a law's vagueness," it can only do so when it gives "notice to the complainant that his conduct is proscribed." *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 499 (1982). The principle has no application where a statute fails to define the proscribed conduct in the first place. *Planned Parenthood of Cent. N.J. v. Farmer*, 220 F.3d 127, 138 (3d Cir. 2000) (putative scienter requirement in statute proscribing abortion procedures irrelevant where "the procedure itself" was not "identified or readily susceptible of identification").

Here, only one provision, § 31(b)(1), requires any scienter, and that provision still imposes liability based on what covered services should have "reason to know" about the "materially detrimental" effects of

speech. That falls short. *See Stahl v. City of St. Louis*, 687 F.3d 1038, 1041 (8th Cir. 2012) (scienter requirement failed to cure vagueness when violation turned on the reactions of third parties since whether speaker "should know that certain speech or activities likely will" prompt such reactions was "impossible to predict"). Even treating "reason to know" as a valid scienter requirement, it still only "modifies a vague term," *Planned Parenthood*, 220 F.3d at 138, failing to answer what acts are detrimental. *Cf. Hill v. Colorado*, 530 U.S. 703, 732 (2000) (Br. 47) (knowledge requirement sufficient where statute defined proscribed conduct).

C. The "dark pattern" restriction is unconstitutionally vague.

The district court also correctly held the "dark pattern" restriction, § 31(b)(7), unconstitutionally vague. 1-ER-44–45. That provision prohibits publishing information in ways that "lead or encourage" minors to "take any action" that a covered service "has reason to know is materially detrimental" to a child's "health" or "well-being." 1-ER-43 (emphasis omitted). This includes the way websites, like ESPN.com or X, might display articles or posts on a continuously scrollable webpage, or

the way services like Netflix or YouTube place related titles, subsequent episodes, or new videos in a sidebar. *NetChoice II*, 113 F.4th at 1123 n.8.

The problem, again, is that the Act gives covered services no way to know when those choices will be "materially detrimental" to a given child's well-being, as opposed to being useful and interesting—even if (*cf.* Br. 50) reasonable people can agree that certain extreme scenarios are likely proscribed. *See supra* Part III.B. It thus makes no difference that the term "dark pattern" is defined in California law. *Cf.* Br. 51 (citing Cal. Civ. Code § 1798.140(*l*)). The provision is vague not because covered services are unsure which of their display choices are covered, but because the services cannot know *when* those display choices will expose them to liability for publishing content in ways that are "materially detrimental" to children. *See* 2-SER-494–96 ¶¶ 11–17; 2-SER-510–11 ¶¶ 18–19; 2-SER-477 ¶ 15; 2-SER-487–90 ¶¶ 16–19; 2-SER-531–32 ¶¶ 6–7.

The State again claims the "reason to know" standard mitigates the vagueness of what constitutes "materially detrimental" to "well-being." Br. 50. But that standard is again irrelevant because, as in *Planned Parenthood*, 220 F.3d at 138, "the 'what' that must be proven *is* vague,"

1-ER-44, and because covered services cannot possibly know how any given minor will react to the way information is published. *See Stahl*, 687 F.3d at 104. The State's assertion that "the restriction does not apply" when a covered business "lacks knowledge of any harm," Br. 52, both misstates the statute—services are liable if they *should* know about a harm—and makes no difference since the Act fails to define *what* is detrimental.

IV. The Court May Also Affirm On Alternative Grounds.

A. The information-use and "dark pattern" restrictions violate the First Amendment to the extent NetChoice challenges them.

In addition to challenging the Act in full based on its content-based scope and pervasive First Amendment defects, *supra* Part I, NetChoice also brings narrower facial claims targeting discrete applications of specific provisions. These provisions' unconstitutional applications are "substantial" compared to any "legitimate sweep" under *Moody*, 603 U.S. at 723–24. The district court agreed as to § 31(a)(9)'s application to content moderation policies and community standards, which it enjoined on this ground. 1-ER-31–33. The district court declined to enjoin the information use, § 31(b)(1)–(4), and "dark pattern," § 31(b)(7), provisions

on this basis, 1-ER-33–36, having already found those provisions unconstitutional for three other reasons. This Court could nonetheless affirm portions of the injunction below by holding that these provisions individually are facially invalid to the extent NetChoice challenges them.

The State below misapprehended the framework that governs these alternative First Amendment claims. To be sure, courts evaluating a facial challenge must measure a law's "applications [that] violate the First Amendment" against "the rest." *Moody*, 603 U.S. at 725. But the "rest" is not always all applications of a statutory provision; comparing one to the other depends on "the breadth of the remedy" sought. *Citizens United v. FEC*, 558 U.S. 310, 331 (2010); *see John Doe No. 1 v. Reed*, 561 U.S. 186, 194 (2010) (facial challenges need "not seek to strike [a law] in all its applications" and can be made "to the extent of th[e] reach" identified by plaintiff). Thus, the possibility that a law violates the First Amendment "only in some cases" does not foreclose facial relief; it simply limits the "relief to which [a plaintiff is] entitled." *Isaacson v. Horne*, 716 F.3d 1213, 1230 (9th Cir. 2013); *see United States v. Supreme Ct. of N.M.*, 839 F.3d 888, 915 (10th Cir. 2016) (analysis does not involve "the

constitutional validity of all or virtually all of the applications of the challenged provision," just "the subset of applications targeted").

A different rule would defy logic. It would allow the government to "insulate" even plainly unconstitutional applications from targeted facial challenge by embedding them in broad provisions with a wide array of applications. As this Court recognized, that would be improper. *NetChoice II*, 113 F.4th at 1117 (government may not "insulate a specific provision of law from a facial challenge under the First Amendment by bundling it with other" provisions). Nothing in this Court's recent decision *Arizona Attorneys for Criminal Justice v. Mayes*, 127 F.4th 105 (9th Cir. 2025), suggests otherwise. As the district court recognized, the plaintiffs in that case sought to invalidate a statute in *all* its applications, despite conceding the constitutionality of its "primary" ones. 1-ER-30 (citing *Ariz. Att'ys*, 127 F.4th at 107, 111–12). The case has no bearing where a plaintiff seeks to challenge only specific applications. *See, e.g.*, *Americans for Prosperity*, 594 U.S. at 611, 618–19 (granting facial relief as applied to a specific tax schedule).[14]

[14] The Supreme Court and federal circuits have repeatedly granted this kind of targeted facial relief. *See, e.g.*, *Brockett v. Spokane Arcades, Inc.*,

NetChoice's narrower alternative requests for relief make all the difference.

1. Information-use provisions

These provisions restrict how and for what purposes online services may use "personal information" they lawfully receive from minor users. § 31(b)(1)–(4). Each is unconstitutional to the extent it applies to covered services' use of such information "to publish content or to make information available," 1-SER-176 ¶¶ 6–7, and NetChoice challenges them *only* "to the extent of that reach." *John Doe No. 1*, 561 U.S. at 194. Any hypothetical application of these provisions to other business activities—including collecting or selling personal information for other purposes—falls outside the scope of NetChoice's limited challenge.

The district court originally held these provisions facially unconstitutional, focusing on precisely the range of applications

---

472 U.S. 491, 503–07 (1985) (facial relief "insofar" as law "reach[ed] protected materials"); *United States v. Grace*, 461 U.S. 171, 175, 183 (1983) (facial relief as to law's applications to sidewalks); *PETA, Inc. v. N.C. Farm Bureau Fed'n*, 60 F.4th 815, 835–38 (4th Cir. 2023) (facial relief as "applied" to certain newsgathering activities); *Project Veritas Action Fund v. Rollins*, 982 F.3d 813, 826, 840 (1st Cir. 2020) (facial relief against certain applications only); *Smith v. Butterworth*, 866 F.2d 1318, 1320–21 (11th Cir. 1989) ("insofar as [law] applie[d] to" certain witnesses), *aff'd*, 494 U.S. 624 (1990).

NetChoice now challenges. *See* 1-SER-205–09. Specifically, the district court found these provisions regulate speech by restricting the availability and use of information on a content- and speaker-basis. 1-SER-188–90. It held § 31(b)(1) was not narrowly tailored and would force services to make subjective assessments as to minors of different ages, burdening "substantially more speech than is necessary." 1-SER-205–06 (citation omitted). It further held § 31(b)(2) and (b)(3) failed narrow tailoring because they are not limited to preventing minors from receiving "information deemed harmful" but also apply to beneficial targeted content. 1-SER-206–08. The district court was unpersuaded the State had a legitimate interest in preventing the dissemination of protected but "unsolicited content." 1-SER-207–08. And § 31(b)(4) failed scrutiny, the district court held, because the State presented no evidence that it materially alleviated any real harm. 1-SER-208–09.

When this Court vacated that first preliminary injunction in part in light of *Moody*, it did not disturb the district court's reasoning that these specified applications of the information-use provisions violate the First Amendment. *NetChoice II*, 113 F.4th at 1126 n.9. But it noted that NetChoice's challenge was at that time arguably broader. Now, however,

NetChoice has narrowed its challenge such that these unconstitutional applications comprise the universe of challenged applications, and thus a facial injunction is appropriate.

The State cannot escape constitutional scrutiny by recasting these provisions as "privacy" protections, Br. 2. As this Court recently confirmed, a law that bars entities from using or compiling minors' personal data "for the purpose of marketing or advertising" a product regulates speech based on content because the "provision turns on prohibiting the use of certain information." *Junior Sports Mags., Inc. v. Bonta*, 2025 WL 1863184, at *2 (9th Cir. July 7, 2025). The Act's information-use restrictions, to the extent NetChoice challenges them, are *worse*, restricting not just commercial but also expressive uses to present or distribute content. That is a paradigmatic "content-based restriction." *Id.*

The State's asserted interest in children's privacy does not justify that restriction. "[A] state may not 'condition privacy on acceptance of a content-based rule that is not drawn to serve the State's asserted interest.'" *Id.* at *3 (quoting *Sorrell*, 564 U.S. at 574). Critically, the State has never shown that these provisions satisfy heightened scrutiny *within*

the range of publishing applications NetChoice challenges. Accordingly, these provisions have no legitimate sweep within that range and are invalid to that extent. *See Americans for Prosperity*, 594 U.S. at 617–18 (holding disclosure statute facially overbroad to the extent applied to one type of tax schedule, since applications within that range were unconstitutional "in every case"); *see also Moody*, 603 U.S. at 708.

2. "Dark pattern" restriction

On remand, NetChoice also brought a narrowed facial challenge to the "dark pattern" restriction, seeking facial relief only to the extent the provision "applies to covered services' use of recommendation algorithms, continuous scroll, autoplay, and other design features that organize content." 1-SER-176 ¶ 8.[15] Because the unconstitutional applications within that scope vastly outnumber any legitimate sweep, the provision is facially invalid to this extent. *See Americans for Prosperity*, 594 U.S. at 611, 618–19.

Any application of § 31(b)(7) within this range restricts speech by regulating "how the display" of information "will be ordered and

[15] NetChoice does not challenge applications where dark patterns are used to deceive minors into providing personal information or forgoing privacy protections. *See* 1-SER-176 ¶ 8.

organized," *Child.'s Health Def. v. Meta Platforms, Inc.*, 112 F.4th 742, 759 (9th Cir. 2024) (quoting *Moody*, 603 U.S. at 740–41), "through features distinctive to the medium," *Brown*, 564 U.S. at 790; *accord* 1-ER-26. The district court thus erred in holding it "unclear" what features were covered or how those features affect content determinations. 1-ER-36. The term encompasses commonplace publishing features that simply organize and filter content, such as newsfeed functions that personalize the user experience. *See* 4-ER-610 ¶ 49; 4-ER-612 ¶ 55; 2-SER-371–72 ¶ 51 n.81; *see also NetChoice II*, 113 F.4th at 1123 n.8. And within NetChoice's narrower challenge, the "dark pattern" restriction is facially invalid because it "suppresses expression out of concern for its likely communicative impact" upon a particular audience, *United States v. Eichman*, 496 U.S. 310, 317–18 (1990), and is thus subject to strict scrutiny in "every case." *Americans for Prosperity*, 594 U.S. at 618.

*****

Because these provisions have no valid applications within their challenged ranges, the injunction may be affirmed on this basis as well.

B. The Act violates the Commerce Clause.

The Act is also invalid under the Commerce Clause, which denies states power to control interstate commerce. *See Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc). The Supreme Court reaffirmed this principle in *National Pork Producers Council v. Ross*, 598 U.S. 356, 376 n.1 (2023), holding that state laws violate the Constitution's "horizontal separation of powers" when they reach activities "wholly outside" a state's borders. And this Court recently applied it in *Flynt v. Bonta*, 131 F.4th 918 (9th Cir. 2025), recognizing that laws have an "impermissible extraterritorial effect" where they regulate "entirely out-of-state activities[.]" *Id.* at 929–31 (rejecting challenge only because the law "regulate[d] conduct within the state").

That is what the Act does. Before a covered provider offers a service, it must discern if a user is a California legal resident and restrict its services accordingly, even if that user is out of state. This is the same defect that required invalidation in *Sam Francis*, 784 F.3d at 1323. It requires the same here. *Cf.* Cal. Civ. Code § 1798.145(a)(7) (CCPA exempts activity "wholly outside of California").

The district court rejected this argument only because it thought the issue insufficiently briefed. 1-ER-54–55. But the record is sufficient to conclude that the Act regulates solely based on residency, wholly beyond California's borders.

C. COPPA preempts the Act.

The Act is also invalid with respect to minors under 13 because it conflicts with and is preempted by COPPA. While the district court found an insufficient record to decide this, 1-ER-54, this Court may do so.

State laws are "inconsistent with," and therefore preempted by, COPPA if they impose "contradictory … requirements" or "stand as obstacles to federal objectives." *Jones v. Google LLC*, 73 F.4th 636, 642 (9th Cir. 2023); *e.g., New Mexico ex rel. Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1120–21 (D.N.M. 2020); *H.K. v. Google LLC*, 595 F. Supp. 3d 702, 711 (C.D. Ill. 2022).

While the district court posited that it is "not clear" that the challenged provisions "contradict" COPPA rather than just "supplement" it, 1-ER-54, they do contradict it. The two laws occupy the same regulatory field—the personal information of minors under 13. But the Act imposes liability for the very same conduct that COPPA allows.

COPPA applies to services "directed to children," 15 U.S.C. § 6502(a)(1), whereas the Act applies to those services children "are likely to access." Cal. Civ. Code § 1798.99.29. COPPA empowers parents to decide what their children can access online; the Act strips parents of that power. And the Act imposes liability for conduct permissible under COPPA—for example, failing to age estimate with enough "certainty," *id.* § 31(a)(5)—whereas COPPA expressly relieves companies of any need to estimate the ages of their users.

The Act is neither "parallel to" nor "proscribe[s] the same conduct" as COPPA. *Jones*, 73 F.4th at 644. It is preempted.

D. Section 230 preempts the Act's provisions that regulate how services moderate third-party content.

Finally, Section 230 facially preempts the information-use and "dark pattern" restrictions, § 31(b)(1)–(4), (7), to the extent these would obligate online services to monitor for and prevent the publication of third-party content that is "materially detrimental to" or not "in the best interests" of minors. *See Doe v. Grindr Inc.*, 128 F.4th 1148, 1153 (9th Cir. 2025) (Section 230 barred claims faulting online service for failing to protect minor plaintiff from harmful user-generated content).

Section 230(c)(1) preempts state laws that impose liability on (1) an interactive computer service (2) in a way that treats it as the publisher or speaker (3) of information provided by a third-party. *See Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009). Statutes that would obligate online services to monitor for, screen, block, or remove third-party content on the services—such as for content a service "knows, or has reason to know, is materially detrimental" to a child, § 31(b)(1)—are preempted. *NetChoice, LLC v. Bonta*, --- F. Supp. 3d ---, 2025 WL 1918742, at *10 (N.D. Cal. July 11, 2025); *e.g.*, *Carr*, 2025 WL 1768621, at *20; *CCIA*, 747 F. Supp. 3d at 1043. Applying § 31(b)(1)–(4) and (7) to this effect is accordingly preempted, and facial relief is warranted within that range. *See Isaacson*, 716 F.3d at 1230.

The district court rejected NetChoice's Section 230 challenge solely because it was skeptical that Section 230 permits pre-enforcement relief. 1-ER-53. But that relief is available, as the district court—in a more recent case brought by NetChoice—now agrees. *NetChoice*, 2025 WL 1918742 at *10 (Freeman, J.).

CONCLUSION

This Court should affirm the preliminary injunction.

Respectfully submitted,

/s/ David M. Gossett

Adam S. Sieff
DAVIS WRIGHT TREMAINE LLP
350 South Grand Avenue
27th Floor
Los Angeles, CA 90071
(213) 633-6800
adamsieff@dwt.com

Ambika Kumar
Bianca G. wChamusco
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue
Suite 3300
Seattle, WA 98104
(206) 757-8030
ambikakumar@dwt.com
biancachamusco@dwt.com

David M. Gossett
Meenakshi Krishnan
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW
Suite 500 East
Washington, DC 20005
(202) 973-4200
davidgossett@dwt.com
meenakshikrishnan@dwt.com

Robert Corn-Revere
FOUNDATION FOR INDIVIDUAL
RIGHTS AND EXPRESSION
700 Pennsylvania Avenue SE
Suite 340
Washington, D.C. 20003
(215) 717-3423 Ext. 209
bob.corn-revere@thefire.org

Attorneys for Plaintiff-Appellee NetChoice, LLC.

Dated: August 11, 2025

CIRCUIT RULE 28-2.6 STATEMENT OF RELATED CASES

I am unaware of any related cases currently pending in this Court.

/s/ *David M. Gossett*
David M. Gossett

August 11, 2025

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FORM 8. CERTIFICATE OF COMPLIANCE FOR BRIEFS

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

9th Cir. Case Number(s): 25-2366

I am the attorney or self-represented party.

This brief contains 13,914 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

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

[●] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[ ] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:

- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to multiple briefs; or
- [ ] a party or parties are filing a single brief in response to a longer joint brief.
- [ ] complies with the length limit designated by court order dated _____.
- [ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature: /s/ *David M. Gossett* **Date:** August 11, 2025

CERTIFICATE OF SERVICE

I hereby certify that on August 11, 2025, I electronically filed the foregoing document with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate ACMS system.

I certify that all participants in the case are registered ACMS users and that service will be accomplished by the appellate ACMS system.

/s/ *David M. Gossett*
David M. Gossett

August 11, 2025

STATUTORY ADDENDUM

Page

A. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-06 77

B. Section 230 of the Communications Decency Act, 47 U.S.C. § 230 94

C. California Consumer Privacy Act of 2018 (CCPA), *as amended by* California Privacy Rights Act of 2020 (CPRA), Cal. Civ. Code §§ 1798.100 *et seq.* 99

A. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06

§ 6501
Definitions

In this chapter:

(1) Child
The term "child" means an individual under the age of 13.

(2) Operator
The term "operator"—

> **(A)** 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 or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce—
>
> > **(i)** among the several States or with 1 or more foreign nations;
> >
> > **(ii)** in any territory of the United States or in the District of Columbia, or between any such territory and—
> >
> > > **(I)** another such territory; or
> > >
> > > **(II)** any State or foreign nation; or
> >
> > **(iii)** between the District of Columbia and any State, territory, or foreign nation; but
>
> **(B)** does not include any nonprofit entity that would otherwise be exempt from coverage under section 45 of this title.

(3) Commission
The term "Commission" means the Federal Trade Commission.

(4) Disclosure
The term "disclosure" means, with respect to personal information—

> **(A)** the release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and
>
> **(B)** making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting, through the Internet, or through—
>
> > **(i)** a home page of a website;
> >
> > **(ii)** a pen pal service;
> >
> > **(iii)** an electronic mail service;
> >
> > **(iv)** a message board; or
> >
> > **(v)** a chat room.

(5) Federal agency
The term "Federal agency" means an agency, as that term is defined in section 551(1) of Title 5.

(6) Internet
The term "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 or radio.

(7) Parent
The term "parent" includes a legal guardian.

(8) Personal information
The term "personal information" means individually identifiable information about an individual collected online, including—

(A) a first and last name;

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

(C) an e-mail address;

(D) a telephone number;

(E) a Social Security number;

(F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or

(G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

(9) Verifiable parental consent
The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

(10) Website or online service directed to children

(A) In general
The term "website or online service directed to children" means—

(i) a commercial website or online service that is targeted to children; or

(ii) that portion of a commercial website or online service that is targeted to children.

(B) Limitation

A commercial website or online service, or a portion of a commercial website or online service, shall not be deemed directed to children solely for referring or linking to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

(11) Person

The term "person" means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

(12) Online contact information

The term "online contact information" means an e-mail address or another substantially similar identifier that permits direct contact with a person online.

§ 6502
Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet

(a) Acts prohibited

(1) In general
It is unlawful for an operator of a website 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 under subsection (b).

(2) Disclosure to parent protected
Notwithstanding paragraph (1), neither an operator of such a website or online service nor the operator's agent shall be held to be 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 subsection (b)(1)(B)(iii) to the parent of a child.

(b) Regulations

(1) In general
Not later than 1 year after October 21, 1998, the Commission shall promulgate under section 553 of Title 5 regulations that—

(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child—

(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and

(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;

(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent—

(i) a description of the specific types of personal information collected from the child by that operator;

(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and

(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;

(C) prohibit conditioning 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; and

(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(2) When consent not required

The regulations shall provide that verifiable parental consent under paragraph (1)(A)(ii) is not required in the case of—

(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;

(B) a request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;

(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request—

> **(i)** if, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or
>
> **(ii)** without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;

(D) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)—

> **(i)** used only for the purpose of protecting such safety;
>
> **(ii)** not used to recontact the child or for any other purpose; and
>
> **(iii)** not disclosed on the site,

if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary—

(i) to protect the security or integrity of its website;

(ii) to take precautions against liability;

(iii) to 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.

(3) Termination of service

The regulations shall permit the operator of a website or an online service to terminate service provided to a child whose parent has refused, under the regulations prescribed under paragraph (1)(B)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child.

(c) Enforcement

Subject to sections 6503 and 6505 of this title, a violation of a regulation prescribed under subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 57a(a)(1)(B) of this title.

(d) Inconsistent State law

No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.

§ 6503
Safe harbors

(a) Guidelines
An operator may satisfy the requirements of regulations issued under section 6502(b) of this title by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved under subsection (b).

(b) Incentives

(1) Self-regulatory incentives
In prescribing regulations under section 6502 of this title, the Commission shall provide incentives for self-regulation by operators to implement the protections afforded children under the regulatory requirements described in subsection (b) of that section.

(2) Deemed compliance
Such incentives shall include provisions for ensuring that a person will be deemed to be in compliance with the requirements of the regulations under section 6502 of this title if that person complies with guidelines that, after notice and comment, are approved by the Commission upon making a determination that the guidelines meet the requirements of the regulations issued under section 6502 of this title.

(3) Expedited response to requests
The Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.

(c) Appeals
Final action by the Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of Title 5.

§ 6504
Actions by States

(a) In general

(1) Civil actions

In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 6502(b) of this title, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin that practice;

(B) enforce compliance with the regulation;

(C) obtain damage, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider to be appropriate.

(2) Notice

(A) In general

Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Commission—

(i) written notice of that action; and

(ii) a copy of the complaint for that action.

(B) Exemption

(i) In general
Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

(ii) Notification
In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(b) Intervention

(1) In general
On receiving notice under subsection (a)(2), the Commission shall have the right to intervene in the action that is the subject of the notice.

(2) Effect of intervention
If the Commission intervenes in an action under subsection (a), it shall have the right—

(A) to be heard with respect to any matter that arises in that action; and

(B) to file a petition for appeal.

(3) Amicus curiae
Upon application to the court, a person whose self-regulatory guidelines have been approved by the Commission and are relied upon as a defense by any defendant to a proceeding under this section may file amicus curiae in that proceeding.

(c) Construction
For purposes of bringing any civil action under subsection (a), nothing in this chapter shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(d) Actions by Commission
In any case in which an action is instituted by or on behalf of the Commission for violation of any regulation prescribed under section 6502 of this title, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that regulation.

(e) Venue; service of process

(1) Venue
Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of Title 28.

(2) Service of process
In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

§ 6505
Administration and applicability

(a) In general
Except as otherwise provided, this chapter shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(b) Provisions
Compliance with the requirements imposed under this chapter shall be enforced under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a)[1] of the Federal Reserve Act (12 U.S.C. 601 et seq. and 611 et seq.), by the Board; and

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;

---

[1] See References in Text note below.

(3) the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board with respect to any Federal credit union;

(4) part A of subtitle VII of Title 49 by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;

(5) the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and

(6) the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(c) Exercise of certain powers

For the purpose of the exercise by any agency referred to in subsection (a)[2] of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this chapter shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (a),[2] each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this chapter, any other authority conferred on it by law.

[2] So in original. Probably should be "subsection (b)".

(d) Actions by Commission

The Commission shall prevent any person from violating a rule of the Commission under section 6502 of this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this chapter. Any entity that violates such rule shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this chapter.

(e) Effect on other laws

Nothing contained in this chapter shall be construed to limit the authority of the Commission under any other provisions of law.

§ 6506
Review

Not later than 5 years after the effective date of the regulations initially issued under section 6502 of this title, the Commission shall—

(1) review the implementation of this chapter, including the effect of the implementation of this chapter on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and

(2) prepare and submit to Congress a report on the results of the review under paragraph (1).

B. Section 230 of the Communications Decency Act, 47 U.S.C. § 230

Protection for private blocking and screening of offensive material

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States—

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material

(1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability
No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[1]

(d) Obligations of interactive computer service
A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws

(1) No effect on criminal law
Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law
Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law
Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law
Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(5) No effect on sex trafficking law
Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—

(A) any claim in a civil action brought under section 1595 of Title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of Title 18; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of Title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

(f) Definitions

As used in this section:

(1) Internet

The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) Access software provider

The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

C. California Consumer Privacy Act of 2018, *as amended by* California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100 *et seq.* (selected sections)

§ 1798.100
General Duties of Businesses that Collect Personal Information

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:

> **(1)** The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.
>
> **(2)** If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.
>
> **(3)** The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if a business acting as a third party controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether that personal information is sold, in a clear and conspicuous manner at the location.

(c) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:

> **(1)** Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.
>
> **(2)** Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.
>
> **(3)** Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title.

(4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title.

(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.

(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.

§ 1798.120
Consumers' Right to Opt Out of Sale or Sharing of Personal Information

(a) **(1)** A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt out of sale or sharing.

> **(2)** A business to which another business transfers the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the transferee assumes control of all of, or part of, the transferor shall comply with a consumer's direction to the transferor made pursuant to this subdivision.

(b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt out" of the sale or sharing of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

(d) A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the

consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information.

§ 1798.140
Definitions

For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

(b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(c) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) "Business" means:

> **(1)** A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to subdivision (d) of Section 1798.199.95.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

(e) "Business purpose" means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(f) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(g) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not

constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (9) of subdivision (a) of Section 1798.185, except as provided

for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded internet websites, applications, or services, other than the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts.

(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

(m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

(n) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(o) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(p) "Homepage" means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

(q) "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

(r) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(s) "Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's internet website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

(t) "Nonpersonalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

(u) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

> **(A)** Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
>
> **(B)** Any personal information described in subdivision (e) of Section 1798.80.
>
> **(C)** Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(2) (A) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern.

(B) (i) For purposes of this paragraph, "publicly available" means any of the following:

(I) Information that is lawfully made available from federal, state, or local government records.

(II) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.

(III) Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

(ii) "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(4) "Personal information" can exist in various formats, including, but not limited to, all of the following:

(A) Physical formats, including paper documents, printed images, vinyl records, or video tapes.

(B) Digital formats, including text, image, audio, or video files.

(C) Abstract digital formats, including compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

(x) "Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(y) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (15) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(aa) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(ab) "Research" means scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including, but not limited to, studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be:

> **(1)** Compatible with the business purpose for which the personal information was collected.
>
> **(2)** Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.

(4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

(ac) "Security and integrity" means the ability of:

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(ad) **(1)** "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally:

(i) Disclose personal information.

(ii) Interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(G) **(i)** A consumer's neural data.

(ii) "Neural data" means information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information.

(2) **(A)** The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(ag) **(1)** "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (9) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(2) For purposes of this title, a business does not share personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with

this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ai) "Third party" means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.

(2) A service provider to the business.

(3) A contractor.

(aj) "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(ak) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph (6) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (6) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

§ 1798.145
Exemptions

(a) **(1)** The obligations imposed on businesses by this title shall not restrict a business's ability to:

(A) Comply with federal, state, or local laws or comply with a court order or subpoena to provide information.

(B) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.

(C) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(D) **(i)** Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:

(I) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

(II) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

(III) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

(ii) For purposes of this subparagraph, a consumer accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services, shall not constitute a natural person being at risk or danger of death or serious physical injury.

(E) Exercise or defend legal claims.

(F) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.

(G) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a

consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(2) **(A)** This subdivision shall not apply if the consumer's personal information contains information related to accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services.

(B) This paragraph does not alter the use of aggregated or deidentified personal information consistent with a business purpose as defined in paragraphs (1), (2), (3), (4), (5), (7), or (8) of subdivision (e) of Section 1798.140, provided that the personal information is only retained in aggregated and deidentified form and is not sold or shared.

(C) This paragraph does not alter the duty of a business to preserve or retain evidence pursuant to California or federal law in an ongoing civil proceeding.

(b) The obligations imposed on businesses by Sections 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, and 1798.135 shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) **(1)** This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-

191)2 and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, provided that the information is not sold or shared in a manner not permitted by this subparagraph, and, if it is inconsistent, that participants be informed of that use and provide consent.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) **(1)** This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) Section 1798.120 shall not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, as defined in Section 651 of the Harbors and Navigation Code, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to Section 4310 of Title 46 of the United States Code, provided that the vessel dealer or vessel manufacturer with which that vessel information or ownership information is shared does not sell, share, or use that information for any other purpose.

(3) For purposes of this subdivision:

(A) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(B) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(C) "Vessel dealer" means a person who is engaged, wholly or in part, in the business of selling or offering for sale, buying or taking in trade for the purpose of resale, or exchanging, any vessel or vessels, as defined in Section 651 of the Harbors and Navigation Code, and receives or expects to receive money, profit, or any other thing of value.

(D) "Vessel information" means the hull identification number, model, year, month and year of production, and information describing any of the following equipment as shipped, transferred, or sold from the place of manufacture, including all attached parts and accessories:

(i) An inboard engine.

(ii) An outboard engine.

(iii) A stern drive unit.

(iv) An inflatable personal floatation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to a consumer for any verifiable consumer request may be extended by up to a total of 90 days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that

any verifiable consumer request is manifestly unfounded or excessive.

(i) **(1)** A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation. A service provider or contractor shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title provided that the service provider or contractor shall be liable for its own violations of this title.

(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in this title provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

(j) This title shall not be construed to require a business, service provider, or contractor to:

(1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(2) Retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained.

(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

(k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business's possession.

(l) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(m) **(1)** This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job

applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following criteria:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2023.

(n) **(1)** The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2023.

(o) **(1)** Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.

(C) "Owner" means a natural person that meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(D) "Director" means a natural person designated in the articles of incorporation of a business as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(E) "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(F) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data.

(q) **(1)** This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) "Educational standardized assessment or educational assessment" means a standardized or nonstandardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business's use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business's use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:

(1) The business has incurred significant expense in reliance on the consumer's consent.

(2) Compliance with the consumer's request to opt out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable.

(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.