

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

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

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

14 Plaintiff,

15 v.

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

18 Defendant.
 19

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

**DEFENDANT’S SUPPLEMENTAL
 BRIEFING ON SCRUTINY AND
 SEVERABILITY**

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

Action Filed: December 14, 2022

20
 21
 22
 23
 24
 25
 26
 27
 28

TABLE OF AUTHORITIES

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

Page

CASES

Am. Acad. of Pain Mgmt. v. Joseph
353 F.3d 1099 (9th Cir. 2004) 1

Am. Soc’y of Authors & Journalists v. Bonta
15 F.4th 954 (9th Cir. 2021)..... 1

Barnes v. Yahoo, Inc.
570 F.3d 1096 (9th Cir. 2009) 5

Burson v. Freeman
504 U.S. 191 (1992)..... 2

Calfarm Ins. Co. v. Deukmejian
771 P.2d 1247 (Cal. 1989) (en banc) 2

Lemmon v. Snap, Inc.
995 F.3d 1085 (9th Cir. 2021) 2

Sorrell v. IMS Health, Inc.
564 U.S. 552 (2011)..... 1

Trans Union Corp. v. F.T.C.
267 F.3d 1138 (D.C. Cir. 2001)..... 1

STATUTES

California Civil Code

§§ 1798.99.31(a)(1)–(4) 2

§ 1798.99.31(a)(5) 3

§ 1798.99.31(a)(6) 3

§ 1798.99.31(a)(7) 4

§ 1798.99.31(a)(8) 4

§ 1798.99.31(a)(9) 5

§ 1798.99.31(a)(10) 5

§ 1798.99.31(b)(1) 5

§ 1798.99.31(b)(2) 5

§ 1798.99.31(b)(3) 6

§ 1798.99.31(b)(4) 6

§ 1798.99.31(b)(5) 7

§ 1798.99.31(b)(6) 7

§ 1798.99.31(b)(7) 7

§ 1798.99.31(b)(8) 3

§ 1798.99.35(c)..... 3

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

TABLE OF AUTHORITIES
(continued)

Page

CONSTITUTIONAL PROVISIONS

United States Constiution
First Amendment 1, 2

OTHER AUTHORITIES

Code of Federal Regulations, Title 16
 § 312.2..... 3
 § 312.7..... 7
 § 312.8..... 3
 § 312.10..... 6, 7

U.S. Surgeon General's Advisory: Social Media & Youth Mental Health (“Social
 Media Advisory”) (2023), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>..... *passim*

1 This brief addresses how First Amendment scrutiny and severability principles apply to AB
2 2273. For the purposes of this briefing, the parties are to assume that AB 2273 regulates speech.
3 Defendant disagrees. No provision of AB 2273 constitutes a prior restraint, Def. Br. 12–16, it
4 does not require that businesses restrict any users’ access to speech, *id.* at 15–16, and no
5 precedent holds that the collection of children’s data is speech subject to heightened scrutiny, *id.*
6 at 10–12. *Sorrell v. IMS Health, Inc.* addressed a restriction that prohibited the sale or disclosure
7 of physician prescriber data by pharmacies or for marketing purposes. 564 U.S. 552, 557 (2011).
8 *Sorrell* did not hold that a business has a right to collect data from individuals. To the contrary,
9 the “serious and unresolved issues” raised by increased data collection capacity due to
10 technological advances remained largely unaddressed. *Id.* at 579. Legal and factual distinctions
11 weigh heavily against expanding the scope of *Sorrell* to declare that businesses have a First
12 Amendment right to collect children’s personal information through complex and opaque means.
13 *Id.* at 575–77 (grounding decision in specifics of challenged law); *see also Am. Soc’y of Authors*
14 *& Journalists v. Bonta*, 15 F.4th 954, 962 & n.7 (9th Cir. 2021) (distinguishing *Sorrell* and other
15 cases on “established form[s] of speech” from those on economic activity).

16 To the extent the collection and use of children’s data can be considered speech, it is
17 commercial. Def. Br. 18–19; *Sorrell*, 564 U.S. at 572 (applying intermediate scrutiny); *Trans*
18 *Union Corp. v. F.T.C.*, 267 F.3d 1138 (D.C. Cir. 2001) (same for sale of credit reports).
19 Businesses use children’s data for a commercial purpose: to increase engagement and create and
20 sell advertising. Egelman Decl. ¶¶12–13. Plaintiff concedes that “many online providers rely on
21 advertisements to earn a significant share of—or all of—the revenue that supports the content and
22 services they provide.” Pl. Br. 2. Thus, the Act qualifies as a commercial speech regulation: it
23 applies to specific products (those likely to be accessed by children); it addresses communications
24 that serve a commercial purpose; and, it protects consumers from harms in a commercial
25 marketplace. *See, e.g., Am. Acad. of Pain Mgmt. v. Joseph*, 353 F.3d 1099, 1106 (9th Cir. 2004).
26 Thus, AB 2273 is subject to, at most, intermediate scrutiny.

27 In any event, AB 2273 satisfies any applicable standard of scrutiny, including strict
28 scrutiny. The State has a compelling interest in protecting the physical, mental, and emotional

1 health and well-being of minors. Def. Br. 19–20. The Act does so in a narrowly tailored way by
2 protecting children from abusive and deceptive data collection and use practices on the products,
3 services, and features (hereinafter “products”) they are likely to access, while allowing collection
4 and use practices that do not cause harm. It regulates the businesses causing the most harm to
5 children. AB 2273 §1(a)(5); U.S. Surgeon General’s Advisory: Social Media & Youth Mental
6 Health (“Social Media Advisory”) 13–15 (2023), [https://www.hhs.gov/sites/default/files/sg-](https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf)
7 [youth-mental-health-social-media-advisory.pdf](https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf); see also *Burson v. Freeman*, 504 U.S. 191, 207
8 (1992) (“States adopt laws to address the problems that confront them. The First Amendment
9 does not require States to regulate problems that do not exist.”). The requirements of AB 2273 are
10 proven solutions and the least restrictive means of protecting children online. The scope of
11 existing children’s data privacy law leaves wide swaths of children unprotected. AB 2273
12 §1(a)(5); Radesky Decl. ¶¶39, 98. And parents and children cannot, and do not want to attempt to,
13 solve these problems alone. Def. Br. 21; Social Media Advisory 13; Radesky Decl. ¶95.

14 Finally, to the extent that the court invalidates any individual provision of AB 2273, the
15 remaining provisions should stand because each is grammatically, functionally, and volitionally
16 severable. See *Calfarm Ins. Co. v. Deukmejian*, 771 P.2d 1247, 1256 (Cal. 1989) (en banc). Each
17 provision is distinct, separate, and independently advances the State’s compelling interest in
18 protecting children’s physical, mental, and emotional health and well-being. See *id.*

19 **DPIA Requirement** (Cal. Civ. Code §§1798.99.31(a)(1)–(4) (all statutory references are to
20 Cal. Civ. Code)): Businesses currently take a reactive, rather than proactive, approach to risk
21 management; mitigation efforts are routinely made only after a child gets hurt. Radesky Decl.
22 ¶¶40–44. This approach compromises children’s safety. To take just one example, Snapchat only
23 ended the use of its speed filter after it had already been linked to multiple adolescent reckless
24 driving incidents and fatalities. *Id.* ¶41; *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021).
25 Harms like these might have been averted had companies adopted a safety-first approach and
26 received more guidance. Radesky Decl. ¶¶33, 40–41; Social Media Advisory 13–14. Under these
27 provisions, businesses must assess how their products use children’s data and whether their data
28 management practices or product designs pose risks to children, and make a plan to mitigate any

1 risk identified in the assessment. As a result, businesses will be proactive and fewer children will
2 be subject to preventable harms. ICO Decl. ¶¶65–67; Radesky Decl. ¶¶90–91. The assessment
3 and mitigation plan are confidential, so businesses can focus on identifying and mitigating
4 potential harm without fear of public scrutiny or revealing trade secrets.

5 This provision is severable from the Act’s other requirements. Additionally, each individual
6 assessment factor is severable as they are distinct, separate, and independently advance the
7 provision’s goal. The cure period, §1798.99.35(c), is likely not severable from this provision.

8 **Age-Appropriate Data Protection** (§§1798.99.31(a)(5), (b)(8)): Protecting children’s data
9 and privacy “necessarily means greater security and well-being.” AB 2273 §1(a)(4). Under
10 federal law, certain businesses “must establish and maintain reasonable procedures to protect”
11 and “take reasonable steps to release children’s personal information only to service providers
12 and third parties who are capable of maintaining the confidentiality, security, and integrity of”
13 children’s data. 16 C.F.R. §312.8. However, these protections apply only when the business
14 knows the user is under 13 or the service is directed to children. *Id.* §312.2. These limitations
15 omit many children from this enhanced protection. AB 2273 §1(a)(5); Radesky Decl. ¶¶39, 87;
16 Egelman Decl. ¶¶44–45; *see also* Social Media Advisory 15 (calling for a higher standard of data
17 privacy for children). AB 2273 rectifies this problem by requiring businesses to provide data and
18 privacy protections to users based on estimated age or, if the business does not estimate age,
19 apply child-appropriate data and privacy protections to all users. Unlike federal law, it protects all
20 children and covers products likely to be accessed by children. Further, this provision regulates
21 only privacy and data protections, allows increasingly permissive data use policies based on age,
22 and need not impact the privacy and data protections applied to adult users. It does not impede
23 businesses’ data collection and use any more than is necessary to protect children.

24 This provision is severable from the Act’s other requirements. No other requirement relies
25 on estimated age. The only other provision referencing age estimation mandates that such
26 information be used only for compliance with this provision, §1798.99.31(b)(8), and would be
27 made obsolete if this provision was invalidated.

28 **High Default Privacy Settings** (§1798.99.31(a)(6)): High privacy settings demonstrably

1 keep children safe. Radesky Decl. ¶¶57–60. For example, when children’s profiles are made
2 public by default, they receive harassing messages from strangers and advertisers—some
3 containing explicit content—within days of opening an account. *Id.*; Social Media Advisory 9.
4 Solutions like creating privacy by default help to mitigate these problems. Radesky Decl. ¶¶57–
5 60; Social Media Advisory 16 (calling for high default privacy settings for children). Existing law
6 does not require high privacy settings by default for children or anyone else. This provision
7 applies default settings only to child-users and allows users to change the default settings.
8 Businesses may also set different default settings when doing so is in the best interest of children.

9 This provision is severable from the Act’s other requirements. Businesses can understand
10 and fulfill this provision’s requirements regardless of their compliance with the Age-Appropriate
11 Data Protection provision or any other provision.

12 **Age-Appropriate Policy Language** (§1798.99.31(a)(7)): Businesses’ policies are often
13 inscrutable to adults, let alone to children. Egelman Decl. ¶¶18–19, 24–27, 52. This provision
14 protects the safety and well-being of minors by requiring that businesses provide policies and
15 standards concisely, prominently, and using clear language suited to the age of the children likely
16 to access the product, thus giving children the tools to make informed decisions about the services
17 with which they interact. No existing law provides such protection. This provision is severable.
18 Businesses can fulfil this provisions’ requirements regardless of their compliance with the Policy
19 Enforcement provision or any other provision.

20 **Restriction on Monitoring and Tracking** (§1798.99.31(a)(8)): This provision protects
21 children’s privacy, which “necessarily means greater security and well-being,” AB 2273 §1(a)(4),
22 by requiring an obvious signal to children when they are being monitored or tracked by another
23 user. Even when children are aware of tracking, they are susceptible to believing that a product
24 stops collecting information from them once they are no longer actively engaged with that
25 product, even when that is not true. Radesky Decl. ¶46(d). Providing an signal alerts children that
26 their data is still being collected. This empowers them to make informed decisions about whether
27 and when to give others access to their information. This provision is severable from the Act’s
28 other requirements. It is not cross-referenced in or dependent on any other provision.

1 **Internal Policy Enforcement** (§1798.99.31(a)(9)): In order for children and parents to
2 make informed decisions about the products children access, businesses have to be accountable
3 for the commitments they make to these consumers. Radesky Decl. ¶93. Businesses need only
4 commit to the policies they intend to follow and to the extent they intend to follow them. *Barnes*
5 *v. Yahoo, Inc.*, 570 F.3d 1096, 1108 (9th Cir. 2009). This provision narrowly creates that
6 accountability while in no way limiting the ability of businesses to adopt, reject, or change any
7 policy at any time. While state law requires privacy policies and prohibits false advertising, there
8 is no law holding online businesses accountable for enforcing their own policies. Def. Br. 14–15.

9 This provision is severable. It is not cross-referenced in or dependent on any other
10 provision. While the Age-Appropriate Language provision regulates policy clarity, this provision
11 regulates policy enforcement.

12 **Responsive Tools** (§1798.99.31(a)(10)): Businesses’ lack of response to child and parent
13 concerns is a pervasive problem; even parents of children whose deaths were linked to a specific
14 online product have been ignored by businesses. Radesky Decl. ¶94; Social Media Advisory 16
15 (calling for responsive tools). This provision narrowly addresses this problem by requiring tools
16 to help children exercise their privacy rights and report concerns. This provision is severable from
17 the Act’s other requirements. It is not cross-referenced in or dependent on any other provision.

18 **Knowingly Harmful Use of Children’s Data** (§1798.99.31(b)(1)): Studies showing
19 businesses using children’s data in ways that cause harm are plentiful. Radesky Decl. ¶¶48–71;
20 Social Media Advisory 6–10. To name just one example, Facebook uses children’s personal
21 information to profile them and place them into interest categories such as alcohol, gambling, and
22 extreme weight loss. Radesky Decl. ¶66. Advertisers can then target specific populations like
23 teenagers interested in alcohol through means like posting on children’s personalized feeds. *Id.*
24 This provision prohibits such practices and narrowly targets data use that businesses know will
25 cause harm, while still allowing businesses to use data in non-detrimental ways and ensuring that
26 they will not be penalized for unknowing violations. This provision is severable from the Act’s
27 other requirements because it is not cross-referenced in or dependent on any other provision.

28 **Profiling Children by Default** (§1798.99.31(b)(2)): As explained above, profiling by

1 default is common because it allows businesses to place users into categories for advertisers.
2 Radesky Decl. ¶66. But profiling can be harmful to children, who are easily influenced and
3 particularly vulnerable to being profiled based on passing interests and behaviors, and
4 assumptions about their similarity to other children. *Id.* ¶89; AB 2273 §1(a)(8); Social Media
5 Advisory 5. Children need to be able to explore, learn, and play without being subject to such
6 categorization. Radesky Decl. ¶89; AB 2273 §1(a)(3). This provision narrowly prohibits profiling
7 by default when done solely for the benefit of businesses, but allows it where necessary to
8 provide services with which children are actively and knowingly engaged or when in the best
9 interest of children. Disabling profiling is also the least restrictive means of protecting children. It
10 does not require businesses to restrict children’s access to content and leaves other kinds of
11 advertising available. Radesky Decl. ¶89; Egelman Decl. ¶15. This provision is severable from
12 the Act’s other requirements. It is not cross-referenced in or dependent on any other provision.

13 **Restriction on Collecting, Selling, Sharing, and Retaining Children’s Data**

14 (§1798.99.31(b)(3)): Excessive data collection and use undoubtedly harms children. Children are
15 unable to avoid harmful unsolicited content—including extreme weight loss content and
16 gambling and sports betting ads—directed at them based on businesses’ data collection and use
17 practices. Radesky Decl. ¶¶63–67. This provision narrowly prohibits this kind of unnecessary and
18 harmful collection and use while allowing collection and use that is necessary for the provision of
19 the service, required by law, or in the best interest of the children. Further, while federal law
20 establishes similar requirements for some children, 16 CFR §312.10, no law covers all children or
21 services likely to be accessed by children. This provision is severable from the Act’s other
22 requirements. It is not cross-referenced in or dependent on any other provision.

23 **Unauthorized Use of Children’s Personal Information** (§1798.99.31(b)(4)): Where the

24 end user is a child, businesses may only use personal information for the reason for which it was
25 collected unless the additional use is in the best interest of the child. For example, a business that
26 uses a child’s IP address solely to provide access to its platform cannot also use the IP address to
27 sell ads. Federal law limits retention of children’s data to the time “necessary to fulfill the
28 purposes for which information was collected,” but does not protect children of all ages or govern

1 other uses of data. 16 CFR §312.10. This provision is severable from the Act's other requirements
2 because it is not cross-referenced in or dependent on any other provision.

3 **Precise Geolocation Information** (§1798.99.31(b)(5) & (6)): Geolocation can be helpful
4 to users, but children are particularly vulnerable to abuses including unknowingly sharing their
5 location or revealing sensitive details about themselves. Egelman Decl. ¶¶13–14; Radesky Decl.
6 ¶46(d). This provision narrowly addresses both of these vulnerabilities by allowing the collection
7 and use of precise geolocation information when strictly necessary to provide the requested
8 service, but limiting collection and use of that information to the time that collection is necessary
9 to provide the service and requiring businesses to provide an obvious signal while the information
10 is being collected. This provision is severable from the Act's other requirements because it is not
11 cross-referenced in or dependent on any other provision.

12 **Use of Dark Patterns** (§1798.99.31(b)(7)): Businesses use dark patterns to nudge children
13 into making decisions that are advantageous to businesses. Egelman ¶51. For example, a child
14 who allows a business to sell and share their data can continue to their desired activity with one
15 click, while a user who wants to protect their data is redirected to a separate page with confusing
16 or misleading instructions. Federal law limits this practice for some children, 16 CFR § 312.7, but
17 does not protect all children. Similarly, dark patterns can make it difficult or impossible for
18 children to avoid harmful content. For example, a child recovering from an eating disorder who
19 wants to avoid extreme dieting content must both contend with dark patterns that make it difficult
20 to unsubscribe from such content and attempt to reconfigure their data settings in the hope of
21 preventing unsolicited content of the same nature. Radesky Decl. ¶¶62–63, 97; Egelman Decl.
22 ¶51. These techniques are prevalent in child-directed online services and children are likely to be
23 more susceptible to manipulation than adults. Egelman Decl. ¶51; Radesky Decl. ¶¶55–56. This
24 provision prohibits the use of dark patterns only for reasons related to the State's compelling
25 interest: protecting children's safety, health, and well-being. This provision is severable from the
26 Act's other requirements. It is not cross-referenced in or dependent on any other provision.

27 For the reasons explained above, AB 2273 can withstand strict scrutiny and should be
28 upheld in its entirety.

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

Dated: August 15, 2023

Respectfully submitted,

ROB BONTA
Attorney General of California
ANYA M. BINSACCA
Supervising Deputy Attorney General
NICOLE KAU
Deputy Attorney General

/s/ Elizabeth K. Watson
ELIZABETH WATSON
Deputy Attorney General
Attorneys for Defendant

SA2022305631/43839329.docx

CERTIFICATE OF SERVICE

Case Name: NetChoice, LLC v. Rob Bonta

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

I hereby certify that on August 15, 2023, I electronically filed the following documents with the Clerk of the Court by using the CM/ECF system:

DEFENDANT'S SUPPLEMENTAL BRIEFING ON SCRUTINY AND SEVERABILITY

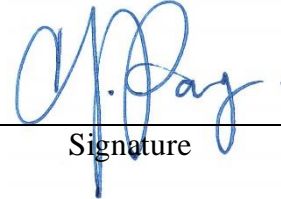
I certify that **all** participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

I declare under penalty of perjury under the laws of the State of California and the United States of America the foregoing is true and correct and that this declaration was executed on August 15, 2023, at San Francisco, California.

G. Pang

Declarant

SA2022305631/43839291.docx



Signature