

# **EXHIBIT 1**

1 AMBIKA KUMAR (*pro hac vice*)  
ambikakumar@dwt.com  
2 DAVIS WRIGHT TREMAINE LLP  
920 Fifth Avenue, Suite 3300  
3 Seattle, Washington 98104  
Telephone: (206) 757-8030

4 ADAM S. SIEFF (CA Bar No. 302030)  
5 adamsieff@dwt.com  
DAVIS WRIGHT TREMAINE LLP  
6 865 South Figueroa Street, 24th Floor  
Los Angeles, California 90017-2566  
7 Telephone: (213) 633-6800

8 DAVID M. GOSSETT (*pro hac vice*)  
davidgossett@dwt.com  
9 MEENAKSHI KRISHNAN (*pro hac vice*)  
meenakshikrishnan@dwt.com  
10 DAVIS WRIGHT TREMAINE LLP  
1301 K Street NW, Suite 500 East  
11 Washington, D.C. 20005  
Telephone: (202) 973-4200

12 ROBERT CORN-REVERE (*pro hac vice*)  
13 bob.corn-revere@thefire.org  
FOUNDATION FOR INDIVIDUAL RIGHTS AND EXPRESSION  
14 700 Pennsylvania Ave. SE, Suite 340  
Washington, DC 20003  
15 (215) 717-3473 Ext. 209

16 Attorneys for Plaintiff  
NETCHOICE, LLC d/b/a NetChoice

17  
18 IN THE UNITED STATES DISTRICT COURT  
19 THE NORTHERN DISTRICT OF CALIFORNIA  
20 SAN JOSE DIVISION

21 NETCHOICE, LLC d/b/a NetChoice,

22 Plaintiff,

23 v.

24 ROB BONTA, ATTORNEY GENERAL  
OF THE STATE OF CALIFORNIA,  
25 in his official capacity,

26 Defendant.  
27  
28

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

**FIRST AMENDED COMPLAINT FOR  
DECLARATORY AND INJUNCTIVE  
RELIEF**

Action Filed: December 14, 2022

## I. PRELIMINARY STATEMENT

1  
2 1. Although styled as a privacy regulation to protect minors, the California Age-  
3 Appropriate Design Code Act (AB 2273)<sup>1</sup> is a content-based restriction on speech that will subject  
4 a global communications medium to state supervision and hobble a free and open resource for  
5 “exploring the vast realms of human thought and knowledge.” *Packingham v. N. Carolina*, 137  
6 S. Ct. 1730, 1737 (2017).

7 2. Among its many infirmities, AB 2273 presses companies to serve as roving censors  
8 of speech on the Internet. The law imposes on private firms, big and small, the obligation to  
9 identify and “mitigate” speech that is “harmful or potentially harmful” to users under 18 years old,  
10 and to “prioritize” speech that promotes such users’ “well-being” and “best interests.” If firms  
11 guess the meaning of these inherently subjective terms wrong—or simply reach different  
12 conclusions than do government regulators—the State is empowered to impose crushing financial  
13 penalties. The State can also impose such penalties if companies fail to enforce their content  
14 moderation standards to the Attorney General’s satisfaction. AB 2273 does this without so much  
15 as a nod to whether the law’s restrictions are necessary to serve a compelling state interest.

16 3. Rather than protect minors, AB 2273 will harm them, along with the Internet as a  
17 whole. Faced with arbitrary application of AB 2273’s draconian penalties, online businesses will  
18 face overwhelming pressure to over-moderate content to avoid the law’s penalties for content the  
19 State deems harmful. Such over-moderation will restrict the availability of information for users  
20 of all ages and stifle important resources, particularly for vulnerable youth who rely on the Internet  
21 for life-saving information.<sup>2</sup> Separately, AB 2273 will require businesses to verify the ages of  
22 their users, which—to the extent it can even be done to the State’s satisfaction—will frustrate  
23 anonymous and casual browsing, magnify privacy concerns, and wrest control over minors’ online  
24 activities from parents and their children.

25  
26 <sup>1</sup> AB 2273 as enacted is docketed as ECF 1 Ex. A and is codified in relevant part beginning at Section 1798.99.28 to Part 4 of Division 3 of the California Civil Code.

27 <sup>2</sup> See “Coalition Letter on Privacy and Free Expression Threats in Kids Online Safety Act” Regarding Opposition to  
28 S. 3663 (Nov. 28, 2022) (“Online services would face substantial pressure to over-moderate, including from state Attorneys General seeking to make political points about what kind of information is appropriate for young people.”), available at <https://cdt.org/wp-content/uploads/2022/11/Coalition-letter-opposing-Kids-Online-Safety-Act-28-Nov-PM.pdf>.



1 State of California.” § 1798.99.35(a).

2 **III. JURISDICTION**

3 10. This action arises under the United States Constitution, particularly the Commerce  
4 Clause, art. I, § 8, cl. 3, and Supremacy Clause, art. VI, and the First, Fourth, and Fourteenth  
5 Amendments, as well as the California Constitution, art. I, §§ 2(a) and 7(a). It also arises under  
6 the Civil Rights Act, 42 U.S.C. §§ 1983 and 1988, the Communications Decency Act, 47 U.S.C.  
7 § 230, and COPPA, 15 U.S.C. §§ 6501 *et seq.*

8 11. This Court has subject-matter jurisdiction over this action under 28 U.S.C. §§ 1331,  
9 1343(a), and 1367(a) because NetChoice’s claims either arise under federal law or else share a  
10 common nucleus of operative fact with claims that arise under federal law.

11 12. This Court has authority under the Declaratory Judgment Act, 28 U.S.C. § 2201(a),  
12 to decide this dispute and award relief because it presents an actual case or controversy within the  
13 Court’s jurisdiction.

14 **IV. VENUE**

15 13. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) & (2) because  
16 Defendant performs his duties and thus resides in this District, and because the injuries giving rise  
17 to this action have been and will continue to be suffered by NetChoice and its members in Santa  
18 Clara County, California.

19 **V. DIVISIONAL ASSIGNMENT**

20 14. Assignment to the San Jose Division is proper under Local Civil Rule 3-2(c) & (e)  
21 because the injuries giving rise to this action have been and will continue to be suffered by  
22 NetChoice and its members in Santa Clara County, California.

23 **VI. FACTUAL ALLEGATIONS**

24 **A. Online Businesses and Website Architecture**

25 15. Online businesses interact with users in different ways. Most have universally  
26 accessible areas, in which a user can view product listings, preview services, and read reviews  
27 without creating or logging into an account. Many online businesses also have features that are  
28 optimized and available only for individuals who create an account or sign up for membership.

1 Some social media services, for example, permit non-members to view public portions of a user’s  
2 profile, but not to view each post in detail. Similarly, many online businesses require users to  
3 create accounts before they can use or purchase an online service.

4 16. Some businesses opt for a free account-based model, where access to online  
5 services is provided without charge, but users must provide certain information and create accounts  
6 to access those services. Other businesses use a subscription-based model requiring users to create  
7 accounts and pay fees to use the online service. Irrespective of model, many online businesses  
8 rely on advertisements to earn a significant share of—and in some cases, *all* of—the revenue that  
9 supports the content and services they provide.

10 17. Many online businesses that are principally ad-supported publish and deliver  
11 content to users, who engage with particular content by, for example, writing a review, reading a  
12 news article, downloading a movie, streaming an album, “liking” a post, or purchasing books based  
13 on author or genre. This engagement, in turn, enables online businesses to serve users with  
14 advertisements or marketing targeted to their expressed interests.<sup>3</sup> Ads can appear alongside  
15 hosted content, in promoted search results, or in email marketing or newsletters. At its core,  
16 targeted advertising leverages technology to improve commercial speech and makes possible a  
17 wide range of protected *non-commercial* speech. Advertisers pay a premium for the ability to  
18 reach a more specific audience; users benefit from subsidized access to content and more relevant  
19 advertisements; and online business operators—including smaller niche bloggers and individual  
20 “influencers” who use larger services—are able earn a living by monetizing their talents for  
21 creating, curating, and publishing popular and interesting content.<sup>4</sup>

22 18. Even independently of advertising, content promotion is a key service that online  
23 businesses offer—and often a key source of revenue. An online service’s ability to suggest a new  
24 release based on the user’s browsing history, for example, creates value for the user, generates  
25 business for the service, and connects content creators with an audience. This is true across

---

26 <sup>3</sup> See generally David S. Evans, “The Economics of the Online Advertising Industry,” 7 REV. OF NETWORK ECON. 3  
27 (2008), available at <https://doi.org/10.2202/1446-9022.1154>.

28 <sup>4</sup> See, e.g., Joel Matthew, “Understanding Influencer Marketing And Why It Is So Effective,” FORBES (July 30, 2018),  
available at <https://tinyurl.com/3fr7zban>; Jacob Goldenberg *et al.*, “The Research Behind Influencer Marketing,” J.  
OF MARKETING RESEARCH (Feb. 2021), available at <https://tinyurl.com/2j2863m5>.

1 industry—music, movies, television shows, social media posts, and anything else an Internet user  
2 might be interested in purchasing, reading, hearing, or viewing.

3 **B. AB 2273**

4 19. On September 15, 2022, California Governor Gavin Newsom signed AB 2273.

5 20. According to the Assembly bill analysis, one of the Act’s overarching purposes is  
6 to favor certain types of online speech by “elevat[ing] child-centered design in online products and  
7 services that are likely to be accessed by children.”<sup>5</sup> AB 2273 includes legislative findings that  
8 “the design of online products and services on children’s well-being has become a focus of  
9 significant concern,” and that “children should be afforded protections not only by online products  
10 and services specifically directed at them, but by all online products and services they are likely to  
11 access.” AB 2273 § 1(a)(2), (a)(5).

12 **1. The breadth of businesses affected by AB 2273**

13 21. AB 2273 applies to any “business that provides an online service, product, or  
14 feature likely to be accessed by children.” § 1798.99.31(a)-(b). The law defines “children” as any  
15 “consumer or consumers who are under 18 years of age.” § 1798.99.30(b)(1). This definition  
16 encompasses “children” old enough to drive and who might be just days shy of the right to vote,  
17 the right to buy and sell property, the right to marry without parental consent, and the obligation  
18 to serve on a jury.

19 22. The law incorporates the definition of “business” set forth in California Civil Code  
20 Section 1798.140(c), which, pursuant to a recent amendment effective January 1, 2023, reaches  
21 major enterprises that earn more than \$25,000,000 in gross annual revenues, as well as small  
22 websites that buy, sell, or merely share information from as few as 100,000 visitors annually, or  
23 that obtain more than half their revenue from data monetization. Not-for-profit and governmental  
24 entities are excluded.

25 23. Although AB 2273 purports to regulate “online service[s], product[s], or  
26 feature[s],” the statute in fact regulates speech. AB 2273’s references to “system design features,”  
27

28 <sup>5</sup> AB 2273 California Assembly Floor Analysis (Aug. 22, 2022), available at [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=202120220AB2273#](https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202120220AB2273#).

1 “algorithms,” and “targeted advertising systems” all refer to the methods used to disseminate or  
2 circulate speech on the Internet. This fact is underscored by Section 1798.99.30(b)(5)(C), which  
3 clarifies that AB 2273’s reach excludes “the delivery or use of a physical product.”

4 24. AB 2273 defines “likely to be accessed by children” to “mean[] it is reasonable to  
5 expect, based on the following indicators, that the online service, product, or feature would be  
6 accessed by children”:

- 7 (A) The online service, product, or feature is directed to children as defined by  
8 the Children’s Online Privacy Protection Act (15 U.S.C. Sec. 6501 *et seq.*).  
9 (B) The online service, product, or feature is determined, based on competent  
10 and reliable evidence regarding audience composition, to be routinely  
11 accessed by a significant number of children.  
12 (C) An online service, product, or feature with advertisements marketed to  
13 children.  
14 (D) An online service, product, or feature that is substantially similar or the  
15 same as an online service, product, or feature subject to subparagraph (B).  
16 (E) An online service, product, or feature that has design elements that are  
17 known to be of interest to children, including, but not limited to, games,  
18 cartoons, music, and celebrities who appeal to children.  
19 (F) A significant amount of the audience of the online service, product, or  
20 feature is determined, based on internal company research, to be children.

21 § 1798.99.30(b)(4).

22 25. This definition is vague and potentially limitless, given that AB 2273 defines  
23 “children” as all individuals under 18. It is also content-based, as companies must look to the  
24 subject matter of their speech—for example, whether they host “advertisements marketed to  
25 children” or “cartoons, music and celebrities who appeal to children”—to understand whether they  
26 are within the scope of the law.

27 26. As a practical matter, the law extends so widely as to sweep in the vast majority of  
28 companies operating online. The following services, for example, would likely qualify:

- 29 a. All major news outlets, including The New York Times, Wall Street  
30 Journal, and Washington Post; ABC, CBS, and NBC; CNN, Fox News, and  
31 MSNBC; as well as a significant number of local news services.  
32 b. The websites of every major sports league, including MLB, MLS, NBA,  
33 NFL, and NHL, and sports outlets serving the United States, including  
34 ESPN, FiveThirtyEight, the Golf Channel, NBC Sports, Sports Illustrated,  
35 Telemundo, and Yahoo Sports.



- c. Most online magazines and podcast channels.
- d. E-books and e-reader apps, as well as book forums.
- e. Online education and credential programs.
- f. Social media services.
- g. Video and music streaming services.
- h. Online video games.
- i. Individual blogs and discussion forums, such as those focused on news, economics, political science, ballet, fashion, cooking, chronic illness, physical fitness, mental health, sexuality, religion, history, video games, and countless other topics.
- j. Online self-help and suicide-prevention services that treat both adult and child populations.

27. If the law is allowed to take effect, AB 2273 would impose impermissible burdens on an extraordinary range of covered businesses and could result in a fundamentally changed Internet.

## **2. The law's Data Protection Impact Assessments**

28. Section 1798.99.31(a)(1) of AB 2273 mandates that “[b]efore any new online services, products, or features are offered to the public,” a covered business must (i) complete a “Data Protection Impact Assessment” (DPIA) for “any online service, product, or feature likely to be accessed by children”; (ii) maintain documentation of the DPIA for as long as that service, product, or feature is likely to be accessed by children; and (iii) biennially review all its DPIAs. A service must complete a DPIA “on or before July 1, 2024, for any online service, product, or feature likely to be accessed by children offered to the public *before* July 1, 2024,” § 1798.99.33(a) (emphasis added)—that is, for all existing covered services, products, and features. Accordingly, online businesses must take significant steps *now* to plan for and implement eventual compliance with AB 2273, long *before* AB 2273’s purported effective date.

29. Each DPIA must describe “the risks of material detriment to children that arise from the data management practices” related to that online product, service, or feature. It must also state whether the service, product, or feature “could” “harm” minors in various ways, such as by exposing them to “potentially harmful” content, contacts, and conduct; whether algorithms or “targeted advertising” “could harm children”; and whether and how the product, service, or feature

1 “uses system design features to increase, sustain, or extend use of the online product, service, or  
2 feature by children, including the automatic playing of media, rewards for time spent, and  
3 notifications.” § 1798.99.31(a)(1)(B). In conjunction with the DPIA, the business must also  
4 “create a timed plan to mitigate or eliminate” any risks identified in the DPIA “before the online  
5 service, product, or feature is accessed by children.” § 1798.99.31(a)(2).

6 30. The Act does not define the terms “material detriment,” “harm,” or “harmful.”  
7 Thus, the Attorney General apparently has discretion to deem *any* type of asserted harm—however  
8 the Attorney General defines “harm,” and notwithstanding that others might disagree—as  
9 constituting a “risk of material detriment” that must be documented. A business could be expected  
10 to document the risks, for example, that photographs and videos depicting the global effects of  
11 climate change, the war in Ukraine, school shootings, or atrocities in Syria could cause minors  
12 anxiety; or that a content recommendation for the next episode of a cartoon TV series could “harm”  
13 a minor who is struggling to focus on homework or to get more exercise.

14 31. The possibility that the State might consider a particular piece of content or feature  
15 “harmful” to some or all minors, combined with the risk of having been found to violate the law  
16 due to an inadequate DPIA, will pressure businesses to identify distant or unlikely harms—and to  
17 self-censor accordingly.

18 32. Under the Act, the California Attorney General may at any time order a covered  
19 entity to provide him with any DPIA that it has completed, or with a list of all DPIAs it has  
20 completed. §1798.99.31(a)(3)-(4).

21 33. The DPIA requirement applies equally to large global services and single-person  
22 blogs, so long as they meet California’s definition of a “business.” As one independent journalist  
23 explained about his own publication: “Our comment system? DPIA. Our comment voting? DPIA.  
24 Our comment promotion? DPIA. The ability to listen to our podcast? DPIA. The ability to share  
25 our posts? DPIA. The ability to join our insider chat? DPIA. The ability to buy a t-shirt? DPIA.  
26 The ability to post our stories to Reddit, Twitter, Facebook, or LinkedIn? DPIA (for each of those,  
27 or can we combine them? I dunno). Our feature that recommends similar articles? DPIA. Search?

28

1 DPIA. Subscribe to RSS? DPIA.”<sup>6</sup>

2 **3. The statute’s age verification requirements**

3 34. Section 1798.99.31(a)(5) requires regulated businesses to “[e]stimate the age of  
4 child users with a reasonable level of certainty appropriate to the risks that arise from the data  
5 management practices of the business or apply the privacy and data protections afforded to children  
6 to all consumers.”

7 35. The Act does not define “reasonable level of certainty appropriate to the risks.”  
8 Left in the dark, covered businesses must either configure the privacy settings for each of their  
9 offerings to their most speech- and content-restrictive levels for all users regardless of age, or  
10 attempt to verify the age of users with near certainty.

11 36. But age certainty is not realistic. Age verification technologies are inherently  
12 unreliable.<sup>7</sup> Most methods rely on users either to attest to their ages or to submit official documents  
13 verifying their ages.<sup>8</sup> For users determined to bypass the rules, there are “straightforward  
14 workarounds” to both of these methods, which businesses often cannot avert.<sup>9</sup> And any method  
15 that involves submitting official documents increases the risk that those documents could be stolen  
16 or leaked.<sup>10</sup> More invasive age-verification methods—such as artificial intelligence, facial  
17 analysis, or facial recognition technologies—are far from foolproof and pose their own  
18 transparency, security, and privacy concerns.<sup>11</sup> To the extent AB 2273’s “reasonable . . . certainty”  
19 standard effectively requires companies to adopt such invasive age-verification methods, the law  
20 likely conflicts with other states’ privacy laws—such as laws that regulate the collection of

21 \_\_\_\_\_  
22 <sup>6</sup> Mike Masnick, “Dear California Law Makers: How The Hell Can I Comply With Your New Age-Appropriate  
23 Design Code,” TechDirt (Aug. 24, 2022), available at [https://www.techdirt.com/2022/08/24/dear-california-law-  
24 makers-how-the-hell-can-i-comply-with-your-new-age-appropriate-design-code/](https://www.techdirt.com/2022/08/24/dear-california-law-makers-how-the-hell-can-i-comply-with-your-new-age-appropriate-design-code/).

25 <sup>7</sup> French National Commission on Information and Liberties, “Online Age Verification: Balancing Privacy and the  
26 Protection of Minors” (Sept. 22, 2022) (concluding that age verification mandates are “inevitably imperfect” because  
27 they “can easily be circumvented,” noting that “23% of minors say they can bypass blocking measures”), available at  
28 <https://tinyurl.com/yzv7ynem>.

<sup>8</sup> Jackie Snow, “Why Age Verification Is So Difficult for Websites,” WALL ST. J. (Feb. 27, 2022), available at [https://  
on.wsj.com/3R0ORMT](https://on.wsj.com/3R0ORMT).

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> See David McCabe, “Anonymity No More? Age Checks Come to the Web,” N.Y. TIMES (Oct. 27, 2021), available  
at <https://nyti.ms/3S6U2ME>.

1 biometric data—and subjects online businesses to a patchwork of inconsistent obligations.  
2 Perversely, AB 2273 contradicts the consumer-data-minimization mandates of the State’s own  
3 privacy law, the California Privacy Rights Act (CPRA), and might well result in a net loss of  
4 privacy for California minors and adults alike.

5 37. In practice, many online businesses are likely to respond to the law by offering to  
6 the public only what they predict the Attorney General will deem suitable for the youngest  
7 children. The resulting system of self-censorship will dramatically change the vibrant and  
8 egalitarian “modern public square” online. *Packingham*, 137 S. Ct. at 1737.

9 **4. *The statute’s requirements for the display and enforcement of policies,***  
10 ***terms, and standards***

11 38. Section 1798.99.31(a)(9) requires businesses to “[e]nforce published terms,  
12 policies, and community standards established by the business, including, but not limited to,  
13 privacy policies and those concerning children.”

14 39. This far-reaching provision empowers the government to oversee and second-guess  
15 whether an online publisher has correctly enforced its own discretionary content moderation  
16 standards. Content moderation requires discretionary judgment about what speech to permit and  
17 whether content is, for example, racist, sexist, inflammatory, spiteful, threatening, or otherwise out  
18 of step with an online publisher’s values. Different businesses might reach different conclusions  
19 depending on the type of community they are trying to create. Federal law explicitly recognizes  
20 that such editorial judgment is both discretionary and cannot be regulated by the government. 47  
21 U.S.C. § 230(c)(2).

22 40. Section 1798.99.31(a)(9) eliminates both this discretion as well as the element of  
23 private action by empowering the State to penalize any covered business that fails to adequately  
24 enforce its own editorial standards and policies. Permitting the State to monitor an online  
25 publisher’s content moderation decisions intrudes into the publisher’s right to make editorial  
26 decisions about the types of content to host or exclude in pursuit of its mission, and incentivizes  
27 publishers to forgo content moderation altogether—a dire prospect for content-sharing services,  
28

1 for which content moderation *is* the product they provide.<sup>12</sup>

2 **5. The statute’s prohibitions on use of information**

3 41. AB 2273 prohibits covered services from taking actions that are otherwise protected  
4 by the Constitution or federal law.

5 42. First, Section 1798.99.31(b)(1) forbids an online service from using “the personal  
6 information of any child in a way that the business knows, or has reason to know, is materially  
7 detrimental to the physical health, mental health, or well-being of a child.” Under this rule, an  
8 online business must guess what constitutes a use that is “materially detrimental” to the mental or  
9 physical health—or to the even more amorphous concept of the “well-being”—of a child or teen.

10 43. Second, Section 1798.99.31(b)(3) bars a business from collecting, selling, sharing,  
11 or retaining “any personal information that is not necessary to provide an online service, product,  
12 or feature with which a child is actively and knowingly engaged,” unless “the business can  
13 demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal  
14 information is in the best interests of children likely to access the online service, product, or  
15 feature.” The law does not define or delimit what might constitute “the best interests of children”  
16 or what might constitute a “compelling reason” for the use of information.

17 44. Third, if the “end user is a child,” Section 1798.99.31(b)(4) precludes a business  
18 from using “personal information for any reason other than a reason for which that personal  
19 information was collected, unless the business can demonstrate a compelling reason that use of the  
20 personal information is in the best interests of children.” This requirement too is plagued by  
21 generalities and undefined terms.

22 45. Beyond vague mandates and undefined purposes, these provisions on their face also  
23 expressly disallow a range of commonplace online speech, including engaging with users to learn  
24 their preferences; using collected information for personalized advertising; providing users  
25 recommendations about books, movies, newspaper articles and other content; or even sending  
26 automated email updates to users.

27  
28 <sup>12</sup> See, e.g., Caitlin Vogus, “Chilling Effects on Content Moderation Threaten Freedom of Expression for Everyone,”  
Center for Democracy & Technology (July 26, 2021), available at <https://tinyurl.com/2p87nvv9>.

1           46.     Guessing wrong about what these provisions proscribe is prohibitively expensive—  
 2 penalties for even negligent errors could exceed \$20 billion. Many services will not or cannot risk  
 3 it. Instead, they will self-censor by banning users whose age they cannot verify; refrain from  
 4 publishing content to certain users; disable editorial features that control the publication, curation,  
 5 and promotion of content on their services; forego efforts to connect their customers with  
 6 suggested content or other users; or shut down altogether. The law poses an existential risk in  
 7 particular to websites that rely on advertising to support dissemination of speech to and among  
 8 users.

9                           **6.     *The statute’s ban on using “dark patterns”***

10           47.     Section 1798.99.31(b)(7) prevents a business from “us[ing] dark patterns to lead or  
 11 encourage children to,” among other things, “take any action that the business knows, or has reason  
 12 to know, is materially detrimental to the child’s physical health, mental health, or well-being.”

13           48.     By incorporation, AB 2273 defines “dark patterns” as “a user interface designed or  
 14 manipulated with the substantial effect of subverting or impairing user autonomy, decision-  
 15 making, or choice.” Cal. Civ. Code § 1798.140(l). Although the statutory term is calculated to  
 16 sound nefarious, it has been construed to reach benign and widely used features such as “autoplay”  
 17 and “newsfeed” functions that use programmed algorithms and machine learning to recommend  
 18 personalized content—features designed to simplify and improve the customer experience.<sup>13</sup>

19           49.     The uncertainty inherent in this prohibition will cause it to sweep far too broadly,  
 20 and inevitably chill programmed editorial decisions to select, promote, and moderate content to  
 21 audiences. This includes a newspaper website recommending articles, a social media platform  
 22 recommending posts, a music- or video-streaming service promoting customized playlists and  
 23 movies based on prior viewing history, a video-sharing platform promoting particular popular  
 24 videos, and an independent blogger pushing out new-post alerts to followers.

25           50.     To comply with this provision, online businesses must either guess whether any of  
 26

27 <sup>13</sup> See, e.g., Katharine Miller, “Can’t Unsubscribe? Blame Dark Patterns,” Stanford University Institute for Human-  
 28 Centered Artificial Intelligence (Dec. 13, 2021) (explaining that the “[a]utoplay” feature on YouTube by which “an  
 algorithm automatically plays the next video and will endlessly serve you more and more content” is recognized as “a  
 dark pattern”), available at <https://tinyurl.com/3em4ckzw>.

1 these content-promotion decisions might be construed to have a “materially detrimental” effect on  
2 a minor before publishing—hoping, again, that they have predicted correctly and that their  
3 predictions match the government’s own subjective assessments—or elect to self-censor. As with  
4 other provisions of AB 2273, many online services are likely to choose self-censorship.

5 \* \* \* \* \*

6 51. The well-being of children is undisputedly of great importance. But AB 2273  
7 regulates far beyond privacy, is not confined to children, and is unnecessary to achieve the  
8 Legislature’s purported privacy goals. The Act will run roughshod over the constitutional and  
9 statutory rights of online services—and ordinary citizens who use and rely on those services—in  
10 a misguided effort to redesign the Internet and restrict speech.

11 **VII. LEGAL PRINCIPLES**

12 52. The provisions of AB 2273 must be evaluated pursuant to federal and state  
13 constitutional limits, as well as federal statutory restrictions.

14 **A. The First Amendment**

15 53. Content-based, viewpoint-based, and speaker-based laws that restrict or burden  
16 speech are presumptively unconstitutional under the First and Fourteenth Amendments. This  
17 principle extends to the editorial judgments of editors and publishers, both as to their own speech  
18 as well as the speech of others. This is true for online media as much as traditional publications  
19 because “the basic principles of freedom of speech and the press, like the First Amendment’s  
20 command, do not vary when a new and different medium for communication appears.” *Brown v.*  
21 *Entm’t Merchants Ass’n*, 564 U.S. 786, 790 (2011) (citation and internal quotation marks omitted).

22 54. Online businesses, including NetChoice’s members, regularly publish content and  
23 make editorial decisions regarding what content to publish, edit, and remove. It is a long-held and  
24 firmly established constitutional principle that such speech is fully protected by the First  
25 Amendment. *Reno v. ACLU*, 521 U.S. 844, 871-72 (1997).

26 55. The First Amendment prohibits prior restraints on speech, including state action  
27 designed to deputize private actors to serve as censors by proxy. *Denver Area Educ. Telecomm.*  
28 *Consortium, Inc. v. F.C.C.*, 518 U.S. 727, 754 (1996). Any government regulation that “subject[s]

1 the distribution of publications to a system of prior administrative restraints,” including a “system  
2 of informal censorship” to promote “juvenile morality” and well-being, carries “a heavy  
3 presumption against its constitutional validity.” *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70-  
4 71 (1963).

5 56. Only certain limited and narrowly defined categories of speech are unprotected by  
6 the First Amendment—defamation, incitement, obscenity, and speech integral to criminal  
7 conduct—and the Supreme Court has rejected efforts to expand these categories as “startling and  
8 dangerous.” *United States v. Stevens*, 559 U.S. 460, 470 (2010). In particular, the Court previously  
9 rejected as “unprecedented and mistaken” California’s attempt to create “a wholly new category  
10 of content-based regulation that is permissible only for speech directed at children.” *Brown*, 564  
11 U.S. at 794. A state’s legitimate interest in child welfare thus “does not include a free-floating  
12 power to restrict the ideas to which children may be exposed.” *Id.* “Speech that is neither obscene  
13 as to youths nor subject to some other legitimate proscription cannot be suppressed solely to protect  
14 the young from ideas or images that a legislative body thinks unsuitable for them.” *Erznoznik v.*  
15 *City of Jacksonville*, 422 U.S. 205, 213-214 (1975).

16 57. Outside the categories of unprotected speech, the First Amendment prohibits the  
17 government from engaging in content-based regulation unless the government can establish that  
18 the measure is (i) necessary to advance a “compelling” governmental interest, (ii) narrowly tailored  
19 to serve that interest, and (iii) the least restrictive means available to achieve that interest. *United*  
20 *States v. Playboy Entm’t Grp., Inc.*, 529 U.S. 803, 813 (2000). Within this protected sphere, the  
21 government cannot dictate a private business’s decisions about what to say or what content to  
22 disseminate. *Miami Herald Publ’g Co. v. Tornillo*, 418 U.S. 241, 258 (1974). Nor can the  
23 government unduly burden or chill protected speech, or discriminate among speakers, particularly  
24 where such restrictions “reflect the Government’s preference for the substance of what the favored  
25 speakers have to say (or aversion to what the disfavored speakers have to say).” *Turner Broad.*  
26 *Sys., Inc. v. F.C.C.*, 512 U.S. 622, 658 (1994).

27 58. In addition to prohibiting *restrictions* on speech, the First Amendment forbids the  
28 government from *compelling* speech in ways that burden and chill constitutionally protected



1 editorial and speech rights. A law “mandating speech that a speaker would not otherwise make”  
2 is “necessarily” a “content-based regulation of speech” subject to strict scrutiny because it “alters  
3 the content of the speech.” *Riley v. Nat’l Fed’n of the Blind of N. Carolina, Inc.*, 487 U.S. 781,  
4 795 (1988). Even compelled commercial disclosures must meet certain requirements to pass  
5 constitutional muster—namely, the standards alternatively articulated in *National Institute of*  
6 *Family & Life Advocates v. Becerra*, 138 S. Ct. 2361 (2018) (*NIFLA*), *Central Hudson Gas &*  
7 *Electric Corporation v. Public Service Commission*, 447 U.S. 557 (1980), and *Zauderer v. Office*  
8 *of Disciplinary Counsel*, 471 U.S. 626 (1985).

9 59. The First Amendment forbids states from imposing liability on publishers for  
10 hosting or promoting allegedly unlawful content unless the law imposing the liability requires the  
11 publisher to know the nature of the allegedly unlawful content. *Smith v. California*, 361 U.S. 147  
12 (1959).

13 60. A law is unconstitutionally overbroad if “a substantial number of its applications  
14 are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Stevens*, 559  
15 U.S. at 473 (citation omitted).

16 61. Vagueness in a law that regulates expression “raise[s] special First Amendment  
17 concerns because of its obvious chilling effect on free speech.” *Brown*, 564 U.S. at 807 (quoting  
18 *Reno*, 521 U.S. at 871-72).

## 19 **B. The Fourth Amendment**

20 62. Under the Fourth Amendment, “searches conducted outside the judicial process,  
21 without prior approval by a judge or a magistrate judge, are *per se* unreasonable, subject only to a  
22 few specifically established and well-delineated exceptions.” *City of Los Angeles v. Patel*, 576  
23 U.S. 409, 419 (2015) (cleaned up).

24 63. One exception to the warrant requirement involves an “administrative search” that  
25 seeks to “ensure compliance with [a] recordkeeping requirement.” *Id.* at 420. But to fall within  
26 this “administrative search exception,” “the subject of the search must be afforded an opportunity  
27 to obtain precompliance review before a neutral decisionmaker.” *Id.* A statutory regime that  
28 permits the government to search and seize the commercially sensitive information of an ordinarily

1 regulated business is thus “facially invalid” where it fails to afford such an opportunity to a party  
2 compelled to “turn over” records. *Id.* at 421.

3 **C. Vagueness and the Due Process Clause**

4 64. The Due Process Clause of the Fourteenth Amendment forbids vague laws—  
5 particularly those that regulate speech protected by the First Amendment.

6 65. The void-for-vagueness doctrine “guarantees that ordinary people have ‘fair notice’  
7 of the conduct a statute proscribes” and “guards against arbitrary or discriminatory law  
8 enforcement by insisting that a statute provide standards to govern the actions of police officers,  
9 prosecutors, juries, and judges.” *Sessions v. Dimaya*, 138 S. Ct. 1204, 1212 (2018).

10 66. A statute can be impermissibly vague either because “it fails to provide people of  
11 ordinary intelligence a reasonable opportunity to understand what conduct it prohibits,” or because  
12 “it authorizes or even encourages arbitrary and discriminatory enforcement.” *Hill v. Colorado*,  
13 530 U.S. 703, 732 (2000).

14 **D. The Dormant Commerce Clause**

15 67. Article I, Section 8 of the U.S. Constitution vests Congress with the power “to  
16 regulate Commerce ... among the several States.” U.S. Const., art. I, § 8, cl. 3. The Commerce  
17 Clause bars state laws that unduly restrict interstate commerce—a restriction on State action  
18 referred to as the “Dormant Commerce Clause.”

19 68. Under the Dormant Commerce Clause, even laws that regulate evenhandedly and  
20 do not purport to discriminate against other states are unconstitutional if they impose burdens on  
21 interstate commerce that are clearly excessive in relation to the putative local benefits. *See Pike*  
22 *v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970). The Dormant Commerce Clause likewise  
23 prohibits states from regulating activities, including speech, when the “practical effect of the  
24 regulation is to control conduct” that occurs “wholly outside” the regulating state’s jurisdiction.  
25 *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989).

26 **E. The Children’s Online Privacy Protection Act**

27 69. Enacted in 1998, the Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501  
28 *et seq.*, created a comprehensive federal scheme to facilitate parental control over children’s online

1 activities and to protect children’s privacy. COPPA defines a “child” as an “individual under the  
2 age of 13.” 15 U.S.C. §§ 6501(1). The Federal Trade Commission (FTC) has authority to enforce  
3 COPPA and has promulgated a rule to implement COPPA, which is known as the COPPA Rule.  
4 *See* 16 C.F.R. § 312.1 *et seq.*

5 70. COPPA makes it “unlawful for an operator of a website or online service directed  
6 to children, or any operator that has actual knowledge that it is collecting personal information  
7 from a child, to collect personal information from a child in a manner that violates the regulations  
8 prescribed” by the FTC. 15 U.S.C. §6502(a)(1). Online operators therefore cannot be liable under  
9 COPPA unless their service is explicitly “directed to children” under 13 or they have “actual  
10 knowledge” that they are collecting, using, or disclosing personal information from children under  
11 13. *Id.*; 16 C.F.R. § 312.2. These requirements are critical to ensuring that companies have  
12 sufficient notice to structure their activities to comply with COPPA, and to do so without unduly  
13 restricting their offerings for all users.

14 71. COPPA precludes states from imposing child-focused privacy rules that differ from  
15 those imposed by COPPA. *See* 15 U.S.C. § 6502(d) (forbidding states from imposing liability “in  
16 connection with an activity or action described in this chapter that is inconsistent with the treatment  
17 of those activities or actions under this section”).

18 72. Unlike AB 2273, COPPA places the decision-making where it should be—with  
19 parents and guardians—and requires covered operators to provide notice of and obtain parental  
20 consent to their privacy practices. The COPPA Rule mandates, for example, that a covered  
21 business “provide notice on the Web site or online service of what information it collects from  
22 children, how it uses such information, and its disclosure practices for such information,” 16  
23 C.F.R. § 312.3(a), and “obtain verifiable parental consent prior to any collection, use, and/or  
24 disclosure of personal information from children,” *id.* § 312.5.

25 **F. Section 230 of the Communications Decency Act**

26 73. Section 230 of the Communications Decency Act, 47 U.S.C. § 230, states that: “No  
27 provider or user of an interactive computer service shall be treated as the publisher or speaker of  
28 any information provided by another information content provider.” *Id.* § 230(c)(1). It also

1 prohibits the imposition of liability for “any action voluntarily taken in good faith to restrict access  
2 to or availability of material that the provider or user considers to be obscene, lewd, lascivious,  
3 filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is  
4 constitutionally protected.” *Id.* § 230(c)(2). An “interactive computer service” is “any information  
5 service, system, or access software provider that provides or enables computer access by multiple  
6 users to a computer server.” *Id.* § 230(f)(2). The “provider” of such a service includes those who  
7 own or operate websites and therefore includes NetChoice’s members that are subject to AB 2273.

8 74. With limited exceptions, Section 230(c)(1) bars the imposition of liability on a  
9 website for claims stemming from the publication of information provided by a third party.  
10 Publication includes not just determining whether to publish, continue to publish, or withdraw  
11 third-party content from publication, but also reviewing, editing, and prioritizing such content. A  
12 service’s decisions as to whether its content-moderation policies have been violated and how to  
13 address any violations, including whether and when to enforce those policies, are protected by  
14 Section 230(c)(2).

15 75. Congress adopted Section 230 to preserve and reinforce First Amendment  
16 protections for online services in light of the unique challenges of the medium. *Bennett v. Google,*  
17 *LLC*, 882 F.3d 1163, 1166 (D.C. Cir. 2018).

18 76. Section 230 expressly preempts inconsistent state laws that seek to hold online  
19 service providers liable for engaging (or failing to engage) in editorial and publishing functions  
20 protected by Section 230(c). 47 U.S.C. § 230(e)(3).

## 21 **VIII. CLAIMS FOR RELIEF**

### 22 **COUNT ONE:**

#### 23 **VIOLATION OF THE FIRST AND FOURTEENTH AMENDMENTS TO THE U.S.** 24 **CONSTITUTION, PURSUANT TO 42 U.S.C. § 1983, AND ARTICLE I, SECTION 2(A)** 25 **OF THE CALIFORNIA CONSTITUTION (FACIAL AND AS APPLIED)**

26 77. Plaintiff incorporates all prior paragraphs of this Complaint.

27 78. AB 2273 violates the expressive rights of NetChoice and its members under both  
the First Amendment and Article I, Section 2(a) of the California Constitution.

28 79. AB 2273 imposes a system of prior administrative restraints that require online

1 services to create DPIA reports for state inspection *before* publishing any “online service, product,  
2 or feature” to the public “likely to be accessed by” any user under the age of 18, including teens  
3 on the cusp of adulthood. Even if it were crystal clear which services meet the “likely to be  
4 accessed” standard or what kinds of content, features, and services constituted a potential harm,  
5 the requirement places online services under threat of government sanction for making any service  
6 available that could be considered harmful to minors and thus imposes a prior restraint. Service  
7 providers face state-imposed sanctions if they publish online without first producing a DPIA, and  
8 they face state sanctions even if they do provide a DPIA but fail to prepare “a timed plan to mitigate  
9 or eliminate the [undefined] risk before the online service, product, or feature is accessed by  
10 children.”

11 80. AB 2273 unconstitutionally deputizes online service providers to act as roving  
12 Internet censors at the State’s behest. Providers must (i) assess the undefined risks their services  
13 and content “could” pose to the “well-being” and “best interests” of children; (ii) devise a plan to  
14 prevent or mitigate any such risks; and (iii) develop, publish, and enforce terms of service and  
15 “community standards.” Failure to predict correctly how the State will choose to view those  
16 efforts, or to interpret the law’s unbounded and inherently subjective terms, invites the prospect of  
17 ruinous liability even for the largest companies. Against the threat of such liability, regulated  
18 entities will almost inevitably choose to restrain speech to comply with the State’s vague, content-  
19 based standards.

20 81. AB 2273 imposes a battery of viewpoint-, content-, and speaker-based restrictions  
21 on speech, and is thus subject to strict scrutiny. AB 2273 only applies, for example, to certain  
22 categories of speech (as defined in Section 1798.140) used by qualifying websites, and it selects  
23 among speakers by exempting not-for-profit and government speakers altogether. More  
24 fundamentally, for businesses that are covered, the law imposes rules and penalties based on what  
25 the content is and whether it is “materially detrimental” to the “mental health, or well-being of a  
26 child,” is strictly “necessary” to provide the service, or is in the “best interests” of minors. These  
27 restrictions “reflect the Government’s preference for the substance of what the favored speakers  
28 have to say (or aversion to what the disfavored speakers have to say),” and require strict scrutiny.

1 *Turner Broad. Sys.*, 512 U.S. at 658.

2 82. AB 2273 compels speech that a speaker would not otherwise make and thus  
3 necessarily operates as content-based regulation because it alters the content of speech.

4 83. AB 2273’s prior restraints, speech restrictions, and compelled speech requirements  
5 fail strict scrutiny and also would fail a lesser standard of scrutiny. The law does not serve a  
6 compelling government interest nor is it narrowly tailored to achieve any such interest. In fact, it  
7 fails to reference any specific legislative findings about the harms the Legislature seeks to address  
8 beyond a broadly professed interest in “privacy protections for children.” And even though the  
9 Legislature recognized that the “same data protection regime may not be appropriate for children  
10 of all ages,” AB 2273 § 1(a)(7), the statute imposes exactly that. The statute’s regime applies to  
11 minors of all ages, including teens, and in effect to the entire Internet. For the same reasons, these  
12 provisions fail intermediate and “exacting” scrutiny.

13 84. Section 1798.99.31(a)(1)-(4) compel businesses to create highly burdensome  
14 DPIAs. These provisions (i) effectuate an unconstitutional system of prior restraints; (ii) restrict  
15 and interfere with the editorial discretion of NetChoice and its members based on content and  
16 speaker; (iii) impermissibly compel speech on the basis of content according to the State’s  
17 assessment of what a DPIA must include; (iv) impermissibly compel disclosure of DPIAs to the  
18 Attorney General upon request and thus further compels speech on the basis of content; and at  
19 minimum (v) imposes an unduly burdensome compelled commercial speech requirement that is  
20 inconsistent with *NIFLA*, 138 S. Ct. 2361, *Central Hudson*, 447 U.S. 557, and *Zauderer*, 471 U.S.  
21 626.

22 85. Section 1798.99.31(a)(5) requires businesses to “estimate” the age of minor users  
23 to a “reasonable level of certainty” specific to each of the risks arising from businesses’ individual  
24 data management practices, or otherwise to universally apply child-appropriate settings before  
25 publishing content. This vague and overbroad provision is a prior restraint and will impermissibly  
26 chill the publication of protected speech to adult audiences, infringe on protections for anonymous  
27 speech, and deter users from services deploying the invasive age-verification mechanisms that AB  
28 2273 appears to require.

1           86.     Section 1798.99.31(a)(9) mandates that businesses enforce community standards  
2 and privacy policies. This provision violates the First Amendment on its face, and as applied to  
3 NetChoice’s covered members, to the extent it impermissibly (i) restricts businesses’ and  
4 NetChoice’s covered members’ ability to exercise their own editorial discretion regarding which  
5 content to leave up or take down, and what to publish or not to publish; (ii) imposes strict liability  
6 on businesses and NetChoice’s covered members without requiring any knowledge element; and  
7 (iii) chills businesses and NetChoice’s covered members from publishing expressive materials.

8           87.     Sections 1798.99.31(b)(1)-(4) limit businesses’ ability to collect basic information  
9 needed to deliver services to users (regardless of whether the users want to share that information)  
10 and the way that businesses may retain, use, or share the information they are allowed to collect.  
11 These provisions violate the First Amendment on their face, and as applied to NetChoice’s covered  
12 members, to the extent they limit an online service’s rights to collect information for the purposes  
13 of curating, recommending, and delivering protected speech to users.

14           88.     Section 1798.99.31(b)(3) prohibits online services from collecting, sharing, or  
15 retaining any “personal information”—in other words, engaging in routine maintenance and  
16 dissemination of information—unless doing so is “necessary” to provide the service, product, or  
17 feature “with which a child is actively and knowingly engaged” or the service demonstrates a  
18 “compelling reason” that the use of such information “is in the best interests of children” likely to  
19 access the service. This section violates the First Amendment on its face, and as applied to  
20 NetChoice’s covered members, to the extent it restricts the collection, retention, and sharing of  
21 personal information to publish content or to make content available.

22           89.     Section 1798.99.31(b)(7) prohibits online services from presenting content in a way  
23 that leads minors to provide more personal information than is “reasonably expected” or to take  
24 actions “detrimental” to their “physical health, mental health, or well-being.” This provision, both  
25 facially and as applied to NetChoice’s members, violates the First Amendment to the extent it: (i)  
26 interferes with an online service’s editorial discretion, and (ii) impermissibly restricts how  
27 publishers may address or promote content that a government censor thinks unsuitable for minors,  
28 including through the use of recommendation algorithms, personalization features, and other

1 design features that organize and display content.

2 90. Unless declared invalid and enjoined, AB 2273 will unlawfully deprive  
3 NetChoice’s members of their fundamental First Amendment rights and their free speech rights  
4 under the California Constitution.

5 **COUNT TWO:**  
6 **VIOLATION OF THE FOURTH AMENDMENT TO THE U.S. CONSTITUTION,**  
7 **PURSUANT TO 42 U.S.C. § 1983 (FACIAL AND AS APPLIED)**

8 91. Plaintiff incorporates all prior paragraphs of this Complaint.

9 92. Section 1798.99.31(a)(1) of AB 2273 violates the Fourth Amendment by requiring  
10 regulated businesses, including Plaintiff’s members, to generate and provide DPIAs to the  
11 Attorney General on demand without any opportunity for precompliance review by a neutral  
12 decisionmaker.

13 93. Plaintiff’s members are online services and content publishers with a reasonable  
14 expectation of privacy in the commercially sensitive information that Section 1798.99.31(a)(1)  
15 commands them to include in their DPIAs and turn over to the Attorney General. None of  
16 Plaintiff’s members operates in a “closely regulated” industry that would fall outside the ambit of  
17 the Fourth Amendment’s protections against unrestricted administrative searches under *Patel*, 576  
18 U.S. at 424-25.

19 94. AB 2273 does not provide any opportunity for precompliance review of the  
20 Attorney General’s demands by a neutral decisionmaker. It accordingly “creates an intolerable  
21 risk that searches authorized by it will exceed statutory limits, or be used as a pretext to harass.”  
22 *Patel*, 576 U.S. at 421. Section 1798.99.31(a)(1) is thus “facially invalid” and must be enjoined.  
23 *Id.* at 428.

24 **COUNT THREE:**  
25 **VOID FOR VAGUENESS UNDER THE FIRST AMENDMENT AND DUE PROCESS**  
26 **CLAUSE OF THE U.S. CONSTITUTION, PURSUANT TO 42 U.S.C. § 1983, AND**  
27 **ARTICLE I, SECTION 7(A) OF THE CALIFORNIA CONSTITUTION (FACIAL AND**  
28 **AS APPLIED)**

95. Plaintiff incorporates all prior paragraphs of this Complaint.

96. AB 2273 contains a series of provisions that do not provide ordinary persons with



1 fair notice of the proscribed conduct. AB 2273 is so dependent on subjective, undefined standards  
2 that it practically mandates arbitrary or discriminatory enforcement against disfavored content,  
3 viewpoints, and speakers.

4 97. AB 2273 fails to define multiple critical terms underpinning the law’s central  
5 requirements and leaves regulators with unbridled discretion to impose massive penalties on  
6 businesses.

7 98. Section 1798.99.30(b)(4) defines the “likely to be accessed by children” threshold  
8 requirement based on whether it is “reasonable to expect,” based on certain listed indicators, that  
9 a service will be “accessed by children.” But this provision offers no clarity to businesses  
10 regarding whether they fall within the statute, as the listed “indicators” are ambiguous in numerous  
11 respects. Section 1798.99.30(b)(4)(D), for example, covers online services, products, or features  
12 that are “substantially similar or the same” as services, products, or features in Section  
13 1798.99.30(b)(4)(B). That subsection qualifies businesses if their services are “determined ... to  
14 be routinely accessed by a significant number of children.” But the statute offers no definition as  
15 to “reasonable to expect,” “substantially similar,” “routinely accessed,” or “significant number,”  
16 depriving businesses of notice as to whether they are subject to AB 2273.

17 99. Section 1798.99.31(a)(5) requires businesses to estimate the age of minor users  
18 “with a reasonable level of certainty appropriate to the risks that arise from the data management  
19 practices of the business.” But the statute includes no definition as to what such an individualized  
20 level of certainty entails. Absent any guidance, regulators will have boundless discretion to  
21 discriminate among businesses, privately review and evaluate each business’s data management  
22 practices without any disclosed criteria, and then subjectively determine what constitutes an  
23 “appropriate” level of certainty for each business.

24 100. Section 1798.99.31(a)(6) obliges businesses to configure all default privacy  
25 settings provided to minors—children or teens—to a “high level of privacy,” unless the business  
26 can demonstrate a “compelling reason” that an alternative setting is in the “best interests of  
27 children.” Here too, the law fails to provide businesses notice as to what it requires. The provision  
28 does not, for example, require the business to configure its privacy settings to the “highest” it

1 offers, or otherwise define the term relative to the business’s default privacy settings. Instead, it  
2 mandates that businesses implement settings with an imprecise, free-floating “high” degree of  
3 privacy. Nor does the law define “compelling reason” or “best interests of children.” The statute  
4 thus provides businesses no way of knowing how to comply.

5 101. Section 1798.99.31(a)(7) compels businesses to display their privacy policies and  
6 community standards “concisely, prominently, and using clear language suited to the age of  
7 children likely to access that online service, product, or feature.” This provision is rife with  
8 ambiguity, as the legislation provides no direction on what such age-appropriate language may  
9 look like. If a site is equally accessible to 4-year-olds, 8-year-olds, and 15-year-olds, for example,  
10 the provision does not specify which type of language would be “suited”—and whether that  
11 language must in all instances to be suited to the youngest child likely to access the site or could  
12 differ among users. Nor does the provision give any indication as to how compliance would be  
13 measured, again leaving those subjective decisions entirely in the hands of the Attorney General.

14 102. Section 1798.99.31(b)(1) forbids businesses from “us[ing]” the personal  
15 information of minors in any way that the business “knows, or has reason to know” is “materially  
16 detrimental to the physical health, mental health, or well-being of a child.” The law provides no  
17 guidance as to what types of personal-information uses would result in such knowledge, or even  
18 the meaning of the undefined term “materially detrimental” harm to a child’s “well-being.” Under  
19 the section’s plain text, a business must change its services if a single child might suffer any of  
20 these unnamed harms—and again, the Attorney General has complete discretion to assess whether  
21 the business should have known about these harms, or even what the harms are in the first place.

22 103. Sections 1798.99.31(b)(3) and (b)(4) expose online services to significant liability  
23 unless they can prove that their use of personal information advances the “best interests of  
24 children,” however a regulator chooses to define that.

25 104. Section 1798.99.31(b)(7) precludes businesses from using so-called “dark patterns”  
26 to “lead or encourage children ... to take any actions that the business knows, or has reason to  
27 know, is materially detrimental to the child’s physical health, mental health, or well-being.” This  
28 provision, too, fails to define pivotal terms, including as to the core definition of dark patterns

1 itself, and leaves regulators with impermissible discretion as to application.

2 105. AB 2273 repeatedly uses vague and undefined terms to describe businesses' key  
3 obligations under the law, leaving the Attorney General with virtually boundless discretion.  
4 Accordingly, both as a facial matter and as applied to NetChoice's covered members, the law fails  
5 to provide constitutionally sufficient notice, and invites arbitrary and discriminatory enforcement  
6 against disfavored content, viewpoints, and speakers.

7 **COUNT FOUR:**  
8 **VIOLATION OF THE COMMERCE CLAUSE OF THE U.S. CONSTITUTION,**  
9 **PURSUANT TO 42 U.S.C. § 1983 (FACIAL AND AS APPLIED)**

10 106. Plaintiff incorporates all prior paragraphs of this Complaint.

11 107. AB 2273 violates the Commerce Clause under *Pike v. Bruce Church, Inc.*, 397 U.S.  
12 137 (1970), and its progeny because the law seeks to impose an unreasonable and undue burden  
13 on interstate commerce that is clearly excessive in relation to any local benefit conferred on the  
14 State of California and is likely to subject businesses to inconsistent state regulations.

15 108. AB 2273 burdens interstate commerce by deterring online service providers from  
16 offering services available across state lines, or else limiting the types of services available within  
17 and across the United States. This is because the Internet is accessible globally, and whether a  
18 covered business wishes to avoid California's regulations or comply with them, doing so  
19 inherently requires Internet services to degrade or withdraw their services for all users in all states.

20 109. AB 2273 also burdens interstate commerce by forcing online service providers to  
21 comply with an inconsistent patchwork of state rules. For example, AB 2273 will in practice  
22 require covered businesses to adopt age-verification tools that might violate other states'  
23 conflicting privacy laws (such as biometric privacy laws).

24 110. The California Legislature has not identified any local interest (as opposed to an  
25 abstract interest in privacy generally) sufficient to justify these onerous impositions on interstate  
26 commerce, and the Act admits that the privacy regime it imposes does not even provide an  
27 appropriate degree of privacy for all the users it affects. Therefore, even if the identified  
28 generalized interest in privacy were deemed sufficiently local, AB 2273's drastic impositions on  
interstate and online commerce far outweigh what little AB 2273 does to further that purpose.

1 111. AB 2273 also violates the Commerce Clause because it regulates extraterritorially  
2 in violation of the rule in *Healy v. Beer Institute, Inc.*, 491 U.S. 324, 336 (1989). For the same  
3 reasons that AB 2273 burdens interstate commerce by depressing or degrading the output and  
4 quality of Internet services available nationwide, AB 2273 necessarily has the practical and *per se*  
5 unconstitutional effect of regulating commercial and speech-related activities that occur wholly  
6 outside California, such as by causing an Internet service based in New York to withhold a product  
7 or service to users in Florida.

8 112. Unless declared invalid and enjoined, AB 2273 will operate to unconstitutionally  
9 burden interstate commerce in violation of the Commerce Clause.

10 **COUNT FIVE:**  
11 **COPPA PREEMPTION, 15 U.S.C. §§ 6501 *et seq.***  
12 **(FACIAL AND AS APPLIED)**

13 113. Plaintiff incorporates all prior paragraphs of this Complaint.

14 114. AB 2273 is preempted by COPPA because AB 2273 is wholly “inconsistent” with  
15 that federal statute with respect to children under the age of 13. 15 U.S.C. § 6502(d). Because the  
16 portions of AB 2273 that apply to children under 13 cannot be severed from the rest of AB 2273,  
17 the entire law is preempted.

18 115. COPPA and the COPPA Rule impose various obligations on businesses with  
19 respect to children under the age of 13. The duties and obligations mandated by AB 2273 are  
20 inconsistent with, and hence preempted by, COPPA and the COPPA Rule.

21 116. First, AB 2273’s wide-ranging scope is inconsistent with, and thus preempted by,  
22 COPPA. COPPA applies to online services “directed” to children under 13, whereas AB 2273  
23 covers services that are not necessarily “directed” to children, but instead “likely to be accessed  
24 by children.” Even more troubling, covered businesses include those that are “substantially similar  
25 or the same” as services that are determined to be “routinely accessed by a significant number of  
26 children” or services that have “design elements that are known to be of interest to children.”  
27 § 1798.99.30(b)(4)(B), (D), (E). Accordingly, whereas COPPA applies to a subset of websites  
28 and online services, AB 2273 effectively applies to almost all websites, including those of  
NetChoice’s members.

1 117. Second, COPPA preempts AB 2273 because AB 2273 imposes on businesses and  
 2 online services privacy obligations with respect to children under 13 that are not required by  
 3 COPPA or the COPPA Rule. Unlike COPPA, AB 2273 would permit the government to  
 4 effectively censor content that can be seen by all minors—even someone just days away from their  
 5 18th birthday or whose parents do not prefer such censorship.

6 118. AB 2273 imposes substantive obligations on businesses with respect to children  
 7 under the age of 13 that far exceed the requirements of the COPPA Rule, which are largely notice-  
 8 and-consent based. In contrast to the COPPA Rule, AB 2273 requires—among other things—that  
 9 businesses create comprehensive and wide-ranging DPIAs, § 1798.99.31(a)(1)-(4); estimate user  
 10 ages to a “reasonable level of certainty” or apply universal privacy standards, § 1798.99.31(a)(5);  
 11 configure privacy settings to a “high” level, unless the business can meet the “best interests of  
 12 children” showing, § 1798.99.31(a)(6); and enforce published terms and policies,  
 13 § 1798.99.31(a)(9). COPPA imposes none of these obligations, and therefore AB 2273 is  
 14 inconsistent with the COPPA notice-and-consent regime.

15 119. AB 2273 requires businesses to refrain from undertaking other actions that are  
 16 allowed under the COPPA Rule, including “profiling a child by default” unless the business meets  
 17 certain narrow requirements, § 1798.99.31(b)(2), and using “dark patterns to lead or encourage  
 18 children” to provide personal information or take any action that the business should know is  
 19 “materially detrimental” to the minor, § 1798.99.31(b)(7). These too are inconsistent with COPPA  
 20 and thus preempted.

21 **COUNT SIX:**  
 22 **SECTION 230 PREEMPTION, 47 U.S.C. § 230 (FACIAL AND AS APPLIED)**

23 120. Plaintiff incorporates all prior paragraphs of the Complaint.

24 121. NetChoice’s members are “interactive computer service[s]” within the meaning of  
 47 U.S.C. § 230 because they own and operate interactive websites.

25 122. Sections 1798.99.31(a)(9), 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) of AB 2273  
 26 violate NetChoice’s members’ rights under 47 U.S.C. § 230(c)(1) because they treat NetChoice’s  
 27 members as the publishers or speakers of information provided by other information content  
 28 providers—that is, their users. By threatening to impose liability on services for failing to enforce

1 their “published terms, policies, and community standards,” Section 1798.99.31(a)(9) necessarily  
2 and impermissibly violates Section 230(c)(1) because it limits services’ discretion in reviewing,  
3 editing, promoting, and deciding whether to publish or remove third-party content. Sections  
4 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) likewise hold online services liable for their decisions  
5 to publish certain third-party content to certain users.

6 123. Section 1798.99.31(a)(9) also violates NetChoice’s members’ rights under 47  
7 U.S.C. § 230(c)(2) because it interferes with their right to take “good faith” actions “to restrict  
8 access to or availability of material that” they “consider[] to be obscene, lewd, lascivious, filthy,  
9 excessively violent, harassing, or otherwise objectionable, whether or not such material is  
10 constitutionally protected.”

11 124. Sections 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) thus violate and are preempted  
12 by 47 U.S.C. § 230(c) to the extent they apply to covered services’ publication of third-party  
13 content.

14 125. Section 1798.99.31(a)(9) thus violates and is preempted by 47 U.S.C. § 230(c) to  
15 the extent it applies to covered services’ enforcement of their content policies and community  
16 standards.

17 126. Sections 1798.99.31(a)(9) and 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) thus  
18 violate and are preempted by Section 230.

19 **IX. PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiff NetChoice respectfully requests that the Court:

21 1. Declare that Section 1798.99.30(b)(4) violates the First and Fourteenth  
22 Amendments to the United States Constitution on its face;

23 2. Declare that the mandates and prohibitions contained within Sections  
24 1798.99.31(a) and .31(b) violate the First and Fourteenth Amendments to the United States  
25 Constitution on their face because, pursuant to the coverage definition in Section  
26 1798.99.30(b)(4), they impermissibly target online services for regulation based on the content  
27 they publish.

28 3. Declare that Sections 1798.99.31(a)(1)–(4) violate the First and Fourteenth

1 Amendments to the United States Constitution on their face;

2 4. Declare that Section 1798.99.31(a)(5) violates the First and Fourteenth  
3 Amendments to the United States Constitution on its face, and as applied to covered NetChoice  
4 members;

5 5. Declare that Section 1798.99.31(a)(9) violates the First and Fourteenth  
6 Amendments to the United States Constitution on its face to the extent that section applies to  
7 covered services' content policies and community standards, and violates the First and Fourteenth  
8 Amendments to the United States Constitution as applied to covered NetChoice members'  
9 enforcement of those policies;

10 6. Declare that Sections 1798.99.31(b)(1)–(2), (b)(4) violate the First and Fourteenth  
11 Amendments to the United States Constitution on their face to the extent those sections apply to  
12 covered services' use of personal information to publish content or to make information available,  
13 and violate the First and Fourteenth Amendments to the United States Constitution as applied to  
14 covered NetChoice members' practices to do so;

15 7. Declare that Section 1798.99.31(b)(3) violates the First and Fourteenth  
16 Amendments to the United States Constitution on its face to the extent that section applies to  
17 covered services' retention, sale, and sharing of personal information to publish content or to make  
18 information available, and violates the First and Fourteenth Amendments to the United States  
19 Constitution as applied to covered NetChoice members' practices to do so;

20 8. Declare that Section 1798.99.31(b)(7) violates the First and Fourteenth  
21 Amendments to the United States Constitution on its face to the extent that section applies to  
22 covered services' use of recommendation algorithms, continuous scroll, autoplay, and other design  
23 features that organize content, and violates the First and Fourteenth Amendments to the United  
24 States Constitution as applied to covered NetChoice members' use of such features;

25 9. Declare that Sections 1798.99.31(a)(5), (9) and 1798.99.31(b)(1)–(4) and (7) are  
26 facially invalid because they are not severable from 1798.99.31(a)(1)–(4) and 1798.99.35(c), and  
27 declare any remaining provisions of AB 2273 invalid to the extent the Court finds those provisions  
28 inseverable from the invalid portions NetChoice challenges;

1           10.     Declare that Sections 1798.99.31(a)(1)-(5), (9) and 1798.99.31(b)(1)-(4) and (7)  
2 violate the Commerce Clause of the U.S. Constitution on their face;

3           11.     Declare that Sections 1798.99.31(a)(1)-(5), (9) and 1798.99.31(b)(1)-(4) and (7)  
4 are inconsistent with and thus preempted by COPPA, 15 U.S.C. §§ 6501 et seq., to the extent  
5 applicable to persons under the age of 13;

6           12.     Declare that Section 230 of the Communications Decency Act, 47 U.S.C. § 230(c),  
7 preempts Section 1798.99.31(a)(9) on its face to the extent applied to covered services'  
8 enforcement of their content policies and community standards; and preempts Sections  
9 1798.99.31(b)(1), (3)-(4), and (7) on their face to the extent these provisions are applied to covered  
10 services' publication of third-party content;

11           13.     Preliminarily and permanently enjoin Defendant and his agents, employees, and all  
12 persons acting under his direction or control from taking any action to enforce Sections  
13 1798.99.31(a)(1)-(5), (9) and 1798.99.31(b)(1)-(4) and (7) against NetChoice and its members,  
14 and any other covered entities, to the extent NetChoice challenges these provisions;

15           14.     Enter judgment in favor of NetChoice;

16           15.     Award NetChoice its reasonable costs and attorneys' fees incurred in bringing this  
17 action, pursuant to 42 U.S.C. § 1988; and

18           16.     Award NetChoice all other such relief as the Court deems just and proper.

19  
20 DATED: October 31, 2024

DAVIS WRIGHT TREMAINE LLP

21 By: /s/ Adam S. Sieff  
22 Adam S. Sieff

23  
24 Attorneys for Plaintiff  
NetChoice, LLC d/b/a NetChoice

25  
26  
27  
28