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

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

ROBERT CORN-REVERE (*pro hac vice* application forthcoming)
bobcornrevere@dwt.com
DAVID M. GOSSETT (*pro hac vice* application forthcoming)
davidgossett@dwt.com
MEENAKSHI KRISHNAN (*pro hac vice* application forthcoming)
meenakshikrishnan@dwt.com
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW, Suite 500 East
Washington, D.C. 20005
Telephone: (202) 973-4200

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

IN THE UNITED STATES DISTRICT COURT

THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, LLC d/b/a NetChoice,

Plaintiff,

v.

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

Defendant.

Case No. 5:22-cv-8861

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

I. PRELIMINARY STATEMENT

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

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

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

---

[1] AB 2273 as enacted is attached as Exhibit A and will be codified in relevant part beginning at Section 1798.99.28 to Part 4 of Division 3 of the California Civil Code.

[2] *See* "Coalition Letter on Privacy and Free Expression Threats in Kids Online Safety Act" Regarding Opposition to 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.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

4. For these and other reasons, AB 2273 is facially unconstitutional on at least four grounds and is preempted by two federal statutes: The Act on its face violates the First Amendment, Fourth Amendment, and the Due Process and Commerce Clauses of the United States Constitution; violates Article I, Sections 2(a) and 7(a) of the California Constitution; and is preempted by the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501 *et seq*., and the COPPA Rule, 16 C.F.R. § 312.1 *et seq*., as well as Section 230 of the Communications Decency Act, 47 U.S.C. § 230. Plaintiff NetChoice, LLC accordingly seeks an order declaring AB 2273 invalid and enjoining its enforcement.

II. PARTIES AND STANDING

5. NetChoice is a non-profit entity organized under Section 501(c)(6) of the Internal Revenue Code created in and existing under the laws of the District of Columbia. NetChoice is a national trade association of online businesses that share the goal of promoting free speech and free enterprise on the Internet. A list of NetChoice's members is available at https://netchoice.org/about/. For more than two decades, NetChoice has worked to promote online commerce and speech and to increase consumer access and options through the Internet. NetChoice's members devote significant attention, time, and money to safeguard children online.

6. Most of NetChoice's members are directly subject to and regulated by AB 2273 and could face serious legal consequences if they fail to comply with the Act's directives. And NetChoice itself anticipates having to divert resources to address these consequences and support its members in connection with AB 2273's demands.

7. NetChoice and its members will suffer irreparable harm—including infringement of their constitutional rights—if AB 2273 is not declared invalid and enjoined before it takes effect.

8. Defendant Rob Bonta is the Attorney General of the State of California. Defendant is responsible for enforcing the provisions of AB 2273 challenged by this action, including because the Act authorizes the Attorney General to bring a "civil action … in the name of the people of the State of California." § 1798.99.35(a).

III. JURISDICTION

9. This action arises under the United States Constitution, particularly the Commerce

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

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

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

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

IV. VENUE

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

V. DIVISIONAL ASSIGNMENT

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

VI. FACTUAL ALLEGATIONS

A. Online Businesses and Website Architecture

14. Online businesses interact with users in different ways. Most have universally accessible areas, in which a user can view product listings, preview services, and read reviews without creating or logging into an account. Many online businesses also have features that are optimized and available only for individuals who create an account or sign up for membership. Some social media services, for example, permit non-members to view public portions of a user's profile, but not to view each post in detail. Similarly, many online businesses require users to create accounts before they can use or purchase an online service.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

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

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

17. Even independently of advertising, content promotion is a key service that online businesses offer—and often a key source of revenue. An online service's ability to suggest a new release based on the user's browsing history, for example, creates value for the user, generates business for the service, and connects content creators with an audience. This is true across industry—music, movies, television shows, social media posts, and anything else an Internet user might be interested in purchasing, reading, hearing, or viewing.

[3] *See generally* David S. Evans, "The Economics of the Online Advertising Industry," 7 REV. OF NETWORK ECON. 3 (2008), available at https://doi.org/10.2202/1446-9022.1154.

[4] *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.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

B. AB 2273

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

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

1. The breadth of businesses affected by AB 2273

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

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

22. Although AB 2273 purports to regulate "online service[s], product[s], or feature[s]," the statute in fact regulates speech. AB 2273's references to "system design features," "algorithms," and "targeted advertising systems" all refer to the methods used to disseminate or circulate speech on the Internet. This fact is underscored by Section 1798.99.30(b)(5)(C), which

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

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

clarifies that AB 2273's reach excludes "the delivery or use of a physical product."

23. AB 2273 defines "likely to be accessed by children" to "mean[] it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children":

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

§ 1798.99.30(b)(4).

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

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

a. All major news outlets, including The New York Times, Wall Street Journal, and Washington Post; ABC, CBS, and NBC; CNN, Fox News, and MSNBC; as well as a significant number of local news services.

b. The websites of every major sports league, including MLB, MLS, NBA, NFL, and NHL, and sports outlets serving the United States, including ESPN, FiveThirtyEight, the Golf Channel, NBC Sports, Sports Illustrated, Telemundo, and Yahoo Sports.

c. Most online magazines and podcast channels.

d. E-books and e-reader apps, as well as book forums.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

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.

26. 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*

27. 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.

28. 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 "uses system design features to increase, sustain, or extend use of the online product, service, or feature by children, including the automatic playing of media, rewards for time spent, and

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

notifications." § 1798.99.31(a)(1)(B). In conjunction with the DPIA, the business must also "create a timed plan to mitigate or eliminate" any risks identified in the DPIA "before the online service, product, or feature is accessed by children." § 1798.99.31(a)(2).

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

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

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

32. The DPIA requirement applies equally to large global services and single-person blogs, so long as they meet California's definition of a "business." As one independent journalist explained about his own publication: "Our comment system? DPIA. Our comment voting? DPIA. Our comment promotion? DPIA. The ability to listen to our podcast? DPIA. The ability to share our posts? DPIA. The ability to join our insider chat? DPIA. The ability to buy a t-shirt? DPIA. The ability to post our stories to Reddit, Twitter, Facebook, or LinkedIn? DPIA (for each of those, or can we combine them? I dunno). Our feature that recommends similar articles? DPIA. Search? DPIA. Subscribe to RSS? DPIA."[6]

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

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

3. *The statute's age verification requirements*

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

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

35. But age certainty is not realistic. Age verification technologies are inherently unreliable.[7] Most methods rely on users either to attest to their ages or to submit official documents verifying their ages.[8] For users determined to bypass the rules, there are "straightforward workarounds" to both of these methods, which businesses often cannot avert.[9] And any method that involves submitting official documents increases the risk that those documents could be stolen or leaked.[10] More invasive age-verification methods—such as artificial intelligence, facial analysis, or facial recognition technologies—are far from foolproof and pose their own transparency, security, and privacy concerns.[11] To the extent AB 2273's "reasonable … certainty" standard effectively requires companies to adopt such invasive age-verification methods, the law likely conflicts with other states' privacy laws—such as laws that regulate the collection of biometric data—and subjects online businesses to a patchwork of inconsistent obligations. Perversely, AB 2273 contradicts the consumer-data-minimization mandates of the State's own privacy law, the California Privacy Rights Act (CPRA), and might well result in a net loss of

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

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

[9] *Id.*

[10] *Id*.

[11] *See* David McCabe, "Anonymity No More? Age Checks Come to the Web," N.Y. TIMES (Oct. 27, 2021), available at https://nyti.ms/3S6U2ME.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

privacy for California minors and adults alike.

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

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

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

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

39. Section 1798.99.31(a)(9) eliminates both this discretion as well as the element of private action by empowering the State to penalize any covered business that fails to adequately enforce its own editorial standards and policies. Permitting the State to monitor an online publisher's content moderation decisions intrudes into the publisher's right to make editorial decisions about the types of content to host or exclude in pursuit of its mission, and incentivizes publishers to forgo content moderation altogether—a dire prospect for content-sharing services, for which content moderation *is* the product they provide.[12]

5. *The statute's prohibitions on use of information*

40. AB 2273 prohibits covered services from taking actions that are otherwise protected

[12] *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.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

by the Constitution or federal law.

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

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

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

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

45. Guessing wrong about what these provisions proscribe is prohibitively expensive—penalties for even negligent errors could exceed $20 billion. Many services will not or cannot risk it. Instead, they will self-censor by banning users whose age they cannot verify; refrain from publishing content to certain users; disable editorial features that control the publication, curation, and promotion of content on their services; forego efforts to connect their customers with

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

suggested content or other users; or shut down altogether. The law poses an existential risk in particular to websites that rely on advertising to support dissemination of speech to and among users.

6. *The statute's ban on using "dark patterns"*

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

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

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

49. To comply with this provision, online businesses must either guess whether any of these content-promotion decisions might be construed to have a "materially detrimental" effect on a minor before publishing—hoping, again, that they have predicted correctly and that their predictions match the government's own subjective assessments—or elect to self-censor. As with other provisions of AB 2273, many online services are likely to choose self-censorship.

[13] *See, e.g.*, Katharine Miller, "Can't Unsubscribe? Blame Dark Patterns," Stanford University Institute for Human-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.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

* * * * *

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

VII. LEGAL PRINCIPLES

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

A. The First Amendment

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

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

54. The First Amendment prohibits prior restraints on speech, including state action designed to deputize private actors to serve as censors by proxy. *Denver Area Educ. Telecomm. Consortium, Inc. v. F.C.C.*, 518 U.S. 727, 754 (1996). Any government regulation that "subject[s] the distribution of publications to a system of prior administrative restraints," including a "system of informal censorship" to promote "juvenile morality" and well-being, carries "a heavy presumption against its constitutional validity." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70-71 (1963).

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

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

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

57. In addition to prohibiting *restrictions* on speech, the First Amendment forbids the government from *compelling* speech in ways that burden and chill constitutionally protected editorial and speech rights. A law "mandating speech that a speaker would not otherwise make" is "necessarily" a "content-based regulation of speech" subject to strict scrutiny because it "alters the content of the speech." *Riley v. Nat'l Fed'n of the Blind of N. Carolina, Inc.*, 487 U.S. 781, 795 (1988). Even compelled commercial disclosures must meet certain requirements to pass

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

constitutional muster—namely, the standards alternatively articulated in *National Institute of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361 (2018) (*NIFLA*), *Central Hudson Gas & Electric Corporation v. Public Service Commission*, 447 U.S. 557 (1980), and *Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626 (1985).

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

59. A law is unconstitutionally overbroad if "a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *Stevens*, 559 U.S. at 473 (citation omitted).

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

B. The Fourth Amendment

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

62. One exception to the warrant requirement involves an "administrative search" that seeks to "ensure compliance with [a] recordkeeping requirement." *Id.* at 420. But to fall within this "administrative search exception," "the subject of the search must be afforded an opportunity to obtain precompliance review before a neutral decisionmaker." *Id.* A statutory regime that permits the government to search and seize the commercially sensitive information of an ordinarily regulated business is thus "facially invalid" where it fails to afford such an opportunity to a party compelled to "turn over" records. *Id.* at 421.

C. Vagueness and the Due Process Clause

63. The Due Process Clause of the Fourteenth Amendment forbids vague laws—

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

particularly those that regulate speech protected by the First Amendment.

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

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

D. The Dormant Commerce Clause

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

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

E. The Children's Online Privacy Protection Act

68. Enacted in 1998, the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 *et seq.*, created a comprehensive federal scheme to facilitate parental control over children's online activities and to protect children's privacy. COPPA defines a "child" as an "individual under the age of 13." 15 U.S.C. §§ 6501(1). The Federal Trade Commission (FTC) has authority to enforce COPPA and has promulgated a rule to implement COPPA, which is known as the COPPA Rule. *See* 16 C.F.R. § 312.1 *et seq.*

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

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

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

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

F. Section 230 of the Communications Decency Act

72. Section 230 of the Communications Decency Act, 47 U.S.C. § 230, states that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." *Id.* § 230(c)(1). It also prohibits the imposition of liability for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." *Id.* § 230(c)(2). An "interactive computer service" is "any information

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

service, system, or access software provider that provides or enables computer access by multiple users to a computer server." *Id.* § 230(f)(2). The "provider" of such a service includes those who own or operate websites and therefore includes NetChoice's members that are subject to AB 2273.

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

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

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

VIII. CLAIMS FOR RELIEF

COUNT ONE: VIOLATION OF THE FIRST AND FOURTEENTH AMENDMENTS TO THE U.S. CONSTITUTION, PURSUANT TO 42 U.S.C. § 1983, AND ARTICLE I, SECTION 2(A) OF THE CALIFORNIA CONSTITUTION

76. Plaintiff incorporates all prior paragraphs of this Complaint.

77. 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.

78. AB 2273 imposes a system of prior administrative restraints that require online services to create DPIA reports for state inspection *before* publishing any "online service, product, or feature" to the public "likely to be accessed by" any user under the age of 18, including teens on the cusp of adulthood. Even if it were crystal clear which services meet the "likely to be accessed" standard or what kinds of content, features, and services constituted a potential harm,

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

the requirement places online services under threat of government sanction for making any service available that could be considered harmful to minors and thus imposes a prior restraint. Service providers face state-imposed sanctions if they publish online without first producing a DPIA, and they face state sanctions even if they do provide a DPIA but fail to prepare "a timed plan to mitigate or eliminate the [undefined] risk before the online service, product, or feature is accessed by children."

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

80. AB 2273 imposes a battery of viewpoint-, content-, and speaker-based restrictions on speech, and is thus subject to strict scrutiny. AB 2273 only applies, for example, to certain categories of speech (as defined in Section 1798.140) used by qualifying websites, and it selects among speakers by exempting not-for-profit and government speakers altogether. More fundamentally, for businesses that are covered, the law imposes rules and penalties based on what the content is and whether it is "materially detrimental" to the "mental health, or well-being of a child," is strictly "necessary" to provide the service, or is in the "best interests" of minors. These restrictions "reflect the Government's preference for the substance of what the favored speakers have to say (or aversion to what the disfavored speakers have to say)," and require strict scrutiny. *Turner Broad. Sys.*, 512 U.S. at 658.

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

82. AB 2273's prior restraints, speech restrictions, and compelled speech requirements

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

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

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

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

85. Section 1798.99.31(a)(9) mandates that businesses enforce community standards and privacy policies. This provision impermissibly (i) restricts businesses' ability to exercise their own editorial discretion regarding which content to leave up or take down, and what to publish or not to publish; (ii) imposes strict liability on businesses without requiring any knowledge element; and (iii) chills businesses from publishing expressive materials.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

86. Sections 1798.99.31(b)(1), (b)(3), and (b)(4) limit businesses' ability to collect information from users (regardless of whether the users want to share that information) and the way that businesses may retain, use, or share the information they are allowed to collect. These provisions interfere with an online service's First Amendment rights to (i) collect information, and (ii) exercise editorial discretion to recommend content for users.

87. Section 1798.99.31(b)(7) prohibits online services from making protected publishing decisions that the government deems "materially detrimental" to a minor's physical or mental health or "well-being." This provision (i) interferes with an online service's First Amendment rights to editorial discretion, and (ii) impermissibly restricts how publishers may address or promote content that a government censor thinks unsuitable for minors.

88. Unless declared invalid and enjoined, AB 2273 will unlawfully deprive NetChoice's members of their fundamental First Amendment rights and their free speech rights under the California Constitution.

COUNT TWO:
VIOLATION OF THE FOURTH AMENDMENT TO THE U.S. CONSTITUTION, PURSUANT TO 42 U.S.C. § 1983

89. Plaintiff incorporates all prior paragraphs of this Complaint.

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

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

92. AB 2273 does not provide any opportunity for precompliance review of the Attorney General's demands by a neutral decisionmaker. It accordingly "creates an intolerable

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

risk that searches authorized by it will exceed statutory limits, or be used as a pretext to harass." *Patel*, 576 U.S. at 421. Section 1798.99.31(a)(1) is thus "facially invalid" and must be enjoined. *Id.* at 428.

COUNT THREE:
VOID FOR VAGUENESS UNDER THE FIRST AMENDMENT AND DUE PROCESS CLAUSE OF THE U.S. CONSTITUTION, PURSUANT TO 42 U.S.C. § 1983, AND ARTICLE I, SECTION 7(A) OF THE CALIFORNIA CONSTITUTION

93. Plaintiff incorporates all prior paragraphs of this Complaint.

94. AB 2273 contains a series of provisions that do not provide ordinary persons with fair notice of the proscribed conduct. AB 2273 is so dependent on subjective, undefined standards that it practically mandates arbitrary or discriminatory enforcement against disfavored content, viewpoints, and speakers.

95. AB 2273 fails to define multiple critical terms underpinning the law's central requirements and leaves regulators with unbridled discretion to impose massive penalties on businesses.

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

97. Section 1798.99.31(a)(5) requires businesses to estimate the age of minor users "with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business." But the statute includes no definition as to what such an individualized level of certainty entails. Absent any guidance, regulators will have boundless discretion to

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

discriminate among businesses, privately review and evaluate each business's data management practices without any disclosed criteria, and then subjectively determine what constitutes an "appropriate" level of certainty for each business.

98. Section 1798.99.31(a)(6) obliges businesses to configure all default privacy settings provided to minors—children or teens—to a "high level of privacy," unless the business can demonstrate a "compelling reason" that an alternative setting is in the "best interests of children." Here too, the law fails to provide businesses notice as to what it requires. The provision does not, for example, require the business to configure its privacy settings to the "highest" it offers, or otherwise define the term relative to the business's default privacy settings. Instead, it mandates that businesses implement settings with an imprecise, free-floating "high" degree of privacy. Nor does the law define "compelling reason" or "best interests of children." The statute thus provides businesses no way of knowing how to comply.

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

100. Section 1798.99.31(b)(1) forbids businesses from "us[ing]" the personal information of minors in any way that the business "knows, or has reason to know" is "materially detrimental to the physical health, mental health, or well-being of a child." The law provides no guidance as to what types of personal-information uses would result in such knowledge, or even the meaning of the undefined term "materially detrimental" harm to a child's "well-being." Under the section's plain text, a business must change its services if a single child might suffer any of these unnamed harms—and again, the Attorney General has complete discretion to assess whether

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

the business should have known about these harms, or even what the harms are in the first place.

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

102. Section 1798.99.31(b)(7) precludes businesses from using "dark patterns" to "lead or encourage children … to take any actions that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being." This provision, too, fails to define pivotal terms and leaves regulators with complete discretion as to application.

103. AB 2273 repeatedly uses vague and undefined terms to describe businesses' key obligations under the law, leaving the Attorney General with virtually boundless discretion. Accordingly, the law fails to provide constitutionally sufficient notice, and invites arbitrary and discriminatory enforcement against disfavored content, viewpoints, and speakers.

COUNT FOUR:
VIOLATION OF THE COMMERCE CLAUSE OF THE U.S. CONSTITUTION, PURSUANT TO 42 U.S.C. § 1983

104. Plaintiff incorporates all prior paragraphs of this Complaint.

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

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

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

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

108. The California Legislature has not identified any local interest (as opposed to an abstract interest in privacy generally) sufficient to justify these onerous impositions on interstate commerce, and the Act admits that the privacy regime it imposes does not even provide an appropriate degree of privacy for all the users it affects. Therefore, even if the identified 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.

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

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

COUNT FIVE:
COPPA PREEMPTION, 15 U.S.C. §§ 6501 *et seq*.

111. Plaintiff incorporates all prior paragraphs of this Complaint.

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

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

114. First, AB 2273's wide-ranging scope is inconsistent with, and thus preempted by, COPPA. COPPA applies to online services "directed" to children under 13, whereas AB 2273 covers services that are not necessarily "directed" to children, but instead "likely to be accessed

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

by children." Even more troubling, covered businesses include those that are "substantially similar or the same" as services that are determined to be "routinely accessed by a significant number of children" or services that have "design elements that are known to be of interest to children." § 1798.99.30(b)(4)(B), (D), (E). Accordingly, whereas COPPA applies to a subset of websites and online services, AB 2273 effectively applies to almost all websites, including those of NetChoice's members.

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

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

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

COUNT SIX:
SECTION 230 PREEMPTION, 47 U.S.C. § 230

118. Plaintiff incorporates all prior paragraphs of the Complaint.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

119. NetChoice's members are "interactive computer service[s]" within the meaning of 47 U.S.C. § 230 because they own and operate interactive websites.

120. Sections 1798.99.31(a)(9), 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) of AB 2273 violate NetChoice's members' rights under 47 U.S.C. § 230(c)(1) because they treat NetChoice's members as the publishers or speakers of information provided by other information content providers—that is, their users. By threatening to impose liability on services for failing to enforce their "published terms, policies, and community standards," Section 1798.99.31(a)(9) necessarily and impermissibly violates Section 230(c)(1) because it limits services' discretion in reviewing, editing, promoting, and deciding whether to publish or remove third-party content. Sections 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) likewise hold online services liable for their decisions to publish certain third-party content to certain users.

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

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

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff NetChoice respectfully requests that the Court:

1. Declare that AB 2273 is entirely preempted by federal law (COPPA) and the Commerce Clause of the U.S. Constitution;

2. Declare that Sections 1798.99.30(b)(4), 1798.99.31(a)(1)-(7) and (9), and 1798.99.31(b)(1), (b)(3), (b)(4), and (b)(7) of AB 2273 are unconstitutional under the U.S. and California constitutions, and otherwise preempted by federal law, including Section 230;

3. Preliminarily and permanently enjoin Defendant and his agents, employees, and all persons acting under his direction or control from taking any action to enforce the Act against NetChoice and its members;

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

4. Enter judgment in favor of NetChoice;

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

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

DATED: December 14, 2022

DAVIS WRIGHT TREMAINE LLP

By: */s/ Adam S. Sieff*
Adam S. Sieff

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

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

EXHIBIT A

Assembly Bill No. 2273

CHAPTER 320

An act to add Title 1.81.47 (commencing with Section 1798.99.28) to Part 4 of Division 3 of, and to repeal Section 1798.99.32 of, the Civil Code, relating to consumer privacy.

[Approved by Governor September 15, 2022. Filed with Secretary of State September 15, 2022.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2273, Wicks. The California Age-Appropriate Design Code Act.

(1) Existing law, the California Privacy Rights Act of 2020, approved by the voters as Proposition 24 at the November 3, 2020, statewide general election, establishes the California Privacy Protection Agency. Existing law vests the agency with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018 and requires the agency to be governed by a board. Existing law requires businesses to protect consumer privacy and information, make certain disclosures to consumers regarding a consumer's rights under the act in a specified manner, and disclose to consumers that a consumer has the right to request specific pieces of information, including the categories of information those businesses have collected about that consumer.

Existing law, the Parent's Accountability and Child Protection Act, requires a person or business that conducts business in California and that seeks to sell specified products or services to take reasonable steps to ensure that the purchaser is of legal age at the time of purchase or delivery, including verifying the age of the purchaser. Existing law prohibits a person or business that is required to comply with these provisions from retaining, using, or disclosing any information it receives in an effort to verify age from a purchaser or recipient for any other purpose, except as specified, and subjects a business or person that violates these provisions to a civil penalty.

This bill would enact the California Age-Appropriate Design Code Act, which, commencing July 1, 2024, would, among other things, require a business that provides an online service, product, or feature likely to be accessed by children to comply with specified requirements, including a requirement to configure all default privacy settings offered by the online service, product, or feature to the settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children, and to provide privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature. The bill would require a business, before any new online services, products, or features are offered to the public, to

complete a Data Protection Impact Assessment, as defined, for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. The bill would require a business to make a Data Protection Impact Assessment available, within 5 business days, to the Attorney General pursuant to a written request and would exempt a Data Protection Impact Assessment from public disclosure, as prescribed. The bill would prohibit a business that provides an online service, product, or feature likely to be accessed by children from taking proscribed action, including, if the end user is a child, using personal information for any reason other than a reason for which the personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

This bill would create the California Children's Data Protection Working Group to deliver a report to the Legislature regarding best practices for the implementation of these provisions, as specified. The bill would require the members of the working group to have certain expertise, including in the areas of children's data privacy and children's rights. The bill would require the working group to take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies, and make prescribed recommendations on best practices, including identifying online services, products, or features likely to be accessed by children.

This bill would authorize the Attorney General to seek an injunction or civil penalty against any business that violates its provisions. The bill would hold violators liable for a civil penalty of not more than $2,500 per affected child for each negligent violation or not more than $7,500 per affected child for each intentional violation. The bill would require any penalties, fees, and expenses recovered in an action brought under the act to be deposited in the Consumer Privacy Fund with the intent that they be used to fully offset costs incurred by the Attorney General in connection with the act.

(2) The California Privacy Rights Act of 2020 authorizes the Legislature to amend the act to further the purposes and intent of the act by a majority vote of both houses of the Legislature, as specified.

This bill would declare that its provisions further the purposes and intent of the California Privacy Rights Act of 2020.

(3) Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

The people of the State of California do enact as follows:

SECTION 1. (a) The Legislature hereby finds and declares all of the following:

(1) The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care in all aspects of their lives.

(2) As children spend more of their time interacting with the online world, the impact of the design of online products and services on children's well-being has become a focus of significant concern.

(3) There is bipartisan agreement at the international level, in both the United States and in the State of California, that more needs to be done to create a safer online space for children to learn, explore, and play.

(4) Lawmakers around the globe have taken steps to enhance privacy protections for children on the understanding that, in relation to data protection, greater privacy necessarily means greater security and well-being.

(5) Children should be afforded protections not only by online products and services specifically directed at them, but by all online products and services they are likely to access. In order to help support the design of online products, services, and features, businesses should take into account the unique needs of different age ranges, including the following developmental stages: 0 to 5 years of age or "preliterate and early literacy"; 6 to 9 years of age or "core primary school years"; 10 to 12 years of age or "transition years"; 13 to 15 years of age or "early teens"; and 16 to 17 years of age or "approaching adulthood."

(6) In 2019, 81 percent of voters said they wanted to prohibit companies from collecting personal information about children without parental consent, and a 2018 poll of Californian parents and teens found that only 36 percent of teenagers and 32 percent of parents say that social networking internet websites do a good job explaining what they do with users' data.

(7) While it is clear that the same data protection regime may not be appropriate for children of all ages, children of all ages should nonetheless be afforded privacy and protection, and online products and services should adopt data protection regimes appropriate for children of the ages likely to access those products and services.

(8) Online services, products, or features that are likely to be accessed by children should offer strong privacy protections by design and by default, including by disabling features that profile children using their previous behavior, browsing history, or assumptions of their similarity to other children, to offer detrimental material.

(9) Ensuring robust privacy protections for children by design is consistent with the intent of the Legislature in passing the California Consumer Privacy Act of 2018, and with the intent of the people of the State of California in passing the California Privacy Rights Act of 2020, which finds and declares that children are particularly vulnerable from a negotiating perspective with respect to their privacy rights.

(10) The California Privacy Protection Agency, created by the California Privacy Rights Act of 2020, has substantial and growing expertise that is integral to the development of privacy policy in California.

(b) Therefore, it is the intent of the Legislature to promote privacy protections for children pursuant to the California Age-Appropriate Design Code Act.

(c) It is the intent of the Legislature that the California Age-Appropriate Design Code promote innovation by businesses whose online products, services, or features are likely to be accessed by children by ensuring that those online products, services, or features are designed in a manner that recognizes the distinct needs of children at different age ranges.

(d) It is the intent of the Legislature that businesses covered by the California Age-Appropriate Design Code may look to guidance and innovation in response to the Age-Appropriate Design Code established in the United Kingdom when developing online services, products, or features likely to be accessed by children.

(e) It is the intent of the Legislature that the California Children's Data Protection Working Group consider the guidance provided by the Information Commissioner's Office in the United Kingdom when developing and reviewing best practices or other recommendations related to the California Age-Appropriate Design Code.

(f) It is the intent of the Legislature that the California Children's Data Protection Working Group and the Department of Justice leverage the substantial and growing expertise of the California Privacy Protection Agency in the implementation of this title.

SEC. 2. Title 1.81.47 (commencing with Section 1798.99.28) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.47. THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

1798.99.28. This title shall be known, and may be cited, as the California Age-Appropriate Design Code Act.

1798.99.29. The Legislature declares that children should be afforded protections not only by online products and services specifically directed at them but by all online products and services they are likely to access and makes the following findings:

(a) Businesses that develop and provide online services, products, or features that children are likely to access should consider the best interests of children when designing, developing, and providing that online service, product, or feature.

(b) If a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests.

1798.99.30. (a) For purposes of this title, the definitions in Section 1798.140 shall apply unless otherwise specified in this title.

(b) For the purposes of this title:

(1) "Child" or "children," unless otherwise specified, means a consumer or consumers who are under 18 years of age.

(2) "Data Protection Impact Assessment" means a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online

service, product, or feature at issue that arises from the provision of that online service, product, or feature.

(3) "Default" means a preselected option adopted by the business for the online service, product, or feature.

(4) "Likely to be accessed by children" means it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children:

(A) The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.).

(B) The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

(C) An online service, product, or feature with advertisements marketed to children.

(D) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B).

(E) An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children.

(F) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.

(5) "Online service, product, or feature" does not mean any of the following:

(A) A broadband internet access service, as defined in Section 3100.

(B) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code.

(C) The delivery or use of a physical product.

(6) "Profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

1798.99.31. (a) A business that provides an online service, product, or feature likely to be accessed by children shall take all of the following actions:

(1) (A) Before any new online services, products, or features are offered to the public, complete a Data Protection Impact Assessment for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. A business shall biennially review all Data Protection Impact Assessments.

(B) The Data Protection Impact Assessment required by this paragraph shall identify the purpose of the online service, product, or feature, how it uses children's personal information, and the risks of material detriment to children that arise from the data management practices of the business. The

Data Protection Impact Assessment shall address, to the extent applicable, all of the following:

(i) Whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product, service, or feature.

(ii) Whether the design of the online product, service, or feature could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online product, service, or feature.

(iii) Whether the design of the online product, service, or feature could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the online product, service, or feature.

(iv) Whether the design of the online product, service, or feature could allow children to be party to or exploited by a harmful, or potentially harmful, contact on the online product, service, or feature.

(v) Whether algorithms used by the online product, service, or feature could harm children.

(vi) Whether targeted advertising systems used by the online product, service, or feature could harm children.

(vii) Whether and how the online product, service, or feature uses system design features to increase, sustain, or extend use of the online product, service, or feature by children, including the automatic playing of media, rewards for time spent, and notifications.

(viii) Whether, how, and for what purpose the online product, service, or feature collects or processes sensitive personal information of children.

(2) Document any risk of material detriment to children that arises from the data management practices of the business identified in the Data Protection Impact Assessment required by paragraph (1) and create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is accessed by children.

(3) Within three business days of a written request by the Attorney General, provide to the Attorney General a list of all Data Protection Impact Assessments the business has completed.

(4) (A) For any Data Protection Impact Assessment completed pursuant to paragraph (1), make the Data Protection Impact Assessment available, within five business days, to the Attorney General pursuant to a written request.

(B) Notwithstanding any other law, a Data Protection Impact Assessment is protected as confidential and shall be exempt from public disclosure, including under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

(C) To the extent any information contained in a Data Protection Impact Assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, disclosure pursuant to this paragraph shall not constitute a waiver of that privilege or protection.

(5) Estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of

the business or apply the privacy and data protections afforded to children to all consumers.

(6) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.

(7) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.

(8) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked.

(9) Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.

(10) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

(b) A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions:

(1) Use the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child.

(2) Profile a child by default unless both of the following criteria are met:

(A) The business can demonstrate it has appropriate safeguards in place to protect children.

(B) Either of the following is true:

(i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged.

(ii) The business can demonstrate a compelling reason that profiling is in the best interests of children.

(3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children likely to access the online service, product, or feature.

(4) If the end user is a child, use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

(5) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature.

(6) Collect any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.

(7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.

(8) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.

(c) (1) A Data Protection Impact Assessment conducted by a business for the purpose of compliance with any other law complies with this section if the Data Protection Impact Assessment meets the requirements of this title.

(2) A single data protection impact assessment may contain multiple similar processing operations that present similar risks only if each relevant online service, product, or feature is addressed.

(d) This section shall become operative on July 1, 2024.

1798.99.32. (a) The California Children's Data Protection Working Group is hereby created to deliver a report to the Legislature, pursuant to subdivision (e), regarding best practices for the implementation of this title.

(b) Working Group members shall consist of Californians with expertise in at least two of the following areas:

(1) Children's data privacy.

(2) Physical health.

(3) Mental health and well-being.

(4) Computer science.

(5) Children's rights.

(c) The working group shall select a chair and a vice chair from among its members and shall consist of the following 10 members:

(1) Two appointees by the Governor.

(2) Two appointees by the President Pro Tempore of the Senate.

(3) Two appointees by the Speaker of the Assembly.

(4) Two appointees by the Attorney General.

(5) Two appointees by the California Privacy Protection Agency.

(d) The working group shall take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies and

shall make recommendations to the Legislature on best practices regarding, at minimum, all of the following:

(1) Identifying online services, products, or features likely to be accessed by children.

(2) Evaluating and prioritizing the best interests of children with respect to their privacy, physical health, and mental health and well-being and evaluating how those interests may be furthered by the design, development, and implementation of an online service, product, or feature.

(3) Ensuring that age assurance methods used by businesses that provide online services, products, or features likely to be accessed by children are proportionate to the risks that arise from the data management practices of the business, privacy protective, and minimally invasive.

(4) Assessing and mitigating risks to children that arise from the use of an online service, product, or feature.

(5) Publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access an online service, product, or feature.

(6) How the working group and the Department of Justice may leverage the substantial and growing expertise of the California Privacy Protection Agency in the long-term development of data privacy policies that affect the privacy, rights, and safety of children online.

(e) On or before January 1, 2024, and every two years thereafter, the working group shall submit, pursuant to Section 9795 of the Government Code, a report to the Legislature regarding the recommendations described in subdivision (d).

(f) The members of the working group shall serve without compensation but shall be reimbursed for all necessary expenses actually incurred in the performance of their duties.

(g) This section shall remain in effect until January 1, 2030, and as of that date is repealed.

1798.99.33. (a) A business shall complete a Data Protection Impact Assessment 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.

(b) This section does not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2024.

1798.99.35. (a) Any business that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation, which shall be assessed and recovered only in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Any penalties, fees, and expenses recovered in an action brought under this title shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160,

with the intent that they be used to fully offset costs incurred by the Attorney General in connection with this title.

(c) (1) If a business is in substantial compliance with the requirements of paragraphs (1) through (4), inclusive, of subdivision (a) of Section 1798.99.31, the Attorney General shall provide written notice to the business, before initiating an action under this title, identifying the specific provisions of this title that the Attorney General alleges have been or are being violated.

(2) If, within 90 days of the notice required by this subdivision, the business cures any noticed violation and provides the Attorney General a written statement that the alleged violations have been cured, and sufficient measures have been taken to prevent future violations, the business shall not be liable for a civil penalty for any violation cured pursuant to this subdivision.

(d) Nothing in this title shall be interpreted to serve as the basis for a private right of action under this title or any other law.

(e) The Attorney General may solicit broad public participation and adopt regulations to clarify the requirements of this title.

1798.99.40. This title does not apply to the information or entities described in subdivision (c) of Section 1798.145.

SEC. 3. The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020.

SEC. 4. The Legislature finds and declares that Section 2 of this act, which adds Title 1.81.46 (commencing with Section 1798.99.28) to Part 4 of Division 3 of the Civil Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The limitation is needed to encourage businesses, by protecting their proprietary interests, to mitigate risks to children online.

O