**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| NETCHOICE,<br>*Plaintiff*,<br>v.<br>ANTHONY G. BROWN, et al.,<br>*Defendants*. | Civil Action No. 1:25-cv-00322-RDB |

**AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF**

1. Under the guise of protecting minors' privacy online, Maryland has enacted sweeping restrictions on free speech. The Maryland Age-Appropriate Design Code Act ("Act") imposes an unconstitutional and unlawful censorship regime that will fundamentally reshape how websites speak to their users and how hundreds of millions of Americans access information—and what information they see—online. *See* Ex. A (enacted legislative text).[1]

2. The Act compels websites to act as government speech police, forces them to stigmatize their own services through mandatory self-criticism, and requires them to alter their protected editorial functions through a vague and subjective "best interests of children" standard that gives state officials nearly boundless discretion to restrict vast amounts of protected speech.

3. Like several other States, Maryland enacted the Act in a misguided attempt to regulate the speech available to minors. *See NetChoice, LLC v. Bonta*, 113 F.4th 1101 (9th Cir. 2024); ECF 56, *NetChoice, LLC v. Yost*, No. 2:24-CV-00047, 2025 WL 1137485, at *2 (S.D. Ohio Apr. 16, 2025); *NetChoice v. Griffin*, 2025 WL 978607, at *1 (W.D. Ark. Mar. 31, 2025) ("*Griffin II*"); *NetChoice, LLC v. Bonta*, 2025 WL 807961, at *15 (N.D. Cal. Mar. 13, 2025); *Comput. &*

[1] This Amended Complaint uses the term "service" or "website" to include all regulated "online service[s]," § 14-4801(m)(1), including applications and other software. Unless otherwise noted, all statutory citations are citations to the Maryland Commercial Law Code.

*Commnc'ns Indus. Ass'n and NetChoice v. Paxton*, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024); *NetChoice, LLC v. Reyes*, 2024 WL 4135626 (D. Utah Sept. 10, 2024).

4. Here, Maryland purports to protect children by regulating "data" and website "design." § 14-4801(c). But like the laws enjoined in *Yost*, *Griffin*, *Bonta*, *Paxton*, and *Reyes*, the Act in fact regulates speech. The Act's central mandate is that for-profit websites must "ensure the best interests of children when designing, developing, and providing" online services that deliver online speech. § 14-4803(2). In both purpose and effect, that mandate is a regulation of speech. Websites cannot evaluate whether their "design" or use of "data" is in the best interests of children "without also demonstrating that the [website] prioritizes the dissemination of *one type of content over another*." *M.P. by & through Pinckney v. Meta Platforms Inc.*, 127 F.4th 516, 525 (4th Cir. 2025) (emphasis added).

5. That this Act is a content-based restriction on speech—not a privacy regulation—is laid bare by the fact that Maryland enacted it on the same day it also enacted the Maryland Online Data Privacy Act ("MODPA"). MODPA is one of the most stringent and comprehensive data privacy bills in the country, with specific and heightened protections for the data of minors. Maryland's simultaneous adoption of MODPA as an independent privacy regime renders this Act superfluous to serve any interest the State has in regulating data privacy of minors. *See* Md. Sen. Bill 541 (2024).

6. Nor does the fact that the Act advances its objectives in part by purporting to regulate "data" avoid the First Amendment problem. "Laws enacted to control or suppress speech may operate at different points in the speech process." *Citizens United v. FEC*, 558 U.S. 310, 336 (2010). The Supreme Court has therefore recognized that "regulation of a medium [of expression] inevitably affects communication itself." *City of Ladue v. Gilleo*, 512 U.S. 43, 48 (1994).

7. Online services rely on user data to disseminate and curate speech. So a presumptive prohibition on websites' use of data is comparable "to a law prohibiting trade magazines from purchasing or using ink." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 571 (2011); *see also W. Watersheds Project v. Michael*, 869 F.3d 1189, 1195–96 (10th Cir. 2017) (the "collection of resource data constitutes the protected creation of speech").

8. In any event, restricting "access to information in private hands" requires strict scrutiny where it serves as "a subsidy to people who wish to speak about certain topics." *Sorrell*, 564 U.S. at 568. This Act does so by favoring topics that meet the Act's vague articulation of minors' "best interests" and burdening everything else. Such a "statute is presumptively inconsistent with the First Amendment [because] it imposes a financial burden on speakers because of the content of their speech," and thus "raises the specter that the government may effectively drive certain ideas or viewpoints from the marketplace." *Simon & Schuster, Inc. v. Members of New York State Crime Victims Bd.*, 502 U.S. 105, 115 (1991).

9. And by imposing the "best interests" mandate on websites that facilitate, curate, and disseminate enormous amounts of *third-party* speech, the Act also "deputizes covered businesses into serving as censors for the State." *Bonta*, 113 F.4th at 1118 (citing *Interstate Cir., Inc. v. City of Dallas*, 390 U.S. 676, 678, 684 (1968)).

10. All of this is blatantly unconstitutional. Maryland lacks a "free-floating power to restrict the ideas to which children may be exposed," *Brown v. Ent. Merch. Ass'n*, 564 U.S. 786, 799 (2011). "On the spectrum of dangers to free expression, there are few greater than allowing the government to change the speech of private actors in order to achieve its own conception of speech nirvana." *Moody v. NetChoice, LLC*, 603 U.S. 707, 741–42 (2024). Laws that "curtail[]

the[] editorial choices" of online services must therefore "meet the First Amendment's requirements." *Id.* at 717.

11. Numerous courts have now applied these principles to block other States' similar attempts to restrict online speech in the interests of protecting minors. In *Bonta*, a California district court has now concluded for the second time that the California Age-Appropriate Design Code—on which this Act is modeled—is likely an unconstitutional restriction of speech and preliminarily enjoined the Act in its entirety. *See* 2025 WL 807961, at *7-14, 33. In *Paxton*, a Texas district court enjoined a law requiring online services to "monitor certain categories of content" deemed harmful "and filter them from being on display for known minors." 747 F. Supp. 3d at 1023. In *Reyes*, a Utah district court likewise enjoined a law that imposed on social media companies "special rules with respect to Utah minors' accounts," including restrictions on core expressive features and the use and collection of data. 748 F. Supp. 3d at 1114. And in *Yost* and *Griffin*, district courts in Ohio and Arkansas similarly enjoined laws that burdened minors' access to online speech. *See Yost*, 2025 WL 1137485, at *15-24; *Griffin*, 2025 WL 978607, at *17.

12. Maryland's approach is just as restrictive—and unconstitutional—in both scope and effect as the laws at issue in these cases. The Act's fundamental flaw is its central command: requiring websites to analyze and restrict substantial amounts of protected expressive content based on whether it would serve the "best interests of children." § 14-4801(c). This vague standard—which defines websites' obligations throughout the Act—is inherently subjective and cannot be applied without evaluating a website's content. It will force websites to restrict speech and self-censor to avoid crushing penalties of up to $7,500 per minor for each violation. § 14-4808(b).

13. If there were any doubt about the Act's censorial aim, it is removed by the provisions compelling mandatory "Data Protection Impact Assessments." § 14-4804. These

assessments force websites to engage in self-criticism and prediction of hypothetical harms that could befall minors who access the service and certain types of content—exactly the type of compelled speech that the Ninth Circuit held unconstitutional in California's similar law. *Bonta*, 113 F.4th at 1117-18.

14. The practical effects of the Act will be severe. To comply with its vague mandates, websites will be forced to:

- Significantly restrict content available to all users;
- Disable core features that allow users to find and share protected information;
- Engage in mandatory self-criticism through compelled assessments; and
- Face impossible choices between over-restricting speech or risking crippling penalties.

15. These harms will befall both regulated websites and their millions of users who depend on the services "to gain access to information[,] communicate with one another," and "engage[] in a wide array of protected First Amendment activity." *Packingham v. North Carolina*, 582 U.S. 98, 105, 107 (2017).

16. The Act also is preempted under multiple federal laws, such as the Children's Online Privacy Protection Act and 47 U.S.C. § 230.

17. Defendants have acknowledged many of the Act's constitutional problems. In a letter to the Maryland Governor, Defendants warned of the "risk that if the legislation is challenged, a reviewing court will construe some of the Maryland Act's provisions . . . to regulate speech or other expressive conduct, and . . . find those provisions unconstitutional." Ex. B. at 2.

18. Defendants understated the Act's problems.

19. Perhaps in recognition of these flaws, Maryland legislators exerted their influence to get NetChoice members to discourage NetChoice from bringing this lawsuit. *See* Ex. C.

20. The well-being of children is undisputedly of great importance. But the Act regulates far beyond privacy, running roughshod over the constitutional and statutory rights of online services—and their users. It is a misguided effort to redesign the Internet and restrict speech.

21. For these reasons and more, this Court should enjoin Defendants from enforcing the Act and declare the Act unlawful.

## PARTIES & STANDING

22. Plaintiff NetChoice is a District of Columbia nonprofit trade association for Internet companies. NetChoice's mission is to promote online commerce and speech and to increase consumer access and options via the Internet, while minimizing burdens that could prevent businesses from making the Internet more accessible and useful. NetChoice's members are listed at NetChoice, About Us, https://netchoice.org/about/.

23. NetChoice has standing to bring its challenges on at least two grounds.

24. *First*, NetChoice has associational standing to challenge the Act, because: (1) some of NetChoice's members have individual standing to sue in their own right; (2) challenging the Act is germane to NetChoice's purpose; and (3) members' individual participation is unnecessary in this purely legal challenge. *See Hunt v. Wash. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977); *Yost*, 2025 WL 1137485, at *7; *Reyes*, 2024 WL 4135626, at *7; *CCIA*, 2024 WL 4051786, at *7-9; *NetChoice, LLC v. Griffin*, 2023 WL 5660155, at *9 (Aug. 31, 2023) ("*Griffin I*").

25. Based on the Act's definitions, § 14-4801(h), many—if not most—of NetChoice's members with online services are directly subject to and regulated by the Act and could face serious legal consequences if they violate it. And importantly, although a handful of members might not be subject to the Act (although under the Act's vague coverage standards they cannot know for sure) it is undeniable that the covered members create, curate, and disseminate enormous amounts

of protected speech, including, *e.g.*, Amazon, Google, Meta, Nextdoor, Pinterest, Netflix, Reddit, and X.

26. This lawsuit is directly germane to NetChoice's mission to promote online commerce and speech and minimize burdens that make the Internet less accessible and useful.

27. And the attributes that make the Act unlawful as to every regulated website apply in substantially similar ways across NetChoice's covered members. Individualized participation in the lawsuit is unnecessary.

28. *Second*, NetChoice has standing to assert the First Amendment rights of members' current and prospective users. *Virginia v. Am. Booksellers Ass'n*, 484 U.S. 383, 392-93 (1988); *Yost*, 2025 WL 1137485, at *8-14; *Griffin II*, 2025 WL 978607, at *6; *CCIA*, 2024 WL 4051786, at *9; *Griffin I*, 2023 WL 5660155, at *11-12.

29. Defendant Anthony G. Brown is the Maryland Attorney General. Defendant is a Maryland resident and is sued in his official capacity.

30. Defendant William D. Gruhn is the Chief of the Division of Consumer Protection of the Office of the Maryland Attorney General. Defendant is a Maryland resident and is sued in his official capacity.

31. The Act gives the Division of Consumer Protection of the Office of the Maryland Attorney General authority to enforce the Act. *See* §§ 14-4807 to -4809.

## JURISDICTION & VENUE

32. This Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331 and 1343(a). This Court has authority to grant legal and equitable relief under 42 U.S.C. § 1983, injunctive relief under 28 U.S.C. § 1651, and declaratory relief under 28 U.S.C. § 2201(a).

33. Federal courts have the power to enjoin unlawful actions by state officials. *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 326 (2015).

34. This Court has personal jurisdiction over Defendants because they reside in and/or conduct a substantial proportion of their official business in Maryland.

35. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants reside in, and the events giving rise to this civil action occurred in, Maryland.

## BACKGROUND

36. **Online services—including NetChoice members—create, disseminate, and facilitate enormous amounts of protected speech.** The "vast democratic forums of the Internet" are home to immense amounts of First Amendment activity. *Packingham*, 582 U.S. at 104 (citing *Reno v. ACLU*, 521 U.S. 844, 868 (1997)). This includes "not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue" such as "chat rooms" and "newsgroups." *Reno*, 521 U.S. at 870.

37. Not less is true of NetChoice members. "On Facebook, for example, users can debate religion and politics with their friends and neighbors or share vacation photos." *Packingham*, 582 U.S. at 104. "And on Twitter, users can petition their elected representatives and otherwise engage with them in a direct manner." *Id.* at 104-05. More generally, these and other "social media" websites, permit users worldwide to engage in massive amounts of expressive activity generating "billions of 'posts' every day" on wide-ranging topics from "vacation photos" to "travel documentaries" to "writing, artwork, and innermost thoughts." *Yost*, 2025 WL 1137485, at *2; *see also Griffin II*, 2025 WL 978607, at *3. Social media services both facilitate the expressive activities of third parties (such as users and content creators) and also "engage[] in expression" themselves through their "display" and "compiling and curating" of protected content (text, audio, images, and video) "created by others." *Moody*, 603 U.S. at 728, 731, 740.

38. Search services also engage in protected expression by allowing their users to find protected expression and information from across the Internet. These services reduce the near-

infinite Internet into useful search results. Many courts have recognized that search engines have a First Amendment right to choose whether and how to display search results. *See Hopson v. Google, LLC*, 2023 WL 2733665, at *3 (W.D. Wis. Mar. 31, 2023); *e-ventures Worldwide, LLC v. Google, Inc.*, 2017 WL 2210029, at *4 (M.D. Fla. Feb. 8, 2017); *Jian Zhang v. Baidu.com Inc.*, 10 F. Supp. 3d 433, 438-43 (S.D.N.Y. 2014).

39. Beyond social media and search services exist a panoply of other digital services that disseminate speech. Video streaming services like Prime Video, Hulu, and Netflix offer on-demand movies, television shows, news, and other content. Audio streaming services, like Spotify, Apple Music, and Audible, offer music, podcasts, and e-books. Wordpress provides hosting services that allow individual content creators, like bloggers and businesses large and small, to host and maintain their own websites. Online news services (like nytimes.com and foxnews.com) and sports services (like ESPN) offer up-to-the-minute current events and sports and also create forums for their users to engage in discourse about the content they read. Online journals (like Science.org), online databases (like pubmed), and digital libraries (like JSTOR) provide access to scientific, historical, economic, and medical research. These are just a few examples; the Internet is "as diverse as human thought." *Reno*, 521 U.S. at 870.

40. **Online services—including NetChoice members—use information to engage in editorial functions to publish, disseminate, and display protected speech to users.** Websites collect and use data to facilitate, curate, and publish all of this speech.

41. The information that websites collect and use varies, from information that helps make the services functional to information that enables websites to better disseminate and display expressive content to their users. Despite this variation, the information that websites use is much like the ink and paper necessary to publish newspapers—and the subscriber addresses necessary

to distribute the newspapers. Put another way, it is an often necessary part of disseminating protected speech to willing viewers and readers. It is also a building block in the further creation of speech.

42. *Data necessary to provide the service.* Data collection is necessary just to provide functional services and content. Websites collect information about IP address, device type, operating system, screen resolution, browser type, language preferences, and time zone to determine where content should be disseminated and how to present it. For example, covered entities require an IP address to disseminate content to a user at all. An IP address acts like a digital mailing address, allowing packets of information to be routed to a particular device or server. Absent an IP address, covered entities could not direct their content to an end recipient.

43. Similarly, other information—like a user's operating system and language preferences—allow covered entities to format their content in a way that will be decipherable to the user, like choosing the correct format of a video based on device type and screen resolution.

44. User data is also needed to deter and detect malicious actors. Many websites log activity and changes on an account to help detect behavior that could signal a compromised account, or help users restore accounts. Without the ability to collect and use data for these purposes, services would be significantly less functional and also less secure.

45. *Information to access services.* Many websites have aspects that are optimized and available only for individuals who create an account. 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.

46. Allowing users to create accounts provides those users with greater security and provides services with a means to provide those users with curated content. But to offer account-

based functionalities, websites must collect and process information that users provide, such as usernames, contact information, and security questions.

47. *Information to exercise editorial discretion to personalize content available to users.* Many websites collect and use information about a person's usage to help personalize experiences on the websites. This aims to ensure that people see the content they want to see, in the order they want to see it, while avoiding or deprioritizing content they do not want to see.

48. For instance, the Supreme Court recognized that personalized feeds—including the curated feeds of "Facebook" and "YouTube"—are protected. *Moody*, 603 U.S. at 734-35, 739-40.

49. "A user does not see everything—even everything from the people she follows—in reverse-chronological order. The platforms will have removed some content entirely; ranked or otherwise prioritized what remains; and sometimes added warnings or labels" *Id.* at 719.

50. That includes when websites use "algorithms" to curate content:

> [W]henever a user signs on, Facebook delivers a *personalized* collection of those stories. Similarly for YouTube. . . . And any person opening the website or mobile app receives an *individualized* list of video recommendations. The key to the scheme is prioritization of content, achieved through the use of *algorithms*. Of the billions of posts or videos (plus advertisements) that could wind up on a user's *customized* feed or recommendations list, only the tiniest fraction do. The selection and ranking is *most often based on a user's expressed interests and past activities*.

*Id.* at 734-35 (emphases added).

51. Websites' use of information to curate and disseminate speech has a long historical pedigree. As one example, Benjamin Franklin's *Poor Richard's Almanack* "focused on the interests of his prospects and customers." Scott Aughtmon, *4 Illuminating Lessons From One of History's Most Inventive Content Marketers*, Content Marketing Institute (Apr. 9, 2014), https://perma.cc/F7KV-DMUU. He "was what we'd call a content curator," taking content created by others and tailoring it to his audience based on information gleaned from his audience. *Id.*

52. Content curation, whether through algorithms or other information-reliant means, allows users to see and engage with content they find most useful. In cyberspace, this includes content from people they "follow" or "subscribe" to, recommended content, alerts about developing events, and advertisements that help make the services viable. Without curation, many online users would be lost in a potential "deluge" of content. *Moody*, 603 U.S. at 719.

53. **Existing options for parental control and oversight.** As multiple courts have recognized, parents have many existing and diverse choices to regulate and oversee whether and how their minor children use the Internet. *See Yost*, 2025 WL 1137485, at *22; *Griffin II*, 2025 WL 978607, at *3; *Reyes*, 2024 WL 4135626, at *13 n.138; Parental Control Guides, Internet Matters, https://perma.cc/VNA6-W76A.

54. These existing market solutions underscore the Act's overreach—less restrictive alternatives both exist and many parents are already using them.

55. And these existing solutions allow parents to tailor their approaches to the needs of their families, which would provide bespoke solutions as compared to one-size-fits-all solutions.

56. Parents decide whether and when to let their minor children use computers, tablets, smartphones, and other devices to access the Internet.

57. Cellular and broadband Internet providers offer families tools to block certain online services from certain devices. *See, e.g.*, Verizon, Verizon Smart Family, https://perma.cc/MCD6-RJAR; AT&T, AT&T Secure Family, https://perma.cc/8XAE-YHRD; T-Mobile, Family Controls and Privacy, https://perma.cc/TN3M-459E.

58. Internet browsers also allow parents to control what online services their children may access. *See, e.g.*, Mozilla, Block and Unblock Websites with Parental Controls on Firefox, https://perma.cc/3786-LSNK. For example, some browsers offer a "kids mode" or allow parents

to see what online services their children are accessing the most. *See* Google, Safety Center, https://perma.cc/AE3B-K8VA. Parents can also use widely available browser extensions to reinforce these tools. *See, e.g.*, Kim Key, *The Best Parental Control Software for 2025*, PCMag (Nov. 15, 2024), https://perma.cc/L6EZ-EWAK.

59. Wireless routers often have settings allowing parents to block particular websites, filter content, monitor Internet usage, and control time spent on the Internet. *See, e.g.*, Netgear, Netgear Smart Parental Controls, https://perma.cc/9L8K-CXMK; tp-link, How to Configure Parental Controls on the Wi-Fi Routers (Case 1), https://perma.cc/T9J6-VRLD.

60. Devices allow parents to limit the time their children spend on the device, curtail the applications that can be used, filter online content, and control privacy settings. *See* Apple, Use Parental Controls on Your Child's iPhone and iPad, https://perma.cc/TX8D-EMQU; Google Family Link, Help Keep Your Family Safer Online, https://perma.cc/MGK7-DPCL; Samsung, Parental Controls Available on Your Galaxy Phone or Tablet, https://perma.cc/H94Q-XWRN.

61. Many third-party applications also allow parents to control and monitor their children's online activities. *See, e.g.*, Kim Key, *The Best Parental Control Software for 2025*, PCMag (Nov. 15, 2024), https://perma.cc/L6EZ-EWAK.

62. In addition, many private entities, including some NetChoice members, provide parents with tools and options to help monitor their minor children's activities on their services.

63. NetChoice members also expend vast resources to improve their services and curate the content on their websites to best ensure that it is appropriate for the user community they seek to foster. Some restrict the publication of content they consider harmful, like violent and sexual content, bullying, harassment, and content that encourages body shaming or eating disorders and seek to promote positive and age-appropriate content. Others take a more hands-off approach under

the philosophy that their users (and parents) can decide for themselves what they wish to engage with and what filters to adopt.

**MARYLAND AGE-APPROPRIATE DESIGN CODE ACT**

64. On April 6, 2024, the Maryland Legislature enacted the Age-Appropriate Design Code Act, which seeks to regulate the content on covered websites under the guise of privacy regulations. At the time the Act was enacted, Maryland already had a panoply of other laws designed to protect minors from harm, both online and offline, including bullying, hazing, stalking, online "surveillance" and other "privacy" harms, and deceptive practices. These separate laws are not the subject of this challenge.

65. Also on April 6, 2024, the Maryland Legislature enacted MODPA, which imposes comprehensive data-privacy regulations. Md. Sen. Bill 541 (2024). MODPA is not the subject of this challenge either.

66. The Age-Appropriate Design Code Act challenged here took effect October 1, 2024. But covered entities' first compelled-speech Data Protection Impact Assessment required by the Act are due April 1, 2026.

67. **Central coverage provisions defining "covered entit[ies]" that are "[r]easonably likely to be accessed by" minors (§ 14-4801(h), (s)).** The Act's speech regulations apply to websites that meet the definition of "covered entity," are not otherwise exempted, and are as the Act defines it "reasonably likely to be accessed by children."

68. *Covered entities.* A "[c]overed entity" is any "sole proprietorship, a limited liability company, a corporation, an association, or any other legal entity that":

> (i) Is organized or operated for the profit or financial benefit of its shareholders or other owners;
> (ii) Collects consumers' personal data or uses another entity to collect consumers' personal data on its behalf;

(iii) Alone, or jointly with its affiliates or subsidiaries, determines the purposes and means of the processing of consumers' personal data;
(iv) Does business in the State; and
(v) 1. Has annual gross revenues in excess of $25,000,000, adjusted every odd-numbered year to reflect adjustments in the Consumer Price Index;
2. Annually buys, receives, sells, or shares the personal data of 50,000 or more consumers, households, or devices, alone or in combination with its affiliates or subsidiaries, for the covered entity's commercial purposes; or
3. Derives at least 50% of its annual revenues from the sale of consumers' personal data.

§ 14-4801(h)(1).

69. To "[c]ollect" personal data means to "buy, rent, gather, obtain, receive, or access personal data relating to a consumer," including "[r]eceiving data from the consumer" and "[o]bserving the consumer's behavior." § 14-4801(f).

70. "Personal data" is any "information that is linked or reasonably able to be linked to an identified or identifiable individual" but "does not include: (i) De-identified data; or (ii) Publicly available information." § 14-4801(n).

71. "Publicly available information" is any "information that: (i) Is lawfully made available from federal, state, or local government records; or (ii) A covered entity has a reasonable basis to believe is lawfully made available to the general public by the consumer or by widely distributed media." § 14-4801(r)(1). But it "does not include biometric data collected by a covered entity about a consumer without the consumer's knowledge." § 14-4801(r)(2).

72. Even if an entity otherwise qualifies as "[c]overed," the entity is exempt if it falls within one of several exempt categories outlined in Section 14-4802. These include certain financial institutions and entities subject to the Health Insurance Portability and Accountability Act of 1996.

73. *"Reasonably likely to be accessed by" minors standard.* For covered entities, the Act's operative requirements only apply to services that are "[r]easonably likely to be accessed by children," § 14-4801(s), *i.e.*, Maryland residents younger than 18, § 14-4801(e).

74. To be "[r]easonably likely to be accessed by children," it must be "reasonable to expect that the online product would be accessed by children, based on satisfying any of the following criteria":

> (1) The online product is directed to children as defined in the federal Children's Online Privacy Protection Act;
> (2) The online product is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children;
> (3) The online product is substantially similar or the same as an online product that satisfies item (2) of this subsection;
> (4) The online product features advertisements marketed to children;
> (5) The covered entity's internal research findings determine that a significant amount of the online product's audience is composed of children; or
> (6) The covered entity knows or should have known that a user is a child.

§ 14-4801(s).

75. A "consumer" is "an individual who is a resident of the State." § 14-4801(g).

76. An "[o]nline product" is any "online service, product, or feature." § 14-4801(m).

77. **Central "best interests of children" standard (§ 14-4801(c)).** The Act's operative speech restrictions all rely on the vague, subjective, multi-faceted, and indeterminate "best interests of children" standard set by the Act. § 14-4801(c).

78. This standard suffuses the Act.

79. This standard necessarily requires consideration of the content on the services and how that content is displayed to users.

80. The Legislature codified its "intent" that:

> (2) Covered entities that develop and provide online products that children are reasonably likely to access *shall ensure* the best interests of children when *designing, developing, and providing* those online products;

> (3) All covered entities that operate in the State and process children's data *in any capacity shall* do so in a manner consistent with the best interests of children;
> (4) If a conflict arises between commercial interests and the best interests of children, covered entities that develop online products likely to be accessed by children *shall* prioritize the privacy, safety, and well-being of children.

§ 14-4803 (emphases added).

81. The mandatory language in this provision may impose a standalone obligation on websites to act in the "best interests of children" and "prioritize the privacy, safety, and well-being of children" across their activities. This mandate applies on top of the Act's specific regulations.

82. Evaluating the "best interests of children" requires an inquiry into whether "a covered entity's use of the personal data of children or the design of an online product [is carried out] in a way that does not":

> (1) Benefit the covered entity to the detriment of children; and
> (2) Result in:
> (i) Reasonably foreseeable and material physical or financial harm to children;
> (ii) Severe and reasonably foreseeable psychological or emotional harm to children;
> (iii) A highly offensive intrusion on children's reasonable expectation of privacy; or
> (iv) Discrimination against children based on race, color, religion, national origin, disability, gender identity, sex, or sexual orientation.

§ 14-4801(c).

None of these terms is defined, and to the extent they resemble terms used in other legal frameworks, it is not clear what they mean as applied to data "processing" and digital "design." Data processing is an intangible activity that does not, by itself, harm anyone, and covered entities will therefore inevitably look beyond their digital processing and design activities to the *content* those activities make available. Either way, covered entities lack the necessary guidance into what this standard requires them to disclose, do, or refrain from doing.

83. **Restrictions on using information to disseminate protected speech based on "best interests of children" standard (§ 14-4806).** The Act also creates a set of default presumptions against online services' ability to receive, use, and handle—or even *delete*—user data (what

the Act calls "processing" and "profiling"). These presumptions can only be overcome if, among other things, covered entities satisfy the "best interests of children" standard.

84. In particular, the Act provides that services that are "accessed or reasonably likely to be accessed" by minors may not "process" the personal data of a minor:

- in a way that is inconsistent with the best interests of children reasonably likely to access the online product, § 14-4806(a)(1); or
- that is not reasonably necessary to provide an online product that the child is actively and knowingly engaged with, § 14-4806(a)(3).

85. "Process" includes any collection, deletion, or use of information: "to perform an operation or set of operations by manual or automated means on personal data," including "collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data." § 14-4801(p).

86. The Act also restricts "profiling" a minor "by default, unless":

- The covered entity can demonstrate . . . appropriate safeguards in place to ensure that profiling is consistent with the best interests of children who access or are reasonably likely to access the online product; and
- profiling is necessary to provide the requested online product, and is done only with respect to the aspects of the online product that the child is actively and knowingly engaged with; *or*
- the covered entity can demonstrate a compelling reason that profiling is in the best interests of children.

§ 14-4806(a)(2) (emphasis added).

87. "Profile" means multiple ways that covered entities might personalize content. Specifically, it is "automated processing of personal data that uses personal data to evaluate, analyze, or predict certain aspects relating to an individual, including an individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." § 14-4801(q).

88. These restrictions go far beyond regulating data.

89. Instead, they restrict access to essential information needed to deliver content to users and a range of commonplace expressive activities that depend on such access. These include engaging with users to learn their preferences; using collected information to curate content; providing users with recommendations about books, movies, newspaper articles, and other content; and even potentially sending automated communications (such as email updates) to users.

90. To overcome these default prohibitions, covered entities must prove a negative under an unworkably subjective standard: that their communicative and expressive services will not benefit the entity "to the detriment of children" or "result in" downstream harm.

91. The Act also prohibits "[a]llow[ing] a person other than a child's parent or guardian to monitor the child's online activity without first notifying the child and the child's parent or guardian." § 14-4806(a)(9). The term "monitor" is not defined but could extend to a range of commonplace online expressive activities, such as "friending" a known contact to see that user's updates or "following" a particular content creator or influencer to view new posts.

92. Finally, the Act prohibits covered entities from using so-called "dark patterns" to: "(i) [c]ause a child to provide personal data beyond what is reasonably expected to provide the online product; (ii) [c]ircumvent privacy protections; or (iii) [t]ake any action that the covered entity knows, or has reason to know, is not in the best interests of children who access or are reasonably likely to access the online product." § 14-4806(a)(7).

93. A "[d]ark pattern means a user interface designed or manipulated with the purpose of subverting or impairing user autonomy, decision making, or choice," including "any practice identified by the Federal Trade Commission as a dark pattern." § 14-4801(i). Despite the ominous label, this term has been interpreted to encompass a range of commonplace publishing features

that simplify and improve user experience, such as "autoplay" and "newsfeed" functions that recommend personalized content.

94. **Compelled-speech Data Protection Impact Assessment about the "design" of websites and their collection and use of data (§ 14-4804).** Beginning April 1, 2026, covered entities must prepare a Data Protection Impact Assessment (Assessment) for every online product, service, or feature they offer "that is reasonably likely to be accessed by children." § 14-4804(a)(1).

95. An Assessment is a "systematic survey to assess compliance with the duty to act in the best interests of children." § 14-4801(j).

96. The Assessment "shall": identify the "purpose" of the online service or feature and how it uses children's data; determine "whether the online product is designed in a manner consistent with the best interests of children reasonably likely to access the online product"; and include "a description of steps that the covered entity has taken and will take to comply with the duty to act in a manner consistent with the best interests of children." § 14-4804(b).

97. In complying with the requirement to assess whether their services are "designed in a manner consistent with the best interests of children," covered entities must address the four categories of harm specified in the second prong of the "best interests of children standard" in relation to the following topics:

- Whether their "data management or processing practices":
  - "could lead to children experiencing or being targeted by contacts that would result in" any such harms;
  - "could permit children to participate in or be subject to conduct that would result in" any such harms; or
  - "are reasonably expected to allow children becoming party to or exploited by a contract through the online product that would result in" any such harms;
- Whether they use "system design features to increase, sustain, or extend the use of the online product, including the automatic playing of media, rewards for time spent, and notifications that would result in" any such harms;

- "Whether, how, and for what purpose" they collect or process "personal data of children and whether those practices would result in" any such harms;
- "Whether and how data collected to understand the experimental impact" of the service or feature "reveals data management or design practices that would result in" any such harms; and
- Whether "algorithms" used by the online service or feature would "result in" any such harms.

§ 14-4804(b)(3).

98. Again, the categories of harm that must be addressed are:

- A "reasonably foreseeable and material physical or financial" harm;
- A "reasonably foreseeable and extreme psychological or emotional" harm;
- A "highly offensive intrusion on children's reasonable expectation" of privacy; and "Discrimination against children based on race, color, religion, national origin, disability, gender identity, sex, or sexual orientation."

99. In addition to those specified categories, covered entities must "[d]etermine whether the online product is designed in a manner consistent with the best interests of children reasonably likely to access the online product through consideration of . . . *[a]ny other factor* that may indicate that the online product is designed in a manner that is inconsistent with the best interests of children." § 14-4804(b)(3)(viii) (emphasis added).

100. Covered entities must produce an Assessment for every qualifying service or feature "offered to the public on or before April 1, 2026" that will continue to be offered to the public after July 1, 2026, and for every qualifying service or feature initially offered after April 1, 2026. § 14-4804(a)(2)-(3).

101. Because an "online product" can mean everything from a "feature" to an entire "online service," § 14-4801(m)(1), entities that offer many "features" may be compelled to prepare multiple Assessments. "A single . . . assessment may contain multiple similar processing operations that present similar risks only if each relevant online product is addressed." § 14-4804(c)(2).

102. In addition to evaluating the foregoing "risks," Assessments must describe "steps that the covered entity *has taken and will take to comply with the duty to act in a manner consistent with the best interests of children*." § 14-4804(b)(4) (emphasis added).

103. The Act also imposes several ongoing obligations related to the Assessments.

104. *First*, covered entities must "[m]aintain documentation of the assessment for as long as the online product is likely to be accessed by children." § 14-4805(1).

105. *Second*, covered entities must "[r]eview each [assessment] as necessary to account for material changes to processing pertaining to the online product within 90 days of such material changes." § 14-4805(2).

106. *Third*, covered entities must make the Assessments available to Defendants in a variety of ways. § 14-4807(a)-(c).

107. In all, the Assessment requirements will both compel speech from covered entities, requiring them to disparage their services and opine on far-ranging and ill-defined harms arising from their content, and lead covered entities to alter their dissemination and display of online content so it serves the (vaguely articulated) "best interests of children."

108. **Enforcement (§ 14-4808).** The Act defines violations of its requirements as "subject to" Maryland's Consumer Protection Act. § 14-4808(a).

109. Maryland's Consumer Protection Act allows the Attorney General to investigate purported violations and seek injunctive and monetary relief, in addition to other fees and costs. §§ 13-405 to 409. It also allows for criminal penalties. § 13-411.

110. Under the Act, covered entities are "subject to a civil penalty not exceeding: (1) $2,500 per affected child for each negligent violation; and (2) $7,500 per affected child for each intentional violation." § 14-4808(b).

111. In addition, Maryland's Consumer Protection Act allows for *administrative* proceedings, where the Division of Consumer Protection acts as both prosecutor and judge. *See* § 13-403 (allowing for cease-and-desist orders, in addition to civil penalties). Maryland courts can only review such administrative orders under deferential standards of review. *Matter of Cricket Wireless, LLC*, 302 A.3d 1062, 1075 (Md. App. 2023).

112. When covered entities are in "substantial compliance"—an undefined term—the Act requires notice and an opportunity to cure. § 14-4809.

113. In light of these penalties, guessing wrong about what the Act means and who it covers is prohibitively expensive. 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 and curation of content on their services; forego efforts to connect their customers with suggested content or other users; or shut down altogether.

## CLAIMS

114. Each First and Fourteenth Amendment challenge set forth below raises the rights of both NetChoice members and those who use or could prospectively use NetChoice members' websites. *Am. Booksellers*, 484 U.S. at 393; *Yost*, 2025 WL 1137485, at *10-14; *Bonta*, 2023 WL 6135551, at *4; *Griffin*, 2023 WL 5660155, at *11-12.

### COUNT I
### 42 U.S.C. § 1983
### VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT ("BEST INTERESTS OF CHILDREN" STANDARD)

115. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

116. As incorporated against the States, the First Amendment's Free Speech and Free Press Clauses provide that government "shall make no Law . . . abridging the Freedom of Speech,

or of the Press." U.S. Const. amend. I. Among other things, the First Amendment protects "publish[ing]," *Reno*, 521 U.S. at 853; "disseminat[ing]," *303 Creative*, 600 U.S. at 594; and "creating, distributing, [and] consuming" speech. *Brown*, 564 U.S. at 792 n.1. Those rights apply to all manner of private entities. *Lovell v. City of Griffin*, 303 U.S. 444, 452 (1938).

117. Minors have robust First Amendment rights, and websites that publish and disseminate speech have the right to publish and disseminate speech to minors without governmental oversight. "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." *Brown*, 564 U.S. at 795 (citation omitted).

118. The Act's central "best interests of children" standard violates the First Amendment.

119. The "best interests of children" standard seeks to restrict protected speech to "protect the young from ideas or images that a legislative body thinks unsuitable for them." *Id.* It does so by "deputizing covered businesses into serving as censors for the State." *Bonta*, 113 F.4th at 1118. "The Supreme Court has previously applied First Amendment scrutiny to laws that deputize private actors into determining whether material is suitable for kids." *Id.* (citing *Interstate Cir., Inc. v. City of Dallas*, 390 U.S. 676, 678 (1968)). That is what this Act does.

120. The "best interests of children standard" is also content based. To evaluate whether online services and features could "result in" the broad categories of harm described under the Act (such as "extreme psychological or emotional harm" or "highly offensive" intrusions of privacy)—or *any* detriment to minors (as needed to weigh against any "benefit" to the entity)—covered entities must examine their content and the speakers on their services. They must also evaluate the

digital "contacts" that could occur through their services, which implicates protected communications as well.

121. These inquiries require websites to draw content-based and speaker-based distinctions. That is so even if the Act attempts to conceal this fact by purporting to regulate website "design" and "use of personal data." § 14-4801(c). *See M.P. v. Meta Platforms*, 127 F.4th at 525 (to assess whether website "design[]" was "dangerous" inevitably required evaluation of "content"). The Supreme Court's "precedents are deeply skeptical of laws that distinguish among different speakers, allowing speech by some but not others," because "[s]peaker-based laws run the risk that the State has left unburdened those speakers whose messages are in accord with its own views." *NIFLA*, 138 S. Ct. at 2378 (cleaned up).

122. The Supreme Court has also recognized that website "design" and the use of "data" are protected expressive activities. For example, "expressive choices" about "organizing," "select[ing]," and "presenting" content are themselves protected First Amendment activities, as are the "distinctive expressive product[s]" that result from those choices. *Moody*, 603 U.S. at 731, 734, 738, 740, 744. The Act requires strict scrutiny because it "interferes with such editorial choices" to "alter[] the content of the compilation." *Id.* at 732.

123. The Act's "reasonabl[e] foreseab[ility]," § 14-4801(c)(2)(i)-(ii), standard imposes further First Amendment problems. In general, the First Amendment forbids States from imposing liability for disseminating *even unprotected* speech unless the publishers know the nature of the allegedly unprotected speech. Negligence is not sufficient. *See Smith v. California*, 361 U.S. 147 (1959); *Counterman v. Colorado*, 600 U.S. 66, 79 & n.5 (2023). Yet this Act penalizes disseminating large volumes of *protected* speech based on negligence.

124. Restrictions on speech "because of its message, its ideas, its subject matter, or its content," *Brown*, 564 U.S. at 790-91, are "presumptively unconstitutional" and may be justified only if the government satisfies strict scrutiny. *Reed*, 576 U.S. at 163. Strict scrutiny requires a State to use "the least restrictive means of achieving a compelling state interest." *Ams. for Prosperity Found. v. Bonta*, 594 U.S. 595, 607 (2021) (quoting *McCullen v. Coakley*, 573 U.S. 464, 478 (2014)).

125. The Act fails each element of this test.

126. *First*, although protecting minors is a compelling interest, "restrict[ing] the ideas to which children may be exposed" is not. *Brown*, 564 U.S. at 794. The State may not "deprive the public of the right and privilege to determine for itself what speech and speakers are worthy of consideration." *Citizens United*, 558 U.S. at 341; *Moody*, 603 U.S. at 742 (government cannot "change the speech of private actors in order to achieve its own conception of speech nirvana"). Moreover, the State has not shown, and cannot show, that a free internet (in general) or data processing (in particular) harms minors. *See Brown*, 564 U.S. at 799 ("The State must specifically identify an 'actual problem' in need of solving" and the curtailment of free speech must be "actually necessary to the solution." (citation omitted).

127. *Second*, the Act is not narrowly tailored. The Act is overbroad because it encompasses an enormous amount of speech that does not harm minors and restricts speech even to older minors nearing adulthood. And the Act is underinclusive because it leaves unregulated numerous actors and activities, such as financial institutions, not-for-profit entities, and medical providers subject to HIPAA, as well as numerous harm-causing activities in the physical world. Such lack of fit "raises serious doubts about whether the government is in fact pursuing the interest it invokes, rather than disfavoring a particular speaker or viewpoint." *Id.* at 802.

128. *Third*, the State did not even attempt to use the least restrictive means. "The State could have easily employed less restrictive means to accomplish its protective goals, such as by (1) incentivizing companies to offer voluntary content filters or application blockers, (2) educating children and parents on the importance of using such tools, and (3) relying on existing criminal laws that prohibit related unlawful conduct." *Bonta,* 113 F.4th at 1121.

129. The "best interests of children" standard fails any form of heightened First Amendment scrutiny and renders unconstitutional both the Act as a whole and each subpart that relies on the standard. This First Amendment claim raises both (1) a First Amendment facial challenge as to both the Act as a whole and each relevant subpart, i.e., because "a substantial number of law's applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep," *Moody*, 603 U.S. at 723; and (2) an as-applied First Amendment claim.

130. As to the facial claim, the entire Act fails First Amendment scrutiny because it is centered around a "best interests of children" standard that will require covered websites to restrict huge amounts of protected speech to minors and adults alike. Those applications are at least "substantial" relevant to (any) plain legitimate sweep. Alternatively, the "best interests" standard is unconstitutional as applied to NetChoice members' content creation, curation, dissemination, and other protected speech activities. And so relief is warranted, at a minimum, as to those activities by NetChoice members.

131. The Act's "best interests of children" standard is integral to each of the Act's operative speech regulations. It cannot be severed. Without this central definition, no other provision in the Act could operate. Thus, all of the Act's speech regulations are invalid.

132. Unless declared invalid and enjoined, the Act's speech restrictions will deprive Plaintiff's members and Internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

**COUNT II**
**42 U.S.C. § 1983**
**VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT**
**("REASONABLY LIKELY TO BE ACCESSED BY CHILDREN" STANDARD)**

133. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

134. The Act's "reasonably likely to be accessed by children" standard—defining which websites are regulated and which avoid regulation—is also a content-based restriction on speech that violates the First Amendment.

135. This standard defines the universe of regulated entities by whether an online service or feature: is "directed to children"; is "routinely accessed" by children; has content "substantially similar to" another entity routinely accessed by children; features "advertisements marketed to children"; has an "audience" composed of children; or knows or "should" know a user is a child. § 14-4801(s).

136. This central coverage definition is content-based on at least two grounds.

137. First, it expressly requires the consideration of a website's content, such as "advertisements marketed to children" and content "substantially similar to" another service or feature routinely accessed by children.

138. Second, the remaining criteria define the regulated universe by reference to the anticipated "audience" and "user" of the speech, e.g., § 14-4801(s)(5), thereby focusing on the "impact that speech has on its listeners." *Playboy Ent. Grp., Inc.*, 529 U.S. 803, 813 (2000). Where "[t]he overriding justification for the regulation is concern for the effect of the subject matter on young viewers," the law "is not justified without reference to the content of the regulated speech."

*Id.*; *see also Sorrell*, 564 U.S. at 577 (regulation to counteract an "influence" on specific "listeners" is "incompatible with the First Amendment"). That is why the Northern District of California concluded that a similar "likely to be accessed by children" standard was content based: "Application of these criteria to determine whether a particular business's online offerings are likely to be accessed by children unavoidably requires an evaluation of content." *Bonta*, 2025 WL 807961, at *9. The "reasonably likely to be accessed by children" standard is therefore subject to strict scrutiny, *see id.*, and it fails strict scrutiny for the same reasons set forth above.

139. Because this coverage definition is inherently content based, it is unconstitutional in all applications and facially invalid on that ground. In the alternative, it is content-based and governs an enormous number of speech-related (and unconstitutional) applications. These applications are substantial relative to any constitutional applications. The standard is therefore overbroad. And because it defines the coverage of the entire Act, its invalidity infects and renders the entire Act facially unconstitutional.

140. The Act's central "reasonably likely to be accessed by children" standard is integral to each of the Act's operative speech regulations. It cannot be severed. Without this central definition, no other provision in the Act could operate. Thus, all of the Act's speech regulations are invalid.

141. Unless declared invalid and enjoined, the Act's speech restrictions will deprive Plaintiff's members and Internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

**COUNT III**
**42 U.S.C. § 1983**
**VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH AMENDMENTS**
**("BEST INTERESTS OF CHILDREN" STANDARD)**

142. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

143. The Act's central command that covered entities design their services and operate in the "best interests of children," § 14-4801(c), also is unconstitutionally vague on its face and violates bedrock principles of free speech and due process. This standardless directive fails to provide fair notice of what speech is restricted, grants enforcement officials unbounded discretion, and will inevitably chill vast amounts of protected expression.

144. "A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox TV Stations, Inc.*, 567 U.S. 239, 253 (2012). And a law is unconstitutionally vague if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *United States v. Williams*, 553 U.S. 285, 304 (2008). The constitutional standard for vagueness is heightened for speech regulations under the First Amendment. *Fox*, 567 U.S. at 253-54. "When a statute 'is capable of reaching expression sheltered by the First Amendment, the [vagueness] doctrine demands a greater degree of specificity than in other contexts.'" *Ctr. for Individual Freedom, Inc. v. Tennant*, 706 F.3d 270, 280 (4th Cir. 2013) (alteration in original) (quoting *Smith v. Goguen*, 415 U.S. 566, 573 (1974)).

145. These vagueness concerns are heightened here, where the Maryland Attorney General Division of Consumer Protection can bring administrative actions to enforce the Act—thus depriving covered entities of a meaningful judicial check on Defendants' interpretation of the Act.

146. In addition to being impermissibly content-based, the Act's "best interests of children," § 14-4801(c), standard fails to provide regulated entities with sufficient notice about the wide range of potential harms that they must account for in (1) their Data Protection Impact Assessments; (2) how they design their "websites" and *every* feature on them, § 14-4801(m)(1); and (3) their use of minors' information.

147. This kind of vague and subjective standard grants Defendants too much discretion. Service to service, day to day, and administration to administration, covered entities obligations may shift—depriving covered entities of necessary notice of what the Act demands.

148. That is especially true in online services, where evidence of purported harms is mixed and must compete with countervailing evidence of benefits. *E.g.*, *Reyes*, 2024 WL 4135626, at *12 (noting Surgeon General's Advisory's "nuanced view" of social media).

149. Such concerns about protected speech have been prevalent throughout American history. *See Brown*, 564 U.S. at 797; U.S. Surgeon General, Television and Growing Up: The Impact of Televised Violence (1972), https://perma.cc/QP4H-73V4.

150. To begin, the Act requires covered entities to make numerous subjective and indeterminate considerations about how the enormous and diverse range of content on their services could affect all minors—regardless of age, socioeconomic status, preferred language, sensitivities, and many other relevant factors.

151. Take just age: The Supreme Court has emphasized the importance of "tak[ing] into account juveniles' differing ages and levels of maturity." *Am. Booksellers*, 484 U.S. at 396.

152. Yet the Act flattens all minors into a mass of "children," and requires covered entities to evaluate what might cause "children" harm.

153. This will encourage covered entities to assess the risks that might befall the most sensitive and youngest users, defaulting to the most restrictive possible understandings of the Act.

154. Under the Act, a covered entity might have to change its services if a single child might suffer any of the Act's broad and ill-defined harms. And the Act's vagueness grants Defendants near-complete discretion to assess what the harms are in the first place.

155. The Act's definition of "best interests of children" multiplies the sheer number of indeterminate analyses covered entities must engage in and heightens the confusion about what those analyses will require.

156. It is telling that the Act uses the phrase "best interests of children." § 14-4801(c); *see, e.g.*, *Bond v. United States*, 572 U.S. 844, 861 (2014) (considering "the ordinary meaning of a defined term" to determine the "fair reading" of the statute).

157. This is a standard applied in the family-law context, and is designed to grant family-law judges "*near-boundless discretion* . . . to determine what is in the child's best interests." *In re Adoption/Guardianship of H.W.*, 460 Md. 201, 218 (2018) (emphasis added).

158. Although that boundless discretion may be appropriate in the family-law context, it is not appropriate in regulations of speech.

159. It is especially inappropriate as the standard by which to evaluate the way that web-sites—and all the features on them—are designed and operate.

160. Each individual prong of the statutory definition is unconstitutionally vague.

161. *First*, it is unclear what it means for a website's use of information to "[b]enefit the covered entity to the detriment of children." § 14-4801(c)(1).

162. Neither "benefit" nor "detriment" is defined.

163. And what a covered entity might consider a "benefit," Defendants could consider a "detriment." For example, although NetChoice members and their users consider personalized content a "benefit," Defendants could disagree.

164. And it is unclear whether the "benefit" and "detriment" must be related, or whether covered entities must weigh completely unrelated benefits and detriments against each other.

165. Even assuming that covered entities could determine how to consistently define "benefits" and "detriments," the Act does not explain about how covered entities are meant to (1) weigh the two against each other; and (2) account for the *benefits* that minors experience.

166. As the Supreme Court has observed, tests that require comparison between "incommensurable" "competing goods" provide insufficient standards for comparison. *Nat'l Pork Producers Council v. Ross*, 598 U.S. 356, 382 (2023).

167. It is unclear how anyone is "supposed to compare or weigh economic costs (to some) against noneconomic benefits (to others)[.] No neutral legal rule guides the way." *Id.* at 381.

168. To "weigh benefits and burdens, it is axiomatic that both must be judicially cognizable and comparable." *Id.* at 393 (Barrett, J., concurring in part).

169. Here, by contrast, the Act may require evaluations into "whether a particular line is longer than a particular rock is heavy." *Bendix Autolite Corp. v. Midwesco Ents., Inc.*, 486 U.S. 888, 897 (1988) (Scalia, J., concurring in judgment).

170. *Second*, the Act does not define how covered entities should evaluate whether the use of information will "[r]esult in . . . [r]easonably foreseeable and material physical or financial harm." § 14-4801(c)(2)(i).

171. The necessary link between a website's design and/or its use of information and physical harm is unclear. Digital processing and design are intangible activities that do not cause harm standing alone. Websites will therefore be forced to hypothesize about the ways such processing and design could give rise to different types of expressive activities, and in turn, how such expression could give rise to behavior that subsequently might harm a minor. Such a chain of speculation is too subjective and indeterminate to establish a fair basis to impose liability, particularly where protected expression is at stake.

172. *Third*, it is particularly unclear how covered entities are expected to evaluate whether the use of information will "[r]esult in . . . [s]evere and reasonably foreseeable psychological or emotional harm." § 14-4801(c)(2)(ii).

173. The possibility of subjective emotional reaction is inherent in any form of communication—whether email, books, music, film, or television.

174. That is why courts have rejected liability for disseminating speech based on reactions not already subsumed within well-defined First Amendment exceptions (such as defamation and fighting words). *See, e.g.*, *Herceg v. Hustler Mag., Inc.*, 814 F.2d 1017 (5th Cir. 1987); *McCollum v. CBS, Inc.*, 202 Cal. App. 3d 989 (1988).

175. *Fourth*, it is also unclear whether information use will "[r]esult in . . . [a] highly offensive intrusion on children's reasonable expectation of privacy." § 14-4801(c)(2)(iii).

176. Neither "highly offensive" nor "reasonable expectation of privacy" are defined.

177. Nor are there any useful guideposts for how to evaluate these concepts online.

178. And, as explained above, the "reasonable expectation[s]," *id.*, of minors of different ages may well be different, *see Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 865-66 (1997).

179. *Fifth*, it is unclear how to evaluate whether and when the use of information will "[r]esult in . . . [d]iscrimination against children based on race, color, religion, national origin, disability, gender identity, sex, or sexual orientation." § 14-4801(c)(2)(iv).

180. Of course, Maryland already prohibits discrimination through its separate, generally applicable antidiscrimination law and other laws. *E.g.*, Md. Code, State Gov't § 20-304.

181. Yet the Act adds to those existing requirements with an additional vague command, seemingly untethered to—or at least distinct from—those existing and reliable standards.

182. The Act "effectively grants [the State] the discretion to [assign liability] selectively on the basis of the content of the speech." *City of Houston v. Hill*, 482 U.S. 451, 465 n.15 (1987).

183. The Act's use of a "reasonabl[e] foreseeab[ility]" standard does not do enough to mitigate the uncertainty. § 14-4801(c)(2).

184. Indeed, the Supreme Court has held that the First Amendment requires more than a mere negligence or reasonableness level of culpability to punish speech disseminators. *Counterman*, 600 U.S. at 79 & n.5.

185. Furthermore, "the relevant provisions are worded at such a high level of generality that they provide little help to businesses in identifying which of those practices or designs may actually harm children." *Bonta*, 113 F.4th at 1122. Maryland "cannot give the Judiciary uncut marble with instructions to chip away all that does not resemble David" while leaving Marylanders "to bear constitutional deprivation in the meantime." *Griffin*, 2025 WL 978607, at *17 (quoting *Percoco v. United States*, 598 U.S. 319, 337 (2023) (Gorsuch, J., concurring in the judgment)).

186. All of these vagueness problems are exacerbated by the Act's breadth.

187. For example, the Act defines "process[ing]" user information to mean "collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data." § 14-4801(p).

188. Thus, a website must analyze whether both its use and non-use ("deleting") of information complies with the "best interests of children" standard.

189. So if a website uses information to present age-appropriate content to a minor, it risks liability. And if a website "deletes" information from a minor and thus does not use it to present age-appropriate content to a minor, it also risks liability.

190. This "heads you lose, tails we win" approach cannot comply with due process: It "authorizes or encourages seriously discriminatory enforcement." *Williams*, 553 U.S. at 304.

191. The Act's vague "best interests of children" standard is integral to each of the Act's operative speech regulations. It cannot be severed. Without this central definition, no other provision in the Act could operate. Thus, all of the Act's speech regulations are invalid.

192. Unless declared invalid and enjoined, the Act's speech restrictions will deprive Plaintiff's members and Internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

**COUNT IV**
**42 U.S.C. § 1983**
**VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH AMENDMENTS**
**("REASONABLY LIKELY TO BE ACCESSED BY CHILDREN" STANDARD)**

193. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

194. The Act's central coverage formula applying the Act to services "[r]easonably likely to be accessed by children," § 14-4801(s), is unconstitutionally vague on its face and violates bedrock principles of free speech and due process.

195. The Act's standards for whether a service is "[r]easonably likely to be accessed by children," *id.*, is suffused with subjective and indeterminate considerations that fail to provide entities with sufficient guidance about whether they have compliance obligations under the Act.

196. Even the Act's attempts at posing objective questions are indeterminate.

197. It is unclear what it means to "be *routinely* accessed by a *significant number* of children." § 14-4801(s)(2) (emphases added).

198. Neither of the emphasized terms are defined.

199. "Significant number" could refer to the total number of minors, or the percentage of minors relative to all users, or something else. Many websites will just not know.

200. For example, the Vermont Legislature passed a similar law (vetoed by the governor) that defined "significant number of children" as "composed of at least *two percent of minor consumers* two through under 18 years of age." Vt. S.289, § 1 (2024) (emphasis added).

201. And even if a website believes it does not meet this criterion, it has to compare itself to nearly every other website online to determine whether it "is *substantially similar or the same as* an online product that satisfies item (2) of this subsection." § 14-4801(s)(3).

202. In other words, even if a website has *zero* minor users, if it is "substantially similar" to an online service or feature that *does* have a "significant number" of minors, it must comply with this Act. And it must do so even if it *does not know* the other (substantially similar) feature meets the "significant number of children" standard.

203. In addition, whether a "covered entity . . . should have known that a user is a child," § 14-4801(s)(6), is too indeterminate. This consideration inherently will require retrospective evaluation that could penalize websites any time they have *even a single minor* access the service if they had information somewhere indicating the minor's status. This expansive catch-all effectively negates the "routine" and "significant" qualifiers elsewhere in the definition.

204. Moreover, the Act brackets websites with dueling mandates. On one hand, they "may not collect or process any personal data beyond what is reasonably necessary." § 14-4806(c). So websites are vaguely constrained in the information they can collect to determine whether users are minors. If Defendants disagree that collecting certain information was "necessary," covered entities face liability. On the other hand, if covered entities do not collect information, they risk Defendants concluding they "should have known" their users include minors. § 14-4801(s)(6).

205. The Act's vague "reasonably likely to be accessed by children" standard is integral to the Act. It cannot be severed because it defines which services must comply with the Act. Without this definition, no other provision in the Act could operate. Thus, the entire Act is invalid.

206. Unless declared invalid and enjoined, the Act will deprive Plaintiff's members and Internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

**COUNT V**
**42 U.S.C. § 1983**
**VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT**
**(DATA PROTECTION IMPACT ASSESSMENT – § 14-4804)**
**(FACIAL AND AS-APPLIED CHALLENGE)**

207. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

208. As incorporated against the States by the Fourteenth Amendment, the First Amendment's Free Speech and Free Press Clauses provide that governments "shall make no Law . . . abridging the Freedom of Speech, or of the Press." U.S. Const. amend. I. The First Amendment protects "publish[ing]," *Reno*, 521 U.S. at 852-53; "disseminat[ing]," *303 Creative LLC v. Elenis*, 600 U.S. 570, 594 (2023); and "creating, distributing, [and] consuming" protected speech. *Brown*, 564 U.S. at 792 n.1.

209. The Act's Data Protection Impact Assessment requirements, § 14-4804, violate the First Amendment both facially and as applied to NetChoice's covered members, to the extent they compel speech and interfere with protected editorial discretion.

210. These requirements are also unconstitutional as applied to NetChoice's members when those members curate and disseminate compilations of protected speech on their services.

211. The First Amendment prohibits governments from compelling speech from private entities, such as the covered entities here.

212. "It is well-established that the First Amendment protects 'the right to refrain from speaking at all.'" *Bonta*, 113 F.4th at 1117 (quoting *Wooley v. Maynard*, 430 U.S. 705, 714 (1977)).

213. That is true even when the government does not compel *public* speech. "[T]he Supreme Court has recognized the First Amendment may apply even when the compelled speech need only be disclosed to the government." *Id.* at 1117-18.

214. A law "mandating speech that a speaker would not otherwise make" is 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.C., Inc.*, 487 U.S. 781, 795 (1988).

215. The Act compels speech that covered entities would not otherwise make and thus necessarily operates as content-based regulation because it alters the content of speech.

216. And the First Amendment prohibits interference with editorial discretion, such as by requiring websites to restrict access to protected speech. *Moody*, 603 U.S. at 734-35, 739-40; *see CCIA*, 2024 WL 4051786, at *19 (enjoining requirement to block content-based categories of speech).

217. The Ninth Circuit held that California's substantively similar compelled-speech and censorship requirements violate the First Amendment. *Bonta*, 113 F.4th at 1116-17.

218. California, too, required covered entities to "create DPIA reports identifying, for each offered online service, product, or feature likely to be accessed by children, any risk of 'material detriment to children that arise from the data management practices of the business.'" *Id.* at 1116 (quoting Cal. Civ. Code § 1798.99.31(a)(1)(A), (B)).

219. Many of the specific disclosures in the two States' laws are substantively identical:

(1) harmful contacts, *compare* § 14-4804(b)(3)(i) ("Whether the data management or processing practices of the online product could lead to children experiencing or being targeted by contacts . . ."), *with* Cal. Civ. Code § 1798.99.31(a)(1)(B)(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.");

(2) harmful conduct, *compare* § 14-4804(b)(3)(ii) ("Whether the data management or processing practices of the online product could permit children to participate in or be subject to conduct . . ."), *with* Cal. Civ. Code § 1798.99.31(a)(1)(B)(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.");

(3) exploitation, *compare* § 14-4804(b)(3)(iii) ("Whether the data management or processing practices of the online product are reasonably expected to allow children becoming party to or exploited by a contract through the online product . . ."), *with* Cal. Civ. Code § 1798.99.31(a)(1)(B)(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.");

(4) algorithms, *compare* § 14-4804(b)(3)(vii) ("Whether algorithms used by the online product . . ."), *with* Cal. Civ. Code § 1798.99.31(a)(1)(B)(v) ("Whether algorithms used by the online product, service, or feature could harm children.");

(5) features, *compare* § 14-4804(b)(3)(iv) ("Whether the online product uses system design features to increase, sustain, or extend the use of the online product, including the automatic playing of media, rewards for time spent, and notifications . . ."), *with* Cal. Civ. Code § 1798.99.31(a)(1)(B)(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."); and

(5) risks to minors, *compare* § 14-4804(b)(3)(v) ("Whether, how, and for what purpose the online product collects or processes personal data of children and whether those practices would result in: [specified harms]."), *with* Cal. Civ. Code § 1798.99.31(a)(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 [the law].").

220. Accordingly, just like California's unconstitutional requirement, the Act here violates the First Amendment for at least two reasons.

221. "First, the DPIA report requirement clearly compels speech by requiring covered businesses to opine on potential harm to children." *Bonta*, 113 F.4th at 1117; *see also X Corp. v. Bonta,* 116 F.4th 888, 901 (9th Cir. 2024) (requirement that companies "recast [their] content-moderation practices in language prescribed by the State, implicitly opining on whether and how certain controversial categories of content should be moderated" violated First Amendment).

Maryland's Assessment requirements compel speech and require covered entities to opine an all manner of potential harm to minors.

222. Furthermore, it "requir[es] a company to publicly condemn itself," which is "more constitutionally offensive." *Nat'l Ass'n of Mfrs. v. SEC*, 800 F.3d 518, 530 (D.C. Cir. 2015).

223. "Second, the DPIA report requirement invites First Amendment scrutiny because it deputizes covered businesses into serving as censors for the State." *Bonta*, 113 F.4th at 1118.

224. 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. FCC*, 518 U.S. 727, 754 (1996). Any government regulation imposing "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).

225. Here, the Act requires covered entities to "[i]nclude a description of steps that the covered entity has taken and will take to comply with the duty to act in a manner consistent with the best interests of children." § 14-4804(b)(4).

226. In other words, even these purported disclosure requirements compel covered entities to remove content from their services.

227. That is true even if the Act purports to not require speech removal. *E.g.*, § 14-4810.

228. To the extent these provisions would require websites to age-gate or otherwise restrict users' access to certain content, it would impede users' access to protected speech.

229. California, too, attempted to argue that California's law "solely requires a company to mitigate risks from its *data management practices*." *Bonta*, 113 F.4th at 1118.

230. *Bonta* concluded that the California law "unquestionably requires a covered business to mitigate" risks, which "construct[s] a censorship scheme." *Id.* A "business cannot assess

the likelihood that a child will be exposed to harmful or potentially harmful materials on its platform without first determining what constitutes harmful or potentially harmful material." *Id.*

231. *Heightened First Amendment scrutiny.* The Act's Assessment requirements trigger and fail strict scrutiny—not any other lower form of First Amendment scrutiny that might apply.

232. These requirements trigger strict scrutiny two times over by (1) compelling speech (2) about content-based categories of topics.

233. They fail strict scrutiny because Defendants cannot show they "further[] a compelling interest and [are] narrowly tailored to achieve that interest." *Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (cleaned up).

234. "Speech . . . 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).

235. Again, the "State could have easily employed less restrictive means to accomplish its protective goals, such as by (1) incentivizing companies to offer voluntary content filters or application blockers, (2) educating children and parents on the importance of using such tools, and (3) relying on existing criminal laws that prohibit related unlawful conduct." *Bonta*, 113 F.4th at 1121.

236. Moreover, Maryland enacted a parallel data privacy regulation that amply serves any data-privacy interest Defendant may assert. *See* Md. Sen. Bill 541 (2024).

237. "The DPIA report requirement—in requiring covered businesses to opine on and mitigate the risk that children are exposed to harmful content online—regulates far more than mere commercial speech." *Id.* at 1119.

238. Accordingly, the standard of scrutiny articulated in *Zauderer v. Off. of Disciplinary Couns. of Sup. Ct. of Ohio*, 471 U.S. 626 (1985), does not apply here.

239. *Zauderer* is limited to efforts to "combat the problem of inherently misleading commercial advertisements" by mandating "only an accurate statement." *Milavetz, Gallop & Milavetz, P.A. v. United States*, 559 U.S. 229, 250 (2010).

240. The Act's compelled-speech Assessments have nothing to do with "commercial speech." *Zauderer*, 471 U.S. at 651.

241. The Assessments are not regulating "misleading" commercial speech. *Id.* 644.

242. The Assessments do not mandate disclosure of "purely factual and uncontroversial information about the terms under which . . . services will be available." *Nat'l Inst. of Fam. & Life Advocs. v. Becerra*, 585 U.S. 755, 768 (2018); *see Zauderer*, 471 U.S. at 651.

243. The Act's compelled-speech Assessments instead require websites to opine on potential harms to minors.

244. *Facially invalid.* The compelled-speech Assessment requirement is facially invalid because "the DPIA report requirement, in every application to a covered business, raises the same First Amendment issues." *Bonta*, 113 F.4th at 1116.

245. Consequently, "a substantial number of [the Act's] applications are unconstitutional." *Moody*, 603 U.S. at 723 (citation omitted).

246. "Whether it be NetChoice's members or other covered businesses providing online services likely to be accessed by children, all of them are under the same statutory obligation to opine on and mitigate the risk that children may be exposed to harmful or potentially harmful content, contact, or conduct online." *Bonta*, 113 F.4th at 1116.

247. So the First Amendment facial challenge here is straightforward "from the face of the law" because all aspects of the Act's speech-restricting provisions, "in every application . . . , raise the same First Amendment issues," so the Court "need not 'speculate about "hypothetical" or "imaginary" cases.'" *X Corp.*, 116 F.4th at 899 (citation omitted); *accord Reyes*, 2024 WL 4135626, at *9 n.92.

248. "While it is certainly possible that in some applications, a covered business will ultimately conclude that it need not address certain risks in its DPIA report because its new service to be offered does not create such risks, there is no question that a covered business at the threshold would still have to inquire into whether the risk exists before it can decline to address it in its DPIA report." *Bonta*, 113 F.4th at 1116 (cleaned up).

249. Because the Act compels speech from all covered entities and that compelled-speech requirement fails strict scrutiny, the Assessment requirements are facially invalid.

250. *Invalid as applied to NetChoice members*. At a minimum, the Assessment requirements are unconstitutional as applied to NetChoice members.

251. Unless declared invalid and enjoined, the Act's Data Protection Impact Assessment requirements will deprive Plaintiff's members and Internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

**COUNT VI**
**42 U.S.C. § 1983**
**VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT**
**(RESTRICTIONS ON DATA, "DARK PATTERNS," AND "MONITORING – § 14-4806)**
**(FACIAL AND AS-APPLIED CHALLENGE)**

252. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

253. Several of the Act's specific restrictions on data and website design also violate the First Amendment both facially and as applied to NetChoice members. These provisions limit

online services' rights to collect and use information for the purposes of protected expressive activity—e.g., creating, curating, recommending, and delivering speech to users. They also unlawfully restrict websites' ability to facilitate protected speech between users and design user interfaces in an engaging and useful way.

254. Speech on the Internet requires "collecting, using, storing, disclosing, analyzing, deleting, and modifying personal data." § 14-4801(p)(2) (definition of "process"). And substantial amounts of online speech also require "automated processing of . . . personal data to evaluate, analyze, or predict certain aspects relating to an individual." § 14-4801(q).

255. For example, when online services—including NetChoice members—process data to curate and disseminate compilations of protected speech on their services, they are protected by the First Amendment. That includes when they use "algorithms" (i.e., "profiling") to implement editorial policies, even if based in part on "user's expressed interests." *Moody*, 603 U.S. at 734-35. Accordingly, the curated feeds of services such as "Facebook" and "YouTube" are protected, *id.* at 734-35, 739-40, as are large volumes of other online speech that depend on data, personalization, and other forms of automated processing.

256. The Act unconstitutionally limits these activities in vague and content-based ways.

257. Specifically, it prohibits "process[ing] the personal data of a child in a way that is inconsistent with the best interests of children reasonably likely to access" the website, § 14-4806(a)(1); "process[ing] personal data of a child that is not reasonably necessary to provide an online [service or feature] that the child is actively and knowingly engaged with," § 14-4806(a)(3); and "profil[ing] a child by default" unless "necessary" and absent "appropriate safeguards . . . to ensure that profiling is consistent with the best interests of children," § 14-4806(a)(2).

258. In other words, websites cannot (i) receive, use, store, analyze, modify, or delete minors' data ("process") to deliver content to minor users, or (ii) conduct "any form of automated processing" of data to understand their audience or personalize content ("profile") *unless* they serve content in minors' "best interests" *and* satisfy the vague "necess[ity]" mandate.

259. In addition, the Act imposes internally inconsistent requirements. For example, the Act defines "process[ing]" to mean "collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data." § 14-4801(p). Thus, a website risks liability both when it uses and declines to use ("deleting") information.

260. These restrictions are unconstitutional prior restraints, burdening both websites' rights to create and disseminate speech and also users' right to receive that speech. The State cannot prohibit websites from using information they "already possess[]" or "'the way in which the information might be used'" to advance the State's preferred message. *Sorrell*, 564 U.S. at 568 (citation omitted).

261. As Defendants have said: "to the extent the Maryland Act's prohibitions impact a covered entity's collection, use, creation, or disclosure of information or burden only certain types of information or speech, . . . a court may consider the provisions to regulate protected speech." Ex. B at 4 (citing *Sorrell*, 564 U.S. at 570). The Act regulates protected speech in precisely this way.

262. Similarly, the Act's vague restriction on "allow[ing]" other users to "monitor [a] child's online activity," § 14-4806(a)(9), appears to require websites to block a variety of commonplace and protected speech activities, such as "friending" and "following" other users, even other minors, friends, colleagues, and family members. This imposes "serious burdens" on speech, *McCullen v. Coakley*, 573 U.S. 464, 487 2014), and triggers First Amendment scrutiny.

263. Finally, the Act's restrictions on so-called "dark patterns" (i.e., persuasive "user interfaces"), § 14-4806(a)(7), likewise violate the First Amendment and are vague. Although the term "dark patterns" is calculated to sound nefarious, its amorphous definition 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.[2] *See* § 14-4801(i) ("dark pattern" defined as a "user interface" designed "with the purpose of subverting or impairing user autonomy, decision making, or choice"). Speech cannot be suppressed or burdened because the State finds it "too persuasive." *Sorrell*, 564 U.S. at 578.

264. The Act's regulation of dark patterns also requires content-based distinctions for speech in minors' "best interests," § 14-4806(7)(iii), compounding the constitutional problem. And the uncertainty inherent in the "dark patterns" prohibitions will cause them 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 popular videos, and an independent blogger pushing out new-post alerts to followers.

265. Finally, all of the foregoing restrictions, § 14-4806(a)(1)-(3), (7), & (9), effectively require websites to either know when their users *are* minors or else limit expressive activities for

[2] *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.

*all* users. Such mandatory age-gating of protected speech is "unprecedented and mistaken." *Brown*, 564 U.S. at 794.

266. Each of these provisions trigger and fail any form of heightened scrutiny for the reasons discussed above.

267. Unless declared invalid and enjoined, these restrictions will deprive Plaintiff's members and Internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and Internet users.

**COUNT VII**
**42 U.S.C. § 1983, 15 U.S.C. §§ 6501, AND**
***EX PARTE YOUNG* EQUITABLE CAUSE OF ACTION**
**PREEMPTION UNDER THE SUPREMACY CLAUSE OF THE CONSTITUTION**

268. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

269. The Act is preempted by the federal Children's Online Privacy Protection Act ("COPPA"). 15 U.S.C. §§ 6501, *et. seq.*

270. COPPA reflects Congress's comprehensive judgments about online data collection and use from minor uses that preempts the contrary decisions made by Maryland through the Act.

271. COPPA expressly preempts any state laws that are "inconsistent" with federal law's "treatment" of data-collection "activities" and "actions" regarding minors. 15 U.S.C. § 6502(d).

272. In general, that "treatment" is notice and parental consent for data collection from children younger than 13 from those websites "directed" to such minors. *Id.* § 6502(a)(1).

273. COPPA's requirements are intended to create a uniform, national standard.

274. The Act is expressly preempted by COPPA in at least three ways.

275. *First*, the Act's treatment of minors younger than 13 is "inconsistent" with COPPA's "treatment" of those minors. *Id.* § 6502(d).

276. COPPA only requires compliance when an "online service that has actual knowledge that it is collecting personal information from a child." *Id.* § 6502(b)(1)(A).

277. The Act here, by contrast, regulates data collection from minors younger than 13 when it is "[r]easonably likely to be accessed by children." § 14-4801(s); *e.g.*, *New Mexico ex rel. Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1120-21 (D.N.M. 2020), *on reconsideration*, 516 F. Supp. 3d 1293 (D.N.M. 2021).

278. In other words, the Act's mens rea requirement is inconsistent with COPPA's.

279. *Second*, the Act's enforcement regime for minors younger than 13 is preempted.

280. Congress established that COPPA's regulations are enforced only by the Federal Trade Commission or state attorneys general *after* notice to the FTC. 15 U.S.C. §§ 6502(c), 6504.

281. But the Act imposes a parallel enforcement regime for such minors, reaching different services, enforceable outside of COPPA's enforcement scheme, and providing different penalties. *E.g.*, *H.K. through Farwell v. Google LLC*, 595 F. Supp. 3d 702, 711 (C.D. Ill. 2022).

282. *Third*, Maryland's regulation of teenagers (minors 13-17) is "inconsistent" with Congress's preemptive determination to (1) regulate only *certain* online services' interactions with minors younger than 13; and (2) to otherwise permit data collection and usage.

283. For these reasons and more, the Act is also impliedly preempted because it frustrates and undermines COPPA's basic purposes and policy goals.

284. The Act interferes with Congress's clear command and intent to establish a uniform, national policy for certain data-privacy practices for minors. With yet another State attempting to enter the fray, online services must increasingly: (1) determine whether they satisfy different coverage formulas; (2) attempt to satisfy different operative requirements; and (3) ensure that their compliance obligations in one State do not violate their obligations in any other State.

285. Unless declared preempted, the Act will cause Plaintiff, its members, and Internet users irreparable harm.

**COUNT VIII**
**42 U.S.C. § 1983, 47 U.S.C § 230, AND**
***EX PARTE YOUNG* EQUITABLE CAUSE OF ACTION**
**PREEMPTION UNDER THE SUPREMACY CLAUSE OF THE CONSTITUTION,**
**(§§ 14-4804, 14-4806)**

286. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

287. 47 U.S.C. § 230 ("Section 230") preempts the Act's Data Protection Impact Assessment requirement, § 14-4804, and the processing and profiling restrictions, § 14-4806, to the extent that they apply to the dissemination of third-party speech.

288. In Section 230, Congress protected websites' "exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content" generated by third parties. *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

289. Section 230(c)(1) provides: "[n]o 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." That includes penalizing actions to "(A) filter, screen, allow, or disallow . . . ; (B) pick, choose, analyze, or digest . . . ; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content" created by third parties. 47 U.S.C. § 230(f)(2).

290. Congress preempted "inconsistent" state law, providing no "cause of action may be brought and no liability may be imposed." *Id.* § 230(e)(3).

291. In other words, Section 230 preempts any cause of action or liability based on a website's exercise of editorial functions over third-party content—including decisions about whether and how to disseminate and display that content.

292. Multiple NetChoice members operate "interactive computer services," that disseminate "information provided by another information content provider." *Id.* § 230(c)(1), (f)(2),

293. The Act would penalize websites for their exercise of traditional editorial functions.

294. Accordingly, the Act is preempted to the extent that it regulates NetChoice's members' exercise of traditional editorial functions over user-created content.

295. Unless declared preempted, the Act's regulation of online services will cause Plaintiff, its members, and Internet users irreparable harm.

## PRAYER FOR RELIEF

Plaintiff requests an order and judgment:

a. declaring that the Maryland Age-Appropriate Design Code Act is unlawful;
b. declaring that the Maryland Age-Appropriate Design Code Act violates the First Amendment to the Constitution, both facially and as applied to NetChoice members' content creation, curation, dissemination, and other protected speech activities;
c. declaring that Sections 14-4801(c), 14-4803(2)-(4), 14-4804, 14-4805, 14-4806(a)(1)-(3), (7), (9), and 14-4807 violate the First Amendment to the Constitution, as incorporated by the Fourteenth Amendment, both facially and to the extent they compel speech, interfere with protected editorial discretion, and restrict the collection and use of information for the purposes of curating, recommending, and delivering protected speech to users;
d. declaring that the Maryland Age-Appropriate Design Code Act is void for vagueness under the First Amendment and the Due Process Clause of the Fourteenth Amendment to the Constitution;
e. enjoining Defendants and their agents, employees, and all persons acting under their direction or control from taking any action to enforce the challenged portions of the Act, at a minimum, against Plaintiff or its members;
f. declaring that the Maryland Age-Appropriate Design Code Act is preempted by the Children's Online Privacy Protection Act;
g. declaring that the Sections 14-4803(2)-(4), 14-4804, 14-4806 are preempted by 47 U.S.C. § 230, to the extent that they apply to the dissemination of third-party speech;
h. declaring that the unlawful portions of the Maryland Age-Appropriate Design Code Act are not severable from the rest of the Act;
i. entering judgment in favor of Plaintiff;
j. awarding Plaintiff its attorneys' fees and costs incurred in bringing this action, including attorneys' fees and costs under 42 U.S.C. § 1988(b) for successful 42 U.S.C. § 1983 claims against state officials; and
k. awarding Plaintiff all other such relief as the Court deems proper and just.

Dated: April 25, 2025

Respectfully submitted,

*/s/ Andrew C. White*
Andrew C. White (Bar No. 08821)
awhite@silvermanthompson.com
Ilona Shparaga (Bar No. 21494)
ishparaga@silvermanthompson.com
SILVERMAN THOMPSON SLUTKIN & WHITE, LLC
400 E Pratt Street, Suite 900
Baltimore, MD 21202
(410) 385-2225 (t)
(410) 547-2432 (f)

*/s/ Steven P. Lehotsky*
Steven P. Lehotsky*
Scott A. Keller*
Serena M. Orloff**
Jeremy Evan Maltz*
LEHOTSKY KELLER COHN LLP
200 Massachusetts Avenue, NW,
Suite 700
Washington, DC 20001
(512) 693-8350
steve@lkcfirm.com
scott@lkcfirm.com
serena@lkcfirm.com
jeremy@lkcfirm.com

**admitted pro hac vice*
*** pro hac vice motion pending*

*Attorneys for Plaintiff NetChoice*