UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

NETCHOICE,
1401 K Street NW STE 502
Washington, DC 20005

Plaintiff,

v.

ANTHONY G. BROWN, in his official capacity as the Maryland Attorney General,
200 St Paul Place
Baltimore, MD 21202

and

WILLIAM D. GRUHN, in his official capacity as the Chief of the Division of Consumer Protection of the Maryland Office of the Attorney General,
200 St Paul Place
Baltimore, MD 21202

Defendants.

Civil Action No. ______________________

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 regime that will fundamentally reshape how websites speak to their users and how Americans access information 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

[1] This 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.

protected editorial functions through a vague and subjective "best interests of children" standard that gives state officials nearly boundless discretion to restrict 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); *Comput. & Commnc'ns Indus. Ass'n v. Paxton*, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024) ("*CCIA*"); *NetChoice, LLC v. Reyes*, 2024 WL 4135626 (D. Utah Sept. 10, 2024); *NetChoice, LLC v. Fitch*, 738 F. Supp. 3d (S.D. Miss. 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023).

4. Here, Maryland purports to regulate data. But regulating how online services present expressive content to their users is not a data regulation. Rather, it is a regulation of the dissemination and display of speech. As the Ninth Circuit concluded when evaluating a similar law, the Act "specifically defines data management practices by reference to the statutory factors a covered business must assess . . . when assessing those risks." *Bonta*, 113 F.4th at 1118. At core, "[t]hose factors require consideration of content or proxies for content." *Id.* The Act therefore imposes governmental oversight over the content online, which will chill the dissemination of protected speech. That is laid bare by the fact that Maryland enacted a data privacy bill in the *same legislative session*, which renders this Act superfluous to serve any interest the State has in regulating data privacy. *See* Md. Sen. Bill 541 (2024).

5. Maryland's approach is just as restrictive—and unconstitutional—in both scope and effect as the law at issue in *Bonta*.

6. The Act's fundamental flaw is its central command: requiring websites to analyze and restrict protected expressive content based on whether state officials might later determine such restriction would serve the "best interests of children"—an inherently subjective standard that

provides little meaningful guidance to websites and invites discriminatory enforcement. § 14-4801(c). This vague mandate will force websites to over-restrict speech and self-censor to avoid crushing penalties of up to $7,500 per minor for each violation. § 14-4808(b).

7. The Act builds on this unconstitutionally vague foundation by compelling speech and restriction of access to content through 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 certain types of content—exactly the type of compelled speech that the Ninth Circuit recently held unconstitutional in California's similar law. *Bonta*, 113 F.4th at 1117-18. And then it requires covered entities to take actions restricting speech—just like California's currently enjoined law. *Id.* at 1118.

8. In addition, the Act restricts how websites are designed and can collect and use information to publish, disseminate, and display speech to minors. The Act creates various presumptions against "processing" (*i.e.*, using) or "profiling" minors' information unless websites can prove they meet the Act's nebulous and content-based standards. § 14-4806. This includes the mere use of a minor's IP address to disseminate content Defendants might later deem to be inconsistent with the "best interests of children."

9. 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.

These results demonstrate that the Act goes far beyond the kinds of comprehensive data-privacy regulations carefully crafted by other States to avoid effects on content.

10. These harms will befall both regulated websites and their users—who use 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).

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

12. Defendants have acknowledged many of the Act's constitutional problems. In a letter to the Maryland Governor, Defendants warned: "there is some 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 as such, subject them to heightened scrutiny under the First Amendment and find those provisions unconstitutional." Ex. B. at 2.

13. Defendants understated the Act's problems.

14. 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.

15. 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.

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

PARTIES & STANDING

17. 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/.

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

19. *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); *Reyes*, 2024 WL 4135626, at *7; *CCIA*, 2024 WL 4051786, at *7-9; *Fitch*, 738 F. Supp. 3d at 766-68; *Yost,* 716 F. Supp. 3d at 549; *Griffin*, 2023 WL 5660155, at *9-10.

20. Based on the Act's definitions, § 14-4801(h), most—if not all—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 the Act's (often vague) directives.

21. Likewise, multiple NetChoice members have services that create, curate, and disseminate compilations of protected speech, including, *e.g.*, Amazon, Google, Meta, Nextdoor, Pinterest, and X.

22. *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); *CCIA*, 2024 WL 4051786, at *9; *Fitch*, 738 F. Supp. 3d at 766-68; *Yost,* 716 F. Supp. 3d at 549-51; *Griffin*, 2023 WL 5660155, at *11-12.

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

24. 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.

25. 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

26. 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).

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

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

29. 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

30. **NetChoice members' covered websites disseminate and facilitate protected speech.** The services operated by Plaintiff's regulated members both disseminate and facilitate all manner of speech protected by the First Amendment against government interference.

31. For example, "social media" and search-engine services "engage[] in expression" through their "display" and "compiling and curating" of protected content (text, audio, images, and video) "created by others." *Moody v. NetChoice, LLC*, 603 U.S. 707, 728, 731, 740 (2024).

32. On "social media" websites, users can "take positions on and engage with others in pursuit of the type of 'political, social, economic, educational, religious, and cultural' activities" protected by the First Amendment. *Fitch*, 738 F. Supp. 3d at 772 (citation omitted); *see Yost*, 716 F. Supp. 3d at 552; *Griffin*, 2023 WL 5660155, at *5-6.

33. Search services allow 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).

34. Services such as streaming services curate collections of movies and television shows. Often, these services personalize recommendations for particular users.

35. Other websites like online news services or sports services employ information they collect from users to present those users with the articles and other content that users might find most useful. For instance, a sports website may prioritize content about individuals' favorite sports teams. And a news service may highlight areas of particular interest for individual users.

36. Thus, regulations affecting websites' ability to disseminate, publish, and display speech in ways that are useful to users will ultimately harm those users.

37. **Websites use information to engage in editorial functions to publish, disseminate, and display protected speech to users.** To facilitate their curation and dissemination of speech—to facilitate their editorial discretion—websites collect and use data from their users.

38. Covered entities' use of information to inform their editorial discretion and to disseminate speech has a long historical pedigree.

39. 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.*

40. 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.

41. The information that websites collect and use vary, from information that helps make the services functional to information that enables websites to better disseminate and display expressive content to their users.

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. 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.

43. User data is also needed to deter and detect malicious actors. Many websites log activity and changes on an account. These logs help websites detect behavior that could signal a compromised account, and they can also help users restore accounts. Logs are also a crucial tool for law enforcement in many contexts. For instance, activity logs can help determine a missing person's last known location, interactions, or travel plans.

44. Without data collection, services could be less functional and less secure.

45. *Information to access services.* Many websites collect information that users provide to create accounts, such as usernames and contact information.

46. 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.

47. Allowing users to create accounts provides those users with greater security and provides services with a means to provide those users with curated content.

48. True, not all websites require users to create accounts to access some or all of the content on the service. Most have some universally accessible areas, in which people can view content without creating or logging into an account. But those areas often do not contain all the speech—or speech-facilitating functionality—that users with accounts can access.

49. It is up to individual websites to determine the proper tradeoff between the benefits of requiring accounts to access services (even if it imposes some private impediments to accessing speech) and making some content available to users that lack accounts or prefer not to log in.

50. *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.

51. 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.

52. "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.

53. That includes when they use "algorithms" to implement their editorial policies, even if "most often" websites display speech based on a "user's expressed interests":

> [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*. But it may also be based on more general features of the communication or its creator. . . . The platforms write *algorithms* to implement th[eir community] standards—for example, to prefer content deemed particularly trustworthy.

Id. at 734-35 (emphases added).

54. Content curation, whether through algorithms or other information-reliant means, allows users to see and engage with content that they may find most useful. This includes content from people they "follow" or "subscribe" to, recommended content from other people or accounts, alerts about developing events, and advertisements that help make the services viable.

55. Without curation, users could be lost in the potential "deluge" of content—which may not be useful, relevant, or appropriate to specific users. *Id.* at 719.

56. **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 Reyes*, 2024 WL 4135626, at *13 n.138; *Fitch*, 738 F. Supp. 3d at 774; *Griffin*, 2023 WL 5660155, at *6-8, Parental Control Guides, Internet Matters, https://perma.cc/VNA6-W76A.

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

58. 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.

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

60. 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.

61. 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.

62. 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.

63. 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.

64. 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.

65. In addition, some NetChoice members provide parents with tools and options to

help monitor their minor children's activities on their services.

66. 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 where appropriate, parents) can decide for themselves what they wish to engage with and what filters to adopt.

MARYLAND AGE-APPROPRIATE DESIGN CODE ACT

67. Maryland enacted the Age-Appropriate Design Code Act, which seeks to regulate the content on covered websites under the guise of privacy regulations.

68. The same legislative session, Maryland also enacted the Maryland Online Data Privacy Act of 2024, which imposes comprehensive data-privacy regulations. Md. Sen. Bill 541 (2024). That separate data-privacy law is not the subject of this challenge.

69. 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.

70. **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 only a subset of large Internet websites.

71. *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).

72. To "[c]ollect" personal data means to "buy, rent, gather, obtain, receive, or access personal data relating to a consumer," including "(i) Receiving data from the consumer; and (ii) Observing the consumer's behavior." § 14-4801(f).

73. "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).

74. "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).

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

76. *"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).

77. 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).

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

79. **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).

80. This standard suffuses the Act.

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

82. 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).

83. The "best interests of children" standard 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.

84. 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).

85. None of these terms is defined, and to the extent they resemble concepts used under other legal frameworks, it is not clear what they mean as applied to data use and digital "design."

86. Covered entities, therefore, lack the necessary guidance into what this standard requires them to disclose, do, or refrain from doing.

87. **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 for every "online product" they offer "that is reasonably likely to be accessed by children." § 14-4804(a)(1).

88. A Data Protection Impact Assessment is a "*systematic survey* to assess compliance with the duty to act in the best interests of children." § 14-4801(j) (emphasis added).

89. This requirement will first compel speech from covered entities, requiring them to disparage their services and opine on far-ranging and ill-defined harms that could purportedly arise from their services' "design" and use of information.

90. It also requires covered entities to address how their services meet the vague and

subjective "[b]est interests of children" standard. § 14-4801(c).

91. In so doing, the Act necessarily compels covered entities to surmise the purported harms from the *content* on their services.

92. Covered entities must "prepare" a "data protection impact assessment" that "shall": "(1) Identify the purpose of the online product; (2) Identify how the online product uses children's data; (3) Determine 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" 28 specific, subject determinations; and (4) "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).

93. Those 28 specified categories include 7 topics with 4 sub-considerations each:

(i) "Whether the data management or processing practices of the online product could lead to children experiencing or being targeted by contacts that would result in";
(ii) "Whether the data management or processing practices of the online product could permit children to participate in or be subject to conduct that would result in";
(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 that would result in";
(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 that would result in";
(v) "Whether, how, and for what purpose the online product collects or processes personal data of children and whether those practices would result in";
(vi) "Whether and how data collected to understand the experimental impact of the product reveals data management or design practices that would result in"; and
(vii) "Whether algorithms used by the online product would result in":
1. Reasonably foreseeable and material physical or financial harm to children;
2. Reasonably foreseeable and extreme psychological or emotional harm to children;
3. A highly offensive intrusion on children's reasonable expectation of privacy; or
4.Discrimination against children based on race, color, religion, national origin, disability, gender identity, sex, or sexual orientation;

§ 14-4804(b)(3).

94. In addition to those specified categories, covered entities are compelled to

"[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).

95. Moreover, the Act will require *many* Assessments—or at least onerous Assessments addressing myriad aspects of covered entities' services.

96. In particular, covered entities must produce an assessment for every qualifying "online product" that "[i]s offered to the public on or before April 1, 2026"; and (2) "[w]ill continue to be offered to the public after July 1, 2026." § 14-4804(a)(2). Similarly, "a covered entity shall complete a data protection impact assessment" for a qualifying "online product that . . . is initially offered to the public after April 1, 2026." § 14-4804(a)(3).

97. 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).

98. The Act then 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).

99. In all, this requirement will compel speech from covered entities, requiring them to disparage their services and opine on far-ranging and ill-defined harms that could purportedly "result" from their services' "design" and "processing" of information.

100. And the Act requires covered entities to work to ameliorate harms, which will necessarily require covered entities to alter their dissemination and display of content.

101. The Act imposes several ongoing obligations related to the Assessments.

102. *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).

103. *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).

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

105. **Restrictions on using information to disseminate protected speech based on "best interests of children" standard (§ 14-4806).** The Act creates a variety of default presumptions against online services using information (what the Act calls "processing" and "profiling") to publish, disseminate, and display protected speech to users.

106. This goes far beyond regulating data.

107. Instead, these provisions essentially create presumptions against collecting or using—or even *deleting*—information when publishing and displaying online speech to users.

108. In so doing, these provisions restrict a range of commonplace online speech, including engaging with users to learn their preferences; using collected information to curate content; providing users recommendations about books, movies, newspaper articles, and other content; or even potentially sending automated email updates to users.

109. Under the Act, covered entities often must prove a negative: That their use of information will not violate the Act's vague "best interests of children" standard.

110. The Act imposes various restrictions on "processing" information, by providing that a "covered entity that provides an online product that is accessed or reasonably likely to be

accessed by children may not":

> (1) Process the personal data of a child in a way that is inconsistent with the best interests of children reasonably likely to access the online product;
> . . .
> (3) Process personal data of a child that is not reasonably necessary to provide an online product that the child is actively and knowingly engaged with;
> (4) Process the personal data of a child end user for any reason other than a reason for which that personal data was collected;
> (5) Process any precise geolocation data of a child by default, unless:
> (i) The collection of the precise geolocation data is strictly necessary for the covered entity to provide the online product; and
> (ii) The precise geolocation data is processed only for the limited time that is necessary to provide the online product;
> (6) Process any precise geolocation data of a child without providing an obvious signal to the child for the duration that the precise geolocation data is being collected;
> . . .
> (8) Process any personal data for the purpose of estimating the age of a child that is actively and knowingly engaged with an online product that is not reasonably necessary to provide the online product; or
> (9) Allow 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).

111. "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).

112. As a result, regardless of whether a service "collect[s]" or "delete[s]" information from users, it must justify that action before doing so—or else risk violating the Act.

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

> (i) 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
> (ii) 1. 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
> 2. The covered entity can demonstrate a compelling reason that profiling is in the best interests of children;

§ 14-4806(a)(2).

114. "Profile" means multiple ways that covered entities might personalize content: "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).

115. Finally, the Act prohibits covered entities from using so-called "dark patterns" to: "(i) Cause a child to provide personal data beyond what is reasonably expected to provide the online product;(ii) Circumvent privacy protections; or (iii) Take 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).

116. 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).

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

118. 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.

119. 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).

120. 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).

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

122. In light of these penalties, guessing wrong about what the Act means 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

123. Each First and Fourteenth Amendment challenge raises the rights of both NetChoice members and those who use or could prospectively use NetChoice members' websites.

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

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

125. The Act's central command that covered entities design their services and operate in the "best interests of children," § 14-4801(c), 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.

126. "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)).

127. 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.

128. 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.

129. 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.

130. 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).

131. Such concerns about protected speech have been prevalent throughout American history. *See Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 797 (2011); U.S. Surgeon General, Television and Growing Up: The Impact of Televised Violence (1972), https://perma.cc/QP4H-73V4.

132. To begin, the Act requires covered entities to make numerous subjective and indeterminate considerations about how their use of data and service design will affect all minors—regardless of age, socioeconomic status, preferred language, and many other relevant factors.

133. 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.

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

135. 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.

136. 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.

137. 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.

138. 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).

139. This is a standard applied in the family 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).

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

141. It is especially inappropriate as the standard by which to evaluate the way that websites—and all the features on them—are designed and operate.

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

143. *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).

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

145. 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.

146. 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.

147. 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.

148. 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).

149. 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.

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

151. 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).

152. *Second*, it is unclear how to evaluate whether the use of information will "[r]esult in . . . [r]easonably foreseeable and material physical or financial harm." § 14-4801(c)(2)(i).

153. The necessary link between a website's design and/or its use of information and physical harm is unclear.

154. *Third*, it is unclear how 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).

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

156. 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).

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

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

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

160. 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).

161. *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).

162. Of course, Maryland already prohibits discrimination through its separate,

generally applicable antidiscrimination law. *E.g.*, Md. Code, State Gov't § 20-304.

163. 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.

164. 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).

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

166. 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 v. Colorado*, 600 U.S. 66, 79 & n.5 (2023).

167. 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.

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

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

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

171. 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.

172. 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.

173. 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.

174. 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
VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH AMENDMENTS
("REASONABLY LIKELY TO BE ACCESSED BY" STANDARD)

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

176. 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.

177. 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.

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

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

180. Neither of the emphasized terms are defined.

181. "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.

182. 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).

183. 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).

184. In other words, even if a website has *zero* minor users, if it is "substantially similar" to a website that *does* have a "significant number" of minors, it must comply with this Act.

185. 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 penalizes websites any time they have even a single minor access the service.

186. 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).

187. 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.

188. 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 III
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)

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

190. 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.

191. 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.

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

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

194. "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)).

195. 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.

196. 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).

197. 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.

198. 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); *Fitch*, 738 F. Supp. 3d at 780 (same).

199. 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.

200. 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)).

201. 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].").

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

203. "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.

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

205. 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).

206. "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.

207. 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).

208. 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).

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

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

211. 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.

212. 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.

213. *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.*

214. *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.

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

216. 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).

217. A State's legitimate interest in child welfare "does not include a free-floating power

to restrict the ideas to which children may be exposed." *Brown*, 564 U.S. at 794. "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).

218. "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.

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

220. "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.

221. 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.

222. *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).

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

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

225. 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.

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

227. *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.

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

229. "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.

230. 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. v. Bonta*, 116 F.4th 888, 899 (9th Cir. 2024) (citation omitted); *accord Reyes*, 2024 WL 4135626, at *9 n.92.

231. "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).

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

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

234. 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 IV
42 U.S.C. § 1983
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT
(RESTRICTIONS ON COLLECTION AND USE OF INFORMATION – § 14-4804)
(FACIAL AND AS-APPLIED CHALLENGE)

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

236. The Act's restrictions on "processing" and "profiling" information to disseminate content to minors violate the First Amendment both facially and as applied to NetChoice members, to the extent they limit an online service's rights to collect and use information for the purposes of curating, recommending, and delivering protected speech to users. § 14-4804.

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

238. In other words, the Act's restrictions on collecting and using information are unconstitutional to the extent they limit covered NetChoice members' rights to collect and use information for the purposes of curating, recommending, and delivering protected speech to users.

239. 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 v. IMS Health Inc.*, 564 U.S. 552, 570 (2011)).

240. When NetChoice members curate and disseminate compilations of protected

speech on their services, they engage in protected speech dissemination and editorial discretion protected by the First Amendment.

241. Accordingly, the curated feeds of services such as "Facebook" and "YouTube" are protected. *Moody*, 603 U.S. at 734-35, 739-40. That includes when they use "algorithms" to implement editorial policies, even if based in part on "user's expressed interests." *Id.* at 734-35.

242. In addition, the "creation and dissemination of information are speech within the meaning of the First Amendment." *Sorrell*, 564 U.S. at 570.

243. Thus, the First Amendment protects covered entities' use of information to choose whether, when, and how to publish, disseminate, and display expressive content to their users.

244. Speech on the Internet requires some amount of "collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data." § 14-4801(p).

245. Yet the Act would create presumptions against using information to determine whether and how to publish and display content to minors.

246. For instance, covered websites would need to demonstrate that their "processing" and "profiling"—*i.e.*, use—of information to disseminate speech to minor users is "consistent with the best interests of children." § 14-4806.

247. That is an undue restriction on speech.

248. The "best interests of children" standard is vague, as explained above.

249. 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.

250. Moreover, preconditions on publishing speech are unconstitutional prior restraints.

251. The Act penalizes covered entities from using information that covered websites "already possess[]," which unconstitutionally restricts "'the way in which [] information might be

used.'" *Sorrell*, 564 U.S. at 568 (citation omitted).

252. The Act's "reasonabl[e] foreseab[ility]," § 14-4801(c)(2)(i)-(ii), standard imposes further First Amendment problems.

253. 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. *Smith v. California*, 361 U.S. 147 (1959). Accordingly, the First Amendment requires more than a mere negligence standard to punish the dissemination of even unprotected speech. *Counterman*, 600 U.S. at 79 & n.5.

254. This Act targets large volumes of protected speech.

255. 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.

256. The Act's restrictions on the use of information to publish speech trigger and fail any form of heightened scrutiny for the reasons discussed above.

257. Unless declared invalid and enjoined, the Act's restrictions on the use of information to publish speech 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, 15 U.S.C. §§ 6501, AND
***EX PARTE YOUNG* EQUITABLE CAUSE OF ACTION**
PREEMPTION UNDER THE SUPREMACY CLAUSE OF THE CONSTITUTION

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

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

260. 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.

261. 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).

262. 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).

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

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

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

266. 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).

267. 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).

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

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

270. 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.

271. 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).

272. *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.

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

274. 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.

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

COUNT VI
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)

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

277. 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.

278. 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).

279. 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).

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

281. 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.

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

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

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

285. 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 §§ 14-4804, 14-4805, 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;
c. 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;
d. 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;

e. declaring that the Maryland Age-Appropriate Design Code Act is preempted by the Children's Online Privacy Protection Act;
f. declaring that the §§ 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;
g. declaring that the unlawful portions of the Maryland Age-Appropriate Design Code Act are not severable from the rest of the Act;
h. entering judgment in favor of Plaintiff;
i. 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
j. awarding Plaintiff all other such relief as the Court deems proper and just.

Dated: February 3, 2025

Respectfully submitted,

Steven P. Lehotsky*
Scott A. Keller*
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
jeremy@lkcfirm.com

**pro hac vice forthcoming*

/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)

Attorneys for Plaintiff NetChoice