UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

NETCHOICE, *Plaintiff*, v. CHARITY CLARK, in her official capacity as the Vermont Attorney General, *Defendant*.	Civil Action No. 2:26-cv-444

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. Vermont has enacted sweeping restrictions on speech. Although styled as a data privacy law, the Vermont Age-Appropriate Design Code Act ("Act") establishes a censorship regime that subjects online communications to state supervision and will hobble a free and open resource for "exploring the vast realms of human thought and knowledge." *Packingham v. North Carolina*, 582 U.S. 98, 107 (2017).[1]

2. The Act's legal infirmities are pervasive, and regulations recently promulgated by the Attorney General compound those defects.

3. *First,* the Act violates the First Amendment by fundamentally restricting how websites curate, disseminate, and publish speech, and what speech they present, who can access it, and when.

[1] The Act is codified at 9 V.S.A. §§ 2449a *et seq*. This Complaint uses the terms "business," "service," or "website" to include all regulated "[c]overed business[es]," § 2449a(10), including their "online products, services, or features," § 2449a(10)(C). Unless otherwise noted, all statutory citations are citations to Title 9 of the Vermont Statutes Annotated.

4. At the threshold, the Act requires a speaker-based and content-based collection of websites to decide whether their services are "reasonably likely to be accessed by" users under 18, and if so, to employ "age assurance" methodologies to discern which users *are* minors. This will burden and discourage access to constitutionally protected speech for minors and adults alike.

5. The Act then compels covered websites to act as the government's speech police by attaching a "duty of care" to their use of "data" and website "design" to ensure their services will not "result in" foreseeable "emotional distress," "compulsive use," or "discrimination" for even a single Vermont minor. § 2449c(b).

6. This duty requires websites to alter their editorial processes based on the predicted "impact that speech has on its listeners." *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 811 (2000). Such a "system of informal censorship" carries "a heavy presumption against its constitutional validity." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70-71 (1963). The State may not quiet speech because it is "too persuasive," *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 577-78 (2011), or distressing. *Snyder v. Phelps*, 562 U.S. 443, 456 (2011). "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 v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 (2011) (cleaned up).

7. The Act also directly restricts speech by strictly limiting how and when websites can receive, use, and process speech and information that is "reasonably linkable to" a Vermont minor or a household device. The Act calls such information "personal data," § 2449a(21), and invokes "privacy" to pervasively restrict it. *See* §§ 2449d, 2449g. But the term extends far beyond any plausible privacy rationale to encompass a wide range of information that is intrinsic to internet communication itself, from basic device data needed to transmit online speech to users at all, to

speech created and posted by users, and everything in between. § 2449d(a)(1)(B). Indeed, the definition extends even to *thoughts* and *ideas* about user-linked information (so-called "derived data"), including "inferences, predictions, or conclusions" drawn from "information or data about a minor or a minor's device." § 2449a(15). The Act prohibits using or even receiving such information unless the State deems it "necessary," which excludes using data "to select, recommend, or prioritize" speech, even to ensure more age-appropriate material. § 2449f(a)(4).

8. The First Amendment forbids these broad-scale controls on information. The First Amendment protects the "selection and ranking" of speech "based on a user's expressed interests and past activities." *Moody v. NetChoice, LLC*, 603 U.S. 707, 734-35 (2024). And, more fundamentally, it protects "information in private hands." *Sorrell*, 564 U.S. at 568 (citing cases). Here, as in *Sorrell*, Vermont "has imposed content- and speaker-based restrictions on the availability and use of [such] information." *Id.* at 571. And here, as there, Vermont may not evade the First Amendment by invoking "privacy" for "disfavored" speech and speakers only. *Id.* at 573.

9. The Act also *compels* websites to speak about their content "recommendation system," § 2449e(2)-(3), flouting websites' "right to refrain from speaking at all," *Wooley v. Maynard*, 430 U.S. 705, 714 (1977). "Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech" and demands strict scrutiny, which the Act does not survive. *Riley v. Nat'l Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781, 795 (1988).

10. *Second,* the Act creates an insurmountable vagueness problem, violating the "fundamental principle in our legal system" that laws "must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). The Act defines its prohibitions in hopelessly abstract terms—like "compulsive use" and "emotional distress," § 2449c—that require websites to predict the effects of speech on each "covered minor,"

regardless of age, preference, background, or sensitivities. *See NetChoice, LLC v. Bonta* ("*Bonta-AADC II*"), 170 F.4th 744, 764-65 (9th Cir. 2026) (affirming injunction of similar provision).

11. The Act and regulations also leave key terms undefined or subject to standards that are circular or leave websites in the dark about what is required of them. For example, under the recently issued regulations, businesses must perform "reasonably necessary" and "commercially reasonable" age assurance methods when "reasonably necessary" if a website's audience is composed of at least two percent minors, based on an assessment using only "reasonably necessary" data. Yet the Act and regulations repeatedly fail to describe what *is* reasonable or necessary. Websites are left to guess—on pain of steep penalties—as to what designs, editorial practices, features, content, and users may subject them to liability. This lack of clarity invites subjective enforcement of the Act and forces websites "to steer far wider of" activities that Vermont might lawfully restrict if the boundaries "were clearly marked." *Baggett v. Bullitt*, 377 U.S. 360, 372 (1964).

12. *Third*, Section 230 of the Communications Decency Act of 1996, 47 U.S.C. § 230, preempts the Act's requirements for "social media" and other provisions that regulate how websites sort and arrange third-party content. "At its core, § 230 bars 'laws[] seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content.'" *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016) (citation omitted). The Act does just that by attaching a "duty of care" to online publication, § 2449c, restricting how speech is "display[ed]," § 2449d(a)(1)(B), curtailing how websites "select, recommend, or prioritize media," § 2449f(a)(4), and otherwise mandating how covered websites "arrang[e] and distribut[e] third-party information." *Force v. Facebook, Inc.*, 934 F.3d 53, 66 (2d Cir. 2019).

13. *Fourth*, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506, preempts the Act's restrictions on minors' data.

14. Enacted shortly after Section 230, COPPA reflects Congress's own considered judgment about how to protect children's online privacy while preserving a free and open internet. Congress chose to regulate the use of minors' online data only when websites have "actual knowledge" that a user is a child under 13 or the website is "directed to" such children. *Id.* § 6501(1), (4)(B). Congress elected not to regulate the data of teen users (as original drafts of the legislation proposed) and not to require any form of age assurance. And for the personal data of known children under 13, Congress placed the control with parents—not government—by allowing websites to collect and use such data so long as they provide notice of their activities to parents and obtain verifiable, informed consent. 16 C.F.R. §§ 312.3(a), 312.5(a)(1).

15. To preserve a uniform, national standard, Congress broadly preempted state liability for "commercial" data activities "that [are] inconsistent with the treatment of [such] activities" under COPPA. 15 U.S.C. § 6502(d). The Act's rigid and wide-ranging restrictions on the collection and use of minors' data are "inconsistent" with COPPA's flexible, parent-oriented "treatment" and thus preempted.

16. *Finally*, the Act violates the Commerce Clause, which precludes "the application of a state statute to commerce that takes place wholly outside of the State's borders," *Mayer v. Ringler Assocs. Inc.*, 9 F.4th 78, 85 (2d Cir. 2021) (citation omitted), and laws that impose "clearly excessive" burdens on interstate commerce relative to "local benefits." *Variscite NY Four, LLC v. N.Y. State Cannabis Control Bd.*, 152 F.4th 47, 65 (2d Cir. 2025).

17. Internet regulations necessarily implicate the Commerce Clause because the internet "does not recognize geographic boundaries." *Am. Booksellers Found. v. Dean*, 342 F.3d

96, 103 (2d Cir. 2003); *see ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999) (citation omitted) (the internet "requires a cohesive national scheme of regulation"). And the Act here goes too far. It "project[s] [Vermont's regulatory choices] onto the rest of the nation," *Am. Booksellers Found.*, 342 F.3d at 103, by controlling how websites use data anywhere in the world so long as the data is "linkable" to a device that can be further linked to a Vermont minor resident. The Act also imposes "clearly excessive" burdens, *Variscite NY Four, LLC*, 152 F.4th at 65, that will fragment online communications, drive smaller websites out of business, and impair the internet's value as a global medium.

18. For these reasons and more, this Court should enjoin Defendant from enforcing the Act against Plaintiff's members and declare the Act unlawful—just as courts have enjoined similar laws. *See, e.g.*, *NetChoice, LLC v. Bonta* ("*Bonta-AADC I*"), 113 F.4th 1101, 1125-26 (9th Cir. 2024); *NetChoice v. Murrill*, 812 F. Supp. 3d 594, 663-64 (M.D. La. 2025); *NetChoice v. Griffin* ("*Griffin III*"), 812 F. Supp. 3d 905, 928 (W.D. Ark. 2025).

PARTIES & STANDING

19. Plaintiff NetChoice is a District of Columbia nonprofit trade association for companies that operate online services. 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://perma.cc/4LHS-74JF.

20. NetChoice has standing to bring its challenges to the Act.

21. 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); *NetChoice, L.L.C. v. Fitch*, 134 F.4th 799, 804-05 (5th Cir. 2025). Based on the Act's definitions, § 2449a, many 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 directives, including Amazon, Audible, Automattic, Discord, Dreamwidth, Goodreads, Google, Meta, Netflix, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, X, and YouTube.

22. NetChoice has standing to assert the First Amendment rights of its members' users. *See Virginia v. Am. Booksellers Ass'n*, 484 U.S. 383, 392-93 (1988); *Defending Educ. v. Croton-Harmon Union Free Sch. Dist.*, 190 F.4th 53, 61 (2d Cir. 2026); *Fitch*, 134 F.4th at 805-07.

23. Separately, NetChoice has standing in its own right as a user of online services. NetChoice regularly uses many of the regulated websites, such as Instagram, X, and YouTube, to disseminate information about its advocacy activities and policy positions, and to educate the public—including teens and young adults—about First Amendment freedoms and other legal protections for online speech. The Act's restrictions will make it more difficult for NetChoice to use these platforms to speak to users in Vermont and elsewhere.

24. Defendant Charity Clark is the Vermont Attorney General. Defendant is a Vermont resident and is sued in her official capacity.

25. The Act gives the Vermont Attorney General authority to enforce the Act. *See* § 2449h(b).

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 and *Ex parte Young*, 209 U.S. 123 (1908), 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 Defendant because she resides in and conducts a substantial proportion of her official business activities in Vermont.

29. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant resides in, and the events giving rise to this civil action occurred in, Vermont.

BACKGROUND

30. **The internet is an expressive, communicative, and informational medium through which NetChoice members create and facilitate protected speech.** The "vast democratic forums of the Internet" are home to immense amounts of protected First Amendment activity. *Packingham*, 582 U.S. at 104 (quoting *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.

31. NetChoice members' services in particular offer "relatively unlimited, low-cost capacity for communication of all kinds." *Id*.

32. "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. "On Twitter [now X], users can petition their elected representatives and otherwise engage with them in a direct manner." *Id.* at 104-05. Social media services both facilitate the expressive activities of third parties (such as users and content creators) and "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. Such services facilitate "billions of posts" of fully protected

speech, *id.* at 734, that enable people to "gain access to information and communicate with one another" in countless ways. *Packingham*, 582 U.S. at 107.

33. Beyond social media exists a panoply of other digital services that disseminate speech. Video streaming services like Disney+, 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 audiobooks. Library apps like Hoopla and Libby allow users to borrow e-books, audiobooks, and other digital materials from participating public libraries and read or listen to them on their phones, tablets, or computers. Blogs like Above the Law and SCOTUSblog provide news, commentary, explainers, and other information, often allowing interested users to subscribe to updates, participate in liveblogging, access podcasts, and otherwise interact with online communities oriented around shared interests. Online news services (like nytimes.com, vtdigger.org, burlingtonfreepress.com, and foxnews.com) and sports services (like ESPN) offer up-to-the-minute news and sports coverage 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 (citation omitted).

34. **Online services, including NetChoice members, require user-linked "data" to publish speech and engage in editorial functions.** Websites could not curate, disseminate, or publish protected expression without collecting and using information that is provided by, or linkable to, users or their devices. Although the Act calls this information "personal data," it extends far beyond the information historically considered sensitive or "personally identifying" in the offline world, such as social security numbers and medical information. It can be analogized

to the ink and paper necessary to publish a newspaper, the facts that inform a news article, the market research behind the topics covered, the subscriber addresses necessary to deliver the newspaper to a customer, and even the article itself.

35. *Data to provide the service.* Data collection is performed by online services to provide functional services and content. Websites collect information about IP addresses, 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.

36. Similarly, other information—like a user's operating system and language preferences—allows 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.

37. User data is also collected and analyzed to deter and detect malicious actors. Many websites use incoming data to look for signals of a compromised account or help users restore their accounts. Without the ability to collect and use data for these purposes, services would be less functional and less secure.

38. *Information to access services.* Many websites have aspects that are 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. Similarly, library apps like Libby and Hoopla require users to create an account to ensure loans of books and other materials are made to verified users and card-holders.

39. Allowing users to create accounts gives them greater security, gives other users the ability to decide whether to grant that particular user access to their content, and gives services a

means to deliver curated and age-appropriate content. But to offer account-based functionalities, websites must collect and process information that users provide, such as usernames, age, contact information, security questions, and settings preferences.

40. *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 websites can make granular, nuanced decisions about which content they want to present to whom, and that users 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 or that does not interest them.

41. For instance, the Supreme Court recognized that the "feeds" of news and other postings—including the curated feeds of "Facebook" and "YouTube"—are protected by the First Amendment. *Moody*, 603 U.S. at 734-35, 739-40. "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.

42. The Supreme Court has also recognized that these protected feeds are often personalized:

> [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 . . . . 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 (cleaned up) (emphasis added).

43. Personalized content curation 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 "deluge" of content. *Id.* at 719. Much of that content may not be relevant, and some may even be inappropriate for specific users. In fact, a common use of personalization is to ensure that users see content that is appropriate and useful for their particular tastes and circumstances, including age-appropriate content for minors.

44. Services beyond social media websites use personalization too. A video streaming service like Hulu might use personalization to recommend shows and movies based on a combination of a user's prior watching habits, direct feedback from users such as "likes" or "dislikes," and preferences selected during account setup. Music streaming services do the same. Library apps like Hoopla may generate recommendations based on titles a reader has marked as a favorite. Online news sources—including the New York Times and Wall Street Journal—and e-reading services also use personalization to recommend articles and books based on content a user has previously engaged with.

45. Services apply their own independent standards when moderating—selecting, prohibiting, prioritizing, or deprioritizing—the personalized content that may appear on a user's feed, including by accounting for users' individual data as part of the moderation process.

46. To implement these judgments, Amazon, Facebook, Instagram, Pinterest, Reddit, Threads, TikTok, Tumblr, X, and YouTube frequently use "algorithms," which the services "write . . . to implement" their own "Community Standards," editorial preferences, and similar

policies, including as to what content may be age-appropriate for users of particular ages. *Id.* at 734-35.

47. Although these curation algorithms are automated, they embody numerous human editorial choices by both the online services and the audiences they serve, reflected in the content presented to users. These expressive compilations therefore do not simply respond "to how users act online—giving them the content they appear to want, without any regard to independent content standards." *Id.* at 736 n.5. Rather, members implement numerous independent judgments about the types of speech they want to foster and the communities they want to help create. These include judgments about what content should be more (or less) prominent in a user's "feed"; how to identify content that might not be appropriate to recommend widely, such as low-quality, clickbait, or violent content; how much new versus familiar content to present; how to implement community guidelines and content policies; and how to moderate content that might be considered more problematic with repeated exposure. Websites also decide what feedback and signals from users help them assess content quality and how to present and organize content. These judgments are dynamic and iterative, reflecting affirmative and ongoing efforts to present a unique expressive offering.

48. **The media have always tailored content to audiences.** The use of engagement information to create speech that audiences enjoy is nothing new. As one example, Benjamin Franklin "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.[2] After purchasing the *Pennsylvania Gazette* in 1729, Franklin announced plans to change the format of the reference

[2] *4 Illuminating Lessons From One of History's Most Inventive Content Marketers*, Content Mktg. Inst. (Apr. 9, 2014), https://perma.cc/F7KV-DMUU.

guides it published: He would no longer publish them serially or alphabetically but would instead exercise judgment to publish useful or interesting portions relevant to colonial manufacturing and invention.[3] Thereafter and throughout the colonial era, the *Pennsylvania Gazette* observed reader interests and what sold best, and adapted the paper's contents to sell more copies.[4] In 1769, the publishers of the *Boston Chronicle* similarly studied reader preferences to make a data-based decision to release an additional regular issue (rather than enlarge their existing weekly paper) to better secure audience interest.[5] And in 1768, the publisher of the *Georgia Gazette* tested reader demand for a proposed pamphlet of religious materials by reviewing pledges of interest in particular subject matter.[6]

49. Successful newspapers of the nineteenth century likewise "studied constituents' tastes" to print items that readers enjoyed.[7] That process became increasingly data-driven as information technology improved and gave publishers more specific insights about their audiences.[8] The advent of broadcast technologies allowed for twentieth-century radio content to

[3] Benjamin Franklin, *Apology for Printers* (June 10, 1731), in 1 The Papers of Benjamin Franklin 194-99 (Leonard W. Labaree ed., 1959) (explaining how he found that popular songs sold papers more quickly than well-translated biblical verses), https://perma.cc/8VWC-HUCR.

[4] Benjamin Franklin, *The Printer to the Reader*, *Pa. Gazette* (Oct. 2, 1729), https://perma.cc/Q4WF-GVQE.

[5] Mein & Fleeming, *To the Public*, *Boston Chronicle*, Jan. 2, 1769, reproduced and discussed by Carl Robert Keyes, The Adverts 250 Project (Jan. 2, 2019), available at https://perma.cc/RM8K-3ZLM.

[6] James Johnston, *Proposed to be Published, A Pamphlet*, *Ga. Gazette*, Jan. 13, 1768, reproduced and discussed by Carl Robert Keyes, The Adverts 250 Project (Jan. 13, 2019), https://perma.cc/NC5P-GB37.

[7] Gerald J. Baldasty, *The Commercialization of News in the Nineteenth Century* 121 (1992), https://tinyurl.com/vza8zxwj.

[8] Philip M. Napoli, *Audience Evolution: New Technologies and the Transformation of Media Audiences* 31-40 (2011).

be channeled to particular audiences by subject matter, formats, and genres (i.e., news, sports, talk, jazz, classical, pop) known to attract particular listeners' attention.[9] Television and film studios likewise organized fan mail "according to the writer's estimated age, gender, and geographic location" to make decisions about what to broadcast where, when, and to whom.[10] The arrival of cable and satellite television in the 1970s further "facilitated the greater granularity in audience composition" that content providers desired.[11] Even pre-internet television used engagement data and deployed recommendation tools roughly equivalent to today's technologies: Digital video recorders such as TiVo could be "programmed to learn from the user's demonstrated viewing behaviors and make program recommendations—and even record programs—based on the user's prior viewing patterns."[12] And even before TiVo, the television networks had long used Nielsen ratings to understand audience preferences and decide what programming to air and when to air it.

50. Today's digital publishing practices carry forward this same longstanding tradition.

51. **There are many existing tools for parents and guardians to control and oversee their children's online activities.** "[P]arents may rightly decide to regulate their child's use of social media—including restricting the amount of time they spend on it, the content they may access, or even those they chat with. And many tools exist to help parents with this endeavor." *NetChoice, LLC v. Griffin* ("*Griffin II*"), 2025 WL 978607, at *3 (W.D. Ark. Mar. 31, 2025) (collecting evidence); *e.g.*, *Bonta-AADC I*, 113 F.4th at 1121.

---

[9] Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* 12-19 (2017).

[10] Napoli, *supra* n.8, at 33.

[11] *Id.* at 40-42.

[12] *Id.* at 60.

52. There are resources that collect all these parental tools in one place.[13]

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

54. Cellular and broadband internet providers also offer families tools to block certain online services from certain devices.[14]

55. Internet browsers also allow parents to control what online services their children may access.[15] Some browsers offer a "kids mode" or allow parents to see what online services their children are accessing the most.[16] Parents can also use widely available browser extensions to reinforce these tools.

56. Wireless routers often have settings allowing parents to block particular websites, filter content, monitor internet usage, and control time spent on the internet.[17]

57. 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.[18]

---

[13] *E.g.*, Internet Matters, *Parental Control Guides*, https://perma.cc/WB2F-LQWF.

[14] *See, e.g.*, Verizon, Verizon Smart Family, https://perma.cc/W24Y-TXJF; AT&T, AT&T Secure Family, https://perma.cc/N5DN-8PKR; T-Mobile, Family Controls and Privacy, https://perma.cc/L5BS-NZ6Z.

[15] *See, e.g.*, Mozilla, *Block and unblock websites with parental controls on Firefox* (last updated Nov. 6, 2026), https://perma.cc/5ERY-FSWL.

[16] *See* Google, Safety Center, *Choose parental controls that are right for your family*, https://perma.cc/V7XB-QXFB.

[17] *See, e.g.*, Netgear, *How do I set up and install NETGEAR Smart Parental Controls?* (last updated July 7, 2025), https://perma.cc/R57A-NV69; tp-link, *How to configure Parental Controls on the TP-Link Wi-Fi Router* (last updated Oct. 21, 2025), https://perma.cc/CU7Y-2CLS.

[18] *See* ConnectSafely, *Set parental controls with the Amazon Kids Parent Dashboard*, Amazon News (last updated Nov. 19, 2025), https://perma.cc/R8TM-AS3N; Apple, *Set up parental controls to manage your child's iPhone or iPad* (Oct. 26, 2026), https://perma.cc/N8RF-83W8; Apple, *Use Screen Time to manage your child's iPhone or iPad* (Oct. 26, 2026),

58. Many third-party applications also allow parents to control and monitor their children's online activities.[19]

59. These existing market solutions underscore the Act's overreach—less restrictive alternatives exist, are available to all parents, and are already used by many.

60. And these existing solutions allow parents to tailor their approaches to the needs of their families, rather than impose a one-size-fits-all approach.

61. **Parental tools provided by NetChoice members.** In addition, NetChoice members provide parents and minors with many tools and options to help ensure that minor children are responsibly using their services.

62. Amazon offers a Parent Dashboard with easy-to-use tools that tailor kids' experiences on Amazon devices to align with individual parenting styles, including decisions about the content kids see and the features they can access on their own.[20] Grown-ups can opt in or out of digital features and (on applicable devices) exercise parental controls over browsing experiences for assurance that kids are safe, even when an adult is not present. The Parent Dashboard allows adults to manage a child's screen time and digital content on up to four individual child profiles across multiple devices. Usage information—including books, videos, skills, and apps—is displayed for at-a-glance consideration. These quick insights help grown-ups understand what

---

https://perma.cc/EPM2-2AJX; Google Family Link, *Help keep your family safer online*, https://perma.cc/HQS4-L2TV; Microsoft, *Set up Microsoft Family Safety* (2026), https://perma.cc/6RFM-JGBB; Samsung, *Manage Family groups and parental controls with your Samsung Account*, https://perma.cc/HGD6-BSPA; Samsung, *Use Digital Wellbeing features on your Galaxy phone or tablet*, https://perma.cc/7MWE-KT6S; Android Help, *Manage how you spend time on your Android phone with Digital Wellbeing* (2026), https://perma.cc/R99F-PYW4.

[19] *See, e.g.*, Benedict Collins, *Best Parental Control App of 2026: Our security experts and parents give their verdict*, TechRadar (Jan. 8, 2026), https://perma.cc/DD9U-U7LH.

[20] *See* Amazon, *Parent Dashboard*, https://perma.cc/VY89-K82F.

their kids are interested in, foster one-on-one conversations based on those findings, and set appropriate screen-time limits.

63. Audible offers a Kids Profile that, among other things, allows parents and guardians to supervise the audiobooks and podcast episodes added to libraries for their children and restrict purchases.[21] This feature allows parents and guardians to choose to what extent to use those controls, based on their parenting philosophies, relationships with their children, the audio content at issue, and other factors.

64. Parents and guardians can also use supervision tools on Facebook, Instagram, and Threads to set daily time limits for their teens and choose whether their teen sees a reminder to close the app or is blocked from using the app entirely once their daily time limit is reached; turn on sleep mode during select days and hours, and choose whether their teen sees a reminder to close the app or is blocked from using the app entirely during those days and times; view and change their teen's content settings; see the average amount of time their teen has spent on Facebook and Instagram over the last week and the total time spent on Facebook and Instagram for each specific day over the last week; see who their teen follows and who follows their teen; see which accounts their teen is currently blocking; see when their teen reports someone and for what reason; and more.[22] Parents and guardians will soon be able to adjust their teen's default experience to require a non-personalized default feed on Facebook and Instagram (and teens will have this option as well).

---

[21] *See* Audible, *Listen with a Kids Profile*, https://tinyurl.com/ve3w98zd.

[22] *See, e.g.*, Instagram, Help Center, *Parental Supervision* (2026), https://perma.cc/8C63-M3Q2; Facebook, Help Center, *Safety Resources for Parents* (2026), https://perma.cc/BR6P-LKV8; Instagram, Help Center, *About Supervision on Threads* (2026), https://perma.cc/9ULG-PKFB.

65. Meta places teens on Facebook, Instagram, and Threads into Teen Accounts. Teen Accounts have built-in protections that limit who can contact teens, the content they see, and the time they spend. For example, with Teen Accounts, teens receive the following default protections: daily time limit notifications after they have spent 60 minutes on Instagram; Sleep Mode, which mutes notifications overnight and sends auto-replies if someone tries to direct message them; private accounts, so people who do not follow a teen cannot see their content or tag, mention, or interact with them; blocks on search terms related to certain sensitive topics like suicide, self-harm, and eating disorders; and more. Teens under 16 cannot change any of these default settings without a parent's permission.[23] In the coming months, Meta will be offering additional default protections for teens that can only be turned off with a parent's permission, including a two-hour daily time limit cumulative across Facebook and Instagram; a block on Facebook and Instagram access between 12 a.m. and 6 a.m.; muted Facebook and Instagram notifications during school hours; and a restriction from seeing the number of likes and reactions on Facebook and Instagram posts, both a teen's own and those from others.

66. On Pinterest, parents can provide guidance on their teens' accounts by setting up a 4-digit passcode, which allows them to lock certain settings related to account management, privacy and data, and social permissions. Teen accounts also are private by default, meaning their accounts and profile information are not automatically discoverable; only the teen and anyone they invite to follow them can see the "pins" and boards they save. Pinterest also experimented with

[23] *See, e.g.*, Instagram, Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents (Sept. 17, 2024), https://perma.cc/8E8A-KNNM; Meta, We're Introducing New Built-In Restrictions for Instagram Teen Accounts, and Expanding to Facebook and Messenger (Apr. 8, 2025), https://perma.cc/6WDW-KPK2; Instagram, About Teen Accounts on Threads (2026), https://perma.cc/6NSK-3YT4.

usage reminders, in which a user who opens the Pinterest app during the school day is reminded to "put Pinterest down, pause notifications, and focus on school."[24]

67. Snapchat's "Family Center" allows parents to see which friends the teen has been recently communicating with on Snapchat, view their list of friends, restrict sensitive content, and report abuse.[25]

68. TikTok provides parents with a suite of controls through its "Family Pairing" feature. Parents and guardians can link their TikTok account to their teen's account and, among other things, set customized daily screen-time limits (including different limits for different days); review a dashboard showing their teen's time on TikTok; use "Time Away" to block access during designated periods such as school hours, family time, or bedtime; control when push notifications are muted; filter keywords and hashtags from supported feeds; restrict search; control whether the teen's account is private; manage direct messaging and who can comment on or otherwise interact with the teen's content; and block particular accounts. Family Pairing also gives parents visibility into certain aspects of their teen's activity, including accounts their teen follows, accounts following the teen, and blocked accounts. TikTok separately applies protections to teen accounts by default. Among other protections, accounts for users ages 13-15 are private by default and cannot send or receive direct messages; users under 18 receive a 60-minute daily screen-time limit by default; and TikTok disables push notifications overnight, beginning at 9 p.m. for users ages 13-15 and 10 p.m. for users ages 16-17.[26]

---

[24] Pinterest, Help Center, *Resources for parents and caregivers of teens* (2026), https://perma.cc/PY7D-2C7K.

[25] *See* Snapchat Support, *What is Family Center?*, https://perma.cc/8763-ACNF.

[26] TikTok, Help Center, *Family Pairing*, https://perma.cc/B538-J862.

69. YouTube offers a "supervised experience" for teens (separate from the supervised experience for minors younger than 13), allowing parents (1) to receive email notifications when a teen uploads a video or starts a livestream; (2) to gain insights into their teen's channel activity (such as uploads, comments, and subscriptions); and (3) to choose whether to link accounts between a parent and teen.[27] YouTube has also developed features and policies directed at promoting digital wellbeing among users.[28] YouTube also has a "Take a Break" feature that lets a user set a reminder to take a break while watching videos.[29] This feature pauses the user's video until they dismiss it or resume playing the video and is enabled by default for minors but is available to all users.

70. YouTube also offers a standalone "YouTube Kids" service that is a filtered version of YouTube built specifically to let children under the age of 13 explore age-appropriate content, and offers additional tools for parents and caregivers to moderate the content children see.[30] YouTube Kids features a curated selection of age-appropriate content. In addition to other tools, it also offers a built-in timer to let parents or caregivers, at their discretion, "limit screen time by telling kids when it's time to stop watching."[31] Parents can manage these tools and settings across devices from their Family Link account, available via both web browser and app.[32]

---

[27] YouTube, The YouTube your kids and teens love, with the protections you want, https://perma.cc/7YZ6-KR82.

[28] *Id.*

[29] *See* YouTube Help, Take a Break Reminder, https://perma.cc/RCK6-PUYV.

[30] *See* YouTube Kids, *A safer online experience for kids*, https://perma.cc/YZA5-BMM6.

[31] *See* YouTube For Families Help, *Limit screen time on YouTube Kids* (2026), https://perma.cc/BPC9-JAZH.

[32] *See* Google Family Link, Help keep your family safer online, https://perma.cc/HQS4-L2TV.

71. NetChoice members also restrict communications between adults and teens on their services, if they allow such messaging at all.

72. On Facebook, Instagram, and Threads, Meta restricts adults 18 and older from starting private chats with teens they are not connected to. By default, teens on Instagram can only receive messages from accounts they follow or have previously connected with; similarly, only friends or other connections can chat with teens on Facebook. Moreover, Instagram encourages teens via prompts and safety notices to be cautious in conversations with adults they are already connected to.[33]

73. Snapchat only allows minors to exchange messages with their friends on Snapchat or with people in their phone contact book. And Snapchat does not recommend minors as suggested friends unless the person is already in their phone contacts or shares mutual friends.

74. TikTok bans users under age 16 from sending or receiving direct messages, and it allows parents and guardians of 16- to 17-year-old users to restrict who can send messages to their teen, or to turn off direct messaging completely through its family pairing feature. For 16- and 17-year-olds, TikTok also turns off direct messaging by default.[34]

75. Some NetChoice members also restrict adults who have been exhibiting potentially suspicious behavior. For example, Meta has developed technology to identify and automatically disable accounts if they exhibit a certain number of the 60+ signals Meta monitors for potentially

[33] *See, e.g.*, Instagram, Help Center, *About Instagram Teen Accounts*, https://perma.cc/4THZ-W3RG; Meta, *Facebook and Messenger Teen Accounts: How Built-in Protections Help Keep Your Teen Safe*, https://perma.cc/GEJ8-QJGC.

[34] *See* TikTok, Safety Center, *Guardian's Guide* (Feb. 6, 2026), https://perma.cc/65G7-2UHT.

suspicious behavior, such as if a teen account blocks or reports an adult, or if someone repeatedly searches for terms that may suggest suspicious behavior.

76. All NetChoice members prohibit minors under 13 from unsupervised access to their main services. Some NetChoice members offer separate experiences for users under 13 with heightened protections geared for that age group. For example, TikTok offers a separate experience specifically designed for users under 13 that has heightened protections and that does not offer the ability to post, communicate with others, maintain a shareable profile, or have followers. Amazon offers Kids tablets that provide a child-friendly experience with parental controls that allow parents to manage their child's time online (*e.g.*, only enabling games after 30 minutes of reading time); an associated subscription (Kids+) provides kids access to a curated set of books, games, videos, and audiobooks. Services like Prime Video and Audible offer Kids profiles that provide content and an experience tailored to younger audiences. And YouTube offers two services (YouTube Kids and a "Supervised Experience" on YouTube) for minors younger than 13 with parental consent.[35] These services allow parents to select content settings, set screen time limits, and otherwise oversee their children's use of the services.

77. **NetChoice members' dedication to beneficial user experiences and user security.** NetChoice's members expend vast resources to improve their services and self-regulate the third-party speech disseminated on their websites to best ensure that it is appropriate for the community of users they seek to foster, especially minors.[36] "Facebook and YouTube" "cull and

[35] *See* YouTube For Families Help, *Important info for parents about YouTube kids* (2026), https://perma.cc/G6VY-T29E; YouTube Help, *What is a supervised kid account on YouTube?* (2026), https://perma.cc/X5K8-X8MQ.

[36] *See* Malena Dailey, *By The Numbers: What Content Social Media Removes And Why* 13 (2021), https://perma.cc/BN2E-768V.

organize uploaded posts" to conform with those platforms' "content-moderation policies," which "lead [them] to remove, disfavor, or label various posts based on their content." *Moody*, 603 U.S. at 719-20. Other NetChoice member websites enforce similar policies. They restrict the publication of harmful speech, such as violent and sexual content, bullying, harassment, and content that encourages body shaming or eating disorders. *See, e.g.*, *id.* at 735 (discussing policies about "hate speech, violent or graphic content, child safety"). In addition, many covered websites promote positive and age-appropriate speech, such as content that encourages a healthy self-image.

VERMONT'S AGE-APPROPRIATE DESIGN CODE ACT

78. The Vermont Legislature passed the Act, S.69, on May 29, 2025. It became law after Governor Phil Scott signed it on June 12, 2025, and it takes effect for covered websites on January 1, 2027.

79. The Act purports to regulate data. In fact, it sweepingly censors speech, targeting publishers like "social media platforms" while exempting the most sensitive data controllers (like financial institutions and medical providers), along with preferred speakers like "government entities" and "journalists."

80. Governor Scott recognized the likely constitutional challenge to the Act but expressed "hope[]" that the Act's delayed implementation would "allow enough time to provide clarity" presumably through the Attorney General's rulemaking authority and to "change the law if necessary."[37] On October 19, 2026—less than three months before the Act takes effect and more than 16 months after enactment—the Attorney General published the final rules (which are confusingly called "proposed" final rules). But instead of providing clarity or mitigating the Act's

[37] *See* Press Release, *Action Taken by Governor Phil Scott on Legislation*, Office of Governor Phil Scott (June 12, 2025), https://perma.cc/TJR3-AC95; §§ 2449f(b), 2449g(b), 2449h (directing and authorizing promulgation of rules).

constitutional defects, the final rules create further ambiguity and confirm that the Act broadly censors protected speech.[38]

81. **Coverage criteria and relevant definitions.** The Act's coverage is defined by a byzantine set of definitions and exclusions that, taken together, target virtually every expressive, communicative, or informational website with subject matter of potential interest to minors while carving out preferred speakers, preferred content, and non-expressive services (like banks, medical providers, and insurance companies) that may store substantial quantities of sensitive personal information but do not transmit ideas and foster communication.

82. Online services are presumptively "covered" by the Act if they (1) conduct business in Vermont, (2) collect "personal data" from users, (3) determine the purposes and means of processing that data, (4) provide "online products, services or features [that] are reasonably likely to be accessed by a minor," and (5) generate a majority of their annual revenue from online services. § 2449a(10).

83. "Online service, product, or feature" means a "digital product that is accessible to the public via the internet, including a website or application[.]" § 2449a(20).

84. But the Act excludes any "entity whose primary purpose is journalism," § 2449b(5), defined to mean "investigating" or "distributing" news or events that the State deems to be of "public interest." 12 V.S.A. § 1615(a)(2). "Public interest" is not defined.

85. The Act also exempts "government" speakers, banks, insurers, financial institutions, "protected health information," public health information, specified "research"

[38] *See* Proposed Rule: Prohibited Data and Design Practices (Office of Vermont Attorney General Oct. 19, 2026), https://perma.cc/GU4C-4ELG ("Data & Design Rule") (attached as Ex. A); Proposed Rule: Age Assurance Privacy (Office of Vermont Attorney General Oct. 19, 2026), https://perma.cc/GU4C-4ELG ("Age Assurance Rule") (attached as Ex. B).

activities, telecommunications services, broadband services, and the "sale, delivery, or use of a physical product," even if sold online. §§ 2449b(1)-(4), (6), 2449a(20). And because the primary services supplied by many other e-commerce websites are offline services that do not fall within the Act's definition of "digital products," the Act's definitions also appear to exclude, for example, rideshare services like Uber and Lyft (offline transportation), Vrbo (offline lodging), and SeatGeek (tickets to live events).

86. As a result, the Act regulates predominantly expressive, informational, educational, and communicative websites whose coverage hinges on whether they are "reasonably likely to be accessed by a minor." § 2449a(10).

87. "Reasonably likely to be accessed" means an "online service, product or feature" with one of the following indicators:

> (A) the online service, product, or feature is directed to children, as defined by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 and the Federal Trade Commission rules implementing that Act;
>
> (B) the online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by an audience that is composed of at least two percent minors two through 17 years of age;
>
> (C) the audience of the online service, product, or feature is determined, based on internal company research, to be composed of at least two percent minors two through 17 years of age; or
>
> (D) the covered business knew or should have known that at least two percent of the audience of the online service, product, or feature includes minors two through 17 years of age, provided that, in making this assessment, the business shall not collect or process any personal data that is not reasonably necessary to provide an online service, product, or feature with which a minor is actively and knowingly engaged.

§ 2449a(26).

88. "Minor" means an individual under 18 years of age, whether or not they are a Vermont resident. § 2449a(19). So websites are classified as "covered" based on the number of minor users they have anywhere in the world, not necessarily in Vermont.

89. A "covered minor" is a "consumer" who "a covered business actually knows is a minor or labels as a minor pursuant to age assurance methods in rules adopted by the Attorney General." § 2449a(12).

90. A "consumer" is an "individual who is a resident of the state," but does not include an individual acting in a commercial or employment context or on behalf of a business or government entity. *See* § 2449a(9).

91. **Age assurance.** The Act's definition of a "covered minor" includes a user who "a covered business actually knows is a minor or labels as a minor pursuant to age assurance methods in rules adopted by the Attorney General." § 2449a(12). "Age assurance" refers to "a range of methods used to determine, estimate, or communicate the age or an age range of an online user." § 2449a(2).

92. The Attorney General's recently promulgated Age Assurance Rule assumes that covered websites are required to use age assurance but does not specify when such age assurance is required, providing only that covered businesses "shall implement proportionate age assurance measures where age assurance is reasonably necessary to comply with any applicable obligation" under the Act. Age Assurance Rule at 1.

93. The Rule defines "proportionate age assurance" as "an age assurance process or technique selected in light of the applicable statutory obligation, the reasonably necessary level of confidence, and the priority afforded to privacy and accessibility." *Id.* at 2-3. The Rule provides that "commercially reasonable and technically feasible" options may include self-declaration,

existing age signals, tokens, and estimation, but the Rule's vague balancing criteria provide little guidance and no safe harbor if websites choose wrong.

94. The California Privacy Protection Agency recently confirmed that "there is currently no privacy-protective way to determine whether a consumer is a child."[39]

95. **Duty of care.** The Act provides that any "covered business that processes a covered minor's data in any capacity owes a minimum duty of care to the covered minor." § 2449c(a). The "minimum duty of care" means that "the use of the personal data of a covered minor and the design of an online service, product, or feature will not result in: (1) reasonably foreseeable emotional distress as defined in 13 V.S.A. § 1061(2) to a covered minor; (2) reasonably foreseeable compulsive use of the online service, product, or feature by a covered minor; or (3) discrimination against a covered minor based upon race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, religion, or national origin." § 2449c(b).

96. "Personal data" means "any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household," but it does not include "de-identified data or publicly available information." § 2449a(21). "De-identified data" means information that cannot be used to "infer information about" or be "linked to" an individual or device; the business "publicly commits" to never "attempt to reidentify the data" even for beneficial purposes; and the business contractually commits any recipients of the data, even those who simply assist in securing it, to comply *with the entire Act*. § 2449a(14). "Publicly available

[39] Memorandum from Maureen Mahoney, Deputy Dir. Pol'y & Legis., CAL. PRIV. PROT. AGENCY, to the Cal. Priv. Prot. Agency Bd. 5 (May 3, 2024), https://perma.cc/4HE3-AMBJ.

information" excludes (among other things) public information the Attorney General would consider a "consumer profile" or that is "available for sale"; any "inference" from such information; and some information a user posts to a website "available to all members of the public," if the user has "a reasonable expectation of privacy" in that information. § 2449a(25).

97. This broad definition of "personal data," which the exclusions do little to limit, reaches information collected and used far beyond Vermont's borders. It would cover information about a Vermont high school senior studying abroad or traveling outside the State. It would reach information linked to an out-of-state parent's device that a minor uses during occasional visits. It could also sweep in information about extended family members (located anywhere) who may post information linkable to a Vermont minor—for example, through family photographs or messages about the minor's activities and achievements. And it would encompass data incorporated into aggregate datasets used to improve a website's functionality or safety for users worldwide, even where those uses have no material connection to Vermont and pose no material risk to a Vermont resident's privacy.

98. The Act adopts the definition of "emotional distress" from 13 V.S.A. § 1061(2): "significant mental suffering or distress that may, but does not necessarily, require medical or other professional treatment or counseling." *See* § 2449c(b)(1). There is no clear line for determining when ordinary emotions and behaviors become unlawful. Although this term may have meaning when used to define *damages* arising from an intentional tort, there is no precedent for using it to define a standard of care in the first place, particularly across faceless internet transactions involving hundreds of thousands of users of varying ages, backgrounds, and sensitivities.

99. "Compulsive use" is defined as "the repetitive use of a covered business's service that materially disrupts one or more major life activities of a minor, including sleeping, eating,

learning, reading, concentrating, communicating, or working." § 2449a(8). Again, although the reference to "major life activities" may have discernible meaning in other contexts when paired with diagnosable physical and mental impairments, it has no concrete meaning applied to ordinary media engagement across hundreds of thousands of users and billions of posts of protected speech.

100. The recently promulgated regulations address the term "compulsive use" but do not clarify it. They reiterate that "[a] data processing or design practice leads to compulsive use where it causes or materially contributes to repetitive use that materially disrupts one or more major life activities of a covered minor." Data & Design Rule at 3. And they clarify only that the Attorney General "may consider all relevant facts" including:

> (1) Increases in time spent, frequency of use, or session length;
> (2) Repeated or habitual patterns of engagement;
> (3) The use of behavioral, psychological, or engagement-optimization techniques;
> (4) Internal testing, experimentation, A/B testing, product development, routinely collected metrics, or research concerning the practice's effects on engagement or disengagement;
> (5) Whether engagement occurs without a covered minor's express and unambiguous request; and
> (6) Whether the covered business's testing, analytics, or research demonstrates that the practice affects a covered minor's ability to disengage.

Data & Design Rule at 3. Each factor may be "considered as evidence," but none "standing alone" is dispositive, *id.* at 4. This is a textbook totality test that provides unfettered post hoc enforcement discretion to the Attorney General and requires businesses to guess how much "repetitive use" constitutes a "material disruption" to "major life activities" across users of different maturities, backgrounds, interests, and sensibilities.

101. The term "discrimination" is entirely undefined. There is no guidance on how websites must avoid it or even what it means in the context of the predominantly expressive services the Act regulates.

102. Although each of these terms is vague, what is clear is that even attempting to implement them requires websites to evaluate the content they disseminate and make value-laden judgments about it. Websites will face pressure to remove or deprioritize disturbing but valuable information—such as research on global warming and histories of the Holocaust. The same pressure will apply to speech a minor might enjoy *too much*—such as Bluey videos, Dog Man e-books, and Candy Crush—and online discourse that criticizes or angers State officials or addresses controversial topics around race, religion, or gender. And because each of these duties is owed to "a" covered minor, § 2449c(b)(1)-(3), they require websites to predict a minor's sensitivities and thus to analyze data the Act elsewhere restricts. *See* § 2449f(a).

103. In an apparent attempt to insulate the law from legal challenge, the Act includes a series of savings clauses. These provide that the "content of the media viewed by a covered minor shall not establish emotional distress, compulsive use, or discrimination," § 2449c(c); that the duty of care does not "require a covered business to prevent or preclude a covered minor from accessing or viewing any piece of media or category of media," § 2449c(d); and that the Act shall not "be interpreted or construed to . . . prevent or preclude any covered minor from deliberately or independently searching for, or specifically requesting, any media." § 2449i(2).

104. But nowhere does the Act suggest that websites can comply with the duty of care (or the Act's other provisions) while remaining content-agnostic, nor is it clear how that would be possible. Even if the content actually "viewed by" a covered minor does not itself "establish" the specified harms, § 2449c(c), it would be impossible to determine whether a service's design and

use of data will foreseeably "result in" compulsive use, emotional distress, or discrimination without considering the nature of the content published.

105. Likewise, although the Act permits minors to "independently" and "deliberately" view particular "pieces" or "categories" of media, §§ 2449c(d), 2449i(2), it does not say how websites can determine whether such viewing is "independent[]" and "deliberate[]."

106. In any event, the Act notably does not disclaim requiring more systemic forms of content-oriented adjustments, such as redesigning algorithms to downrank, deprioritize, decline to promote, or publish less of certain content, or to adjust the overall mix of content to be less engaging or potentially upsetting in any way. These forms of content-based burdens unquestionably require covered websites to make judgments about "the effect of the subject matter on young viewers," just as much as content-based bans. *Playboy Ent. Grp.*, 529 U.S. at 811-12.

107. **Monitoring and filtering defaults (§ 2449d).** The Act also categorically restricts disseminating minors' "social media" unless the minor has "expressly and unambiguously" allowed a "specific known adult" to view the content or "chosen to make [it] public." § 2449d(a)(1). The Act calls these "default privacy settings," but they restrict speech. Websites must monitor what speech minor users publish on their social media accounts, and then, by default, filter and suppress that information to prevent a "known adult user" from viewing or engaging with it. *Id.*

108. These default restrictions apply to the following speech and information on "social media": (A) "the existence of [a] covered minor's account"; (B) "media created or posted by the covered minor"; (C) "like[s]," "comment[s]," and "feedback" of adults about such media or posts; (D) "direct messaging" between minors and adults; (E) posts and media that might reveal the minor's "location"; (F) "the users connected to the covered minor"; and (G) "search engine

indexing of the covered minor's account profile." § 2449d(a)(1)(A)-(G). Services also must configure default settings to prohibit "sending push notifications to the covered minors." § 2449d(a)(1)(H).

109. Many NetChoice members already provide similar controls and default settings for identified minors, but the Act mandates them and pairs them with a gag rule that prevents "request[ing] or prompt[ing] a covered minor to make their privacy settings less protective, unless the change is strictly necessary for the covered minor to access a service or feature they have expressly and unambiguously requested." § 2449d(a)(2)(B).

110. These restrictions would impede: (1) a 17-year-old from using social media to speak out on issues of public importance; (2) a parent from posting a family photograph with the caption "Aloha from Honolulu!" or "Dinner at the Hard Rock Café!"; (3) a sister in college from using social media to find a younger sibling in high school; and (4) even classmates in the same high school class from communicating if one has turned 18 and the other has not.

111. **Notification restrictions.** The Act requires all "push notifications" to minors to be disabled by default and prohibits them between midnight and 6:00 a.m. §§ 2449d(a)(1)(H), 2449f(a)(5). The Data & Design Rule further prohibits *all* notifications that, in the Attorney General's view, "lead[] to compulsive use or subvert[] or impair[] a covered minor's autonomy, decision making, or choice." Data & Design Rule at 6. "Compulsive use," in turn, has no concrete definition and instead is based on a multi-factor totality test that considers commonplace attributes of speech, such as "patterns of engagement" and "[w]hether engagement occurs without a covered minor's express and unambiguous request." *Id.* at 3. These prohibited notifications might communicate that a political candidate has begun a livestream, an artist has announced a concert, the user's high school has implemented a snow day, or a family member has sent an urgent

message. The restrictions will limit when, how often, and whether protected expression reaches willing listeners.

112. **Prohibited "data" and "design" practices (§ 2449f).** The Act imposes strict prohibitions on the collection and use of a covered minor's personal data. A covered business may not (1) "collect, sell, share, or retain any personal data of a covered minor that is not necessary to provide an online service, product, or feature with which the covered minor is actively and knowingly engaged"; (2) "use previously collected personal data of a covered minor for any purpose other than a purpose for which the personal data was collected, unless necessary to comply with any obligation under this chapter"; or (3) "permit any individual, including a parent or guardian of a covered minor, to monitor the online activity of a covered minor or to track the location of the covered minor without providing a conspicuous signal to the covered minor when the covered minor is being monitored or tracked." § 2449f(a)(1)-(3).

113. The Act provides no definition of when data is "necessary" to "provide an online service, product, or feature," or when a minor is "actively and knowingly engaged" with a service or feature. § 2449f(a)(1). But the Act makes clear that using data to "select, recommend, or prioritize media" is not necessary and therefore is prohibited unless such data consists of an "express and unambiguous" request to receive specific content. § 2449f(a)(4)(A). Aside from a minor's "express and unambiguous request," the only minor data a website can use is "user-selected privacy or accessibility settings" or "a search query . . . to select and prioritize media in response to the search." § 2449f(a)(4).

114. The Act further expands these prohibitions to "data processing or design practices that, in the opinion of the Attorney General, lead to compulsive use or subvert or impair user autonomy." § 2449f(b). According to the recently promulgated Rule, these practices include

"asymmetrical interfaces," "autoplay," "behavioral recommendation" systems, continuous media feeds, engagement-based notifications, "reinforcement mechanisms," and "social pressure" features. Data & Design Rule at 4-7. The Rule would define "subvert[ing] or impair[ing]" autonomy as any practice that "materially steers, pressures, manipulates, obstructs, or imposes asymmetrical friction in a manner that meaningfully impairs [a] covered minor's ability to make or effectuate a choice." *Id.* at 4.

115. Although the precise meaning of these terms is vague and inherently unclear, what is clear is that they will block minors' access to protected expression. They will force covered services to turn off numerous commonplace editorial features for arranging and presenting protected speech, including systems that "select, recommend, or prioritize media" content and enable users to find speakers, topics, and communities. § 2449f(a)(4). For example, Spotify could not automatically queue up an Olivia Rodrigo song for a teenage listener after a Taylor Swift track; NetChoice member Netflix could not surface the documentary, David Attenborough: A Life on Our Planet, or even the next episode in a documentary series, like Our Universe; Libby could not recommend another science fiction novel like The Hunger Games.

116. **Compelled speech.** In addition to the above restrictions on speech, the Act also compels websites to speak on government-mandated topics that probe the very core of their expressive judgments.

117. The Act requires online publishers to publicly characterize and explain the internal mechanics of their editorial systems—including why they promote some speech over other speech, which audience signals influence that decision, and how those signals are weighted relative to other inputs. Covered services must explain the "purpose" of the content judgments they make through their content recommendation systems, §§ 2449a(4), 2449e(2), what factors their

algorithms are programmed to consider, how those factors are weighed, and how information minors have voluntarily shared influences the resulting editorial choice. § 2449e(3)(A)-(D).

118. The Act likewise compels explanations of every action the service undertakes that is informed by information received from, or linkable to, covered minors or devices. Again, the service must disclose the "purpose" for each action; the information received from minors to perform that action; how that information is used; each third party receiving the information; and the "purpose" of such receipt. § 2449e(4).

119. **Enforcement.** The Act makes every violation of its requirements, or their implementing rules, an "unfair and deceptive act in commerce" under the Vermont Consumer Protection Act. § 2449h(a). The Attorney General may conduct civil investigations, bring enforcement actions, promulgate rules, and enter assurances of discontinuance. § 2449h(b).

120. Penalties are severe. The Attorney General may seek temporary or permanent injunctions, restitution, investigative and litigation costs, dissolution of a Vermont corporation or revocation of a foreign corporation's authority to operate, and civil penalties of up to $10,000 for each violative "act." § 2458(a)-(b).

121. Neither the Act nor its implementing rules explain what constitutes one "act," when the regulated practices—recommendations, rankings, autoplay, notifications, displays, comments, and messages—occur millions or billions of times per day. Against that potentially enormous exposure, guessing wrong about any of the Act's requirements is prohibitively costly. NetChoice members cannot afford to learn the hard way which ordinary interactions the Attorney General considers unlawful. They will have to treat unidentified users as minors, distribute and recommend less speech, block lawful communications, or attempt to withdraw services from Vermont entirely.

CLAIMS

122. For the claims below, NetChoice raises facial challenges to the provisions in their entirety; facial challenges to the extent the Act applies to specific members' services and features and categorically similar services and features, *see John Doe No. 1 v. Reed*, 561 U.S. 186, 194 (2010); and as-applied challenges on behalf of covered members.

123. Each First and Fourteenth Amendment challenge set forth below raises the rights of NetChoice members; of those who use or could prospectively use NetChoice members' websites; and, where applicable, of NetChoice itself as a user of such services. *See, e.g.*, *Brown*, 564 U.S. at 803, 805 (affirming relief for trade association raising First Amendment rights of members' users to "access . . . violent video games"); *Am. Booksellers Ass'n*, 484 U.S. at 392-93 (holding that bookstore could raise the First Amendment rights of customers); *NetChoice, LLC v. Griffin* ("*Griffin I*"), 2023 WL 5660155, at *9-12 (W.D. Ark. Aug. 31, 2023).

COUNT I
42 U.S.C. § 1983
VIOLATION OF THE FIRST AMENDMENT TO THE U.S. CONSTITUTION
(§ 2449c (duty of care), § 2449d (monitoring and filtering), § 2449f ("data" and "design" prohibitions), § 2449g (age assurance) and accompanying regulations)

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

125. The First Amendment to the Constitution of the United States, as incorporated against the States by the Fourteenth Amendment, provides that a State "shall make no law . . . abridging the freedom of speech." U.S. Const. amend. I.

126. "Above all else," this "means that government generally has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *Barr v. Am. Ass'n of Pol. Consultants, Inc.*, 591 U.S. 610, 618 (2020) (cleaned up). This is true even for speech the government believes to be harmful or discriminatory. *See 303 Creative LLC v. Elenis*, 600 U.S. 570, 592 (2023). And "whatever the challenges of applying the Constitution to ever-advancing

technology, the basic principles of the First Amendment do not vary." *Moody*, 603 U.S. at 733 (cleaned up).

127. "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 extended First Amendment protection not just to the acts of speaking and publishing, but to "disseminat[ing]" speech, *303 Creative*, 600 U.S. at 594; "creating, distributing, [and] consuming" speech, *Brown*, 564 U.S. at 792 n.1; "access[ing]" expressive and informational "forums" like "social media," *Packingham*, 582 U.S. at 104-07; and making "expressive choices" about how to select and display speech and "how the display will be ordered and organized." *Moody*, 603 U.S. at 732, 740.

128. The First Amendment also protects the "use of . . . information" to inform speaking and publishing, including to make speech more "tailored" and "persuasive" to its recipients. *Sorrell*, 564 U.S. at 561, 570, 576; *see id.* at 570 ("Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs.").

129. Across all of these expressive domains, the Court has stressed that "it is not . . . the role of the State or its officials to prescribe what shall be offensive." *Masterpiece Cakeshop Ltd. v. Colo. C.R. Comm'n*, 584 U.S. 617, 638 (2018).

130. **The Act burdens protected expression.** The Act burdens and restricts speech, both as a whole and through its individual provisions.

131. The threshold coverage definitions of "covered business" and "online service, product, or feature" apply to predominantly expressive and informational activities that provide a "quintessential forum for the exercise of First Amendment rights," *Packingham*, 582 U.S. at 104,

such as social media, video streaming, audio streaming, search services,[40] e-books, and blogs. At the same time, these definitions carefully exclude businesses that do not facilitate speech and information, such as (1) the "sale . . . of a physical product," § 2449a(20); (2) offline services that may be transacted through websites but are not expressive or informational and do not constitute "digital product[s]," *id.*; and (3) other predominantly non-expressive services like financial and medical services, § 2449b(2), (6).

132. The Act's substantive provisions also target protected speech and information, such as the "personal data" that allows websites to moderate, curate, and deliver speech, §§ 2449a(21), 2449c, 2449f; the speech "created or posted by" a minor, § 2449d(a)(1)(B); "comment[s]" and other "feedback" on minors' posts, § 2449d(a)(1)(C); messaging, connections, profiles, and notifications, §§ 2449d(a)(1)(D)-(H), 2449f(a)(5); "recommendation system[s]" that present and curate speech, § 2449e(2)-(3); "media" such as "cat videos," § 2449f(a)(4); and the processes by which websites "select, recommend, or prioritize" speech, *id.*

133. The law's "design and data" provisions prohibit using a minor's "personal data" to "select, recommend, or prioritize media," subject to exceptions for a minor's express request, search queries, and user-selected privacy or accessibility settings. § 2449f(a)(4). The final rules significantly expand these restrictions by prohibiting using not only minors' personal data (as the Act defines it) but also their "behavioral data" and "inferred preferences" derived from the minor's personal or behavioral data to select, recommend, or rank media (subject to the law's exceptions). Data & Design Rule at 5. "Behavioral data" is broadly defined as any "activity, interactions, or

[40] *See, e.g.*, *Hopson v. Google, LLC*, 2023 WL 2733665, at *3 (W.D. Wis. Mar. 31, 2023) (confirming that search services are protected by the First Amendment).

engagement" with the platform. *Id.* at 1. This essentially results in a ban on most personalized feeds.

134. Similarly, the Act's "duty of care" burdens protected expression. By requiring that a website's "use" of the data of a covered minor and "design" not "result in" reasonably foreseeable "emotional distress," "compulsive use," or "discrimination," § 2449c(b), the duty of care regulates the very means by which websites select, arrange, and present third-party speech to their users. Those editorial choices are themselves protected expression. *See Moody*, 603 U.S. at 731 ("Deciding on the third-party speech that will be included in or excluded from a compilation—and then organizing and presenting the included items—is expressive activity of its own."). The duty further burdens covered services' independent right to transmit and receive information, and to disseminate speech. *See Sorrell*, 564 U.S. at 570.

135. The Attorney General's implementing regulations confirm that the Act targets expression. They directly target a minor's "engagement with" speech on a covered website, including "viewing history," "dwell time," "navigation patterns," and "notifications." Data & Design Rule at 1-2. They restrict websites from speaking, publishing, recommending, or disseminating protected speech to minor users unless the minor makes an "affirmatively initiated" and "[e]xpress and unambiguous request" for that speech. *Id.* at 1. And the regulations as a whole restrict expression and editorial practices that might "increase[] engagement" unless the Attorney General finds it to be "reasonably undertaken in the best interests of covered minors." *Id.* at 3.

136. These provisions—individually and as a whole—apply "to speakers engaged in online communication" and "target[] 'conduct with a significant expressive element'" with "the inevitable effect of singling out those engaged in expressive activity." *Cornelio v. Connecticut*, 32 F.4th 160, 169 (2d Cir. 2022) (quoting *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706-07 (1986)).

"That implicates the First Amendment[.]" *Id.* (citing *Minneapolis Star & Trib. Co. v. Minn. Comm'r of Revenue*, 460 U.S. 575, 592 (1983)). When a law imposes "special obligations" or "special burdens" on those engaged in speech, "heightened First Amendment scrutiny is demanded." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 641 (1994).

137. The Act as a whole also burdens speech by requiring covered websites to perform "age assurance" to permit users of all ages to access speech. § 2449g; *see Free Speech Coal., Inc. v. Paxton*, 606 U.S. 461, 476 (2025) (age-verification requirements to access "nonpornographic material" burden protected speech (quoting *Reno*, 521 U.S. at 877)).

138. **The Act is content-based, so strict scrutiny applies.** "Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve [a] compelling state interest[]." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015) (citing *R.A.V. v. City of St. Paul*, 505 U.S. 377, 395 (1992)).

139. Laws are content-based if they draw distinctions based "on the message a speaker conveys." *Id.* at 163. Even "facially content neutral" laws are content-based if they "cannot be justified without reference to the content of the regulated speech" or were adopted "because of disagreement with the message the speech conveys." *Id.* at 164 (cleaned up) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)). Speech regulations "cannot escape classification as facially content based simply by swapping an obvious subject-matter distinction for a 'function or purpose' proxy that achieves the same result." *City of Austin v. Reagan Nat'l Advert. of Austin, LLC*, 596 U.S. 61, 74 (2022).

140. The Supreme Court also is "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." *Nat'l Inst. of Fam. & Life Advocs. v. Becerra*, 585 U.S. 755, 777-78 (2018) (cleaned up).

141. The Act and its implementing regulations are content-based, and subject to strict scrutiny, for multiple reasons.

142. First, the Act's coverage criteria are both content-based and speaker-based. The Act excludes a preferred form of content—"news or information concerning issues or events of public interest"—from coverage through its exclusion for "journalism." 12 V.S.A. § 1615(a)(2); § 2449b(5); *see Nat'l Advert. Co. v. Town of Niagara*, 942 F.2d 145, 147 (2d Cir. 1991) (a law that "allow[s] exceptions for . . . news information . . . but not other types of noncommercial speech, [means that] the law contain[s] impermissible content-based restrictions"). And preferred speakers, like journalists, government entities, financial institutions, and insurers, are likewise excluded, as are specific topics, such as "health information" and specified "research." § 2449b(1)-(6). This special treatment for "insurers, researchers, journalists, [and] the State itself" enacts facially "content- and speaker-based restrictions on . . . information." *Sorrell*, 564 U.S. at 571, 573.

143. The Act's individual provisions also are content based.

144. The "duty of care," § 2449c, "deputizes covered businesses into serving as censors for the State," because "a business cannot assess the likelihood that a child will be exposed to harmful or [distressing] materials on its platform without first determining what constitutes harmful . . . material." *Bonta-AADC I*, 113 F.4th at 1118.

145. It is impossible to make predictions about the foreseeable effects of a website's "design" or use of data without also considering the content it publishes. Algebra tutorials are

unlikely to cause compulsive use (for most minors) but may cause emotional distress for a student struggling with math concepts. News about genocide or terrorist attacks or even politics may cause emotional distress but is unlikely to cause compulsive use. And for some minors, online chess will invite both compulsive use and emotional distress brought on by the inexhaustible intricacies of the game and the stress of high-performance competition. *See Griffin III*, 812 F. Supp. 3d at 922 (enjoining "reasonable care" requirement because "[a] law that prohibits platforms from pushing 'certain types of content' but allows them to push other types of content is a content-based law").

146. The implementing regulations also give the Attorney General express and largely unbounded authority to discriminate based on the content of speech: An increase in engagement will not be deemed "compulsive" if the Attorney General finds it to be "undertaken in the best interests of covered minors." Data & Design Rule at 3.

147. The fact that the Act's duty of care purports to regulate "design," "data," and the effects on minor users, rather than content, does not alter this analysis. A law tethered to the "direct impact that speech has on its listeners" is a content-based law. *Playboy Ent. Grp.*, 529 U.S. at 811 (citation omitted); *Boos v. Barry*, 485 U.S. 312, 321 (1988). And websites cannot evaluate the downstream impact of their "design" and data use on minors without also considering how the design "prioritizes . . . content." *See M.P. ex rel. Pinckney v. Meta Platforms Inc.*, 127 F.4th 516, 525 (4th Cir. 2025), *cert. denied*, 146 S. Ct. 287 (2025).

148. Nor is it material that the Act disclaims any intent to require a website to "prevent or preclude" a minor from viewing a particular "piece" of media or "category of media." § 2449c(d). The State may not "proceed upstream and dam the source" of speech by requiring websites to change the "design" and inputs for their content recommendation systems. *Buehrle v. City of Key West*, 813 F.3d 973, 977 (11th Cir. 2015).

149. The Act's monitoring and filtering requirements, § 2449d, also regulate speech on content-based grounds. Although many NetChoice members offer their own protections, the Act and implementing regulations displace those private choices with state-mandated restrictions on "media created or posted by" a minor, § 2449d(a)(1)(A)-(B); "like[s]," § 2449d(a)(1)(C); "connection[s]," "profile[s]," and "location," §§ 2449d(a)(1)(D)-(H), 2449f(a)(5); and any "request or prompt [to] a covered minor" to change these defaults, § 2449d(a)(2)(B), all of which are speaker-based or content-based criteria. As the Ninth Circuit has recognized, "regulation of like counts" and "feedback" restricts protected speech and demands strict scrutiny. *NetChoice, LLC v. Bonta*, 152 F.4th 1002, 1016 (9th Cir. 2025).

150. The Act's prohibitions on using data, including to "select, recommend, or prioritize" media, § 2449f(a)(4), or in ways that, "in the opinion of the Attorney General, lead to compulsive use or subvert or impair user autonomy," § 2449f(b), are content-based too. "[A] law that dictates how to curate or compile others' speech is generally a content-based regulation subject to strict scrutiny." *Volokh v. James*, 148 F.4th 71, 84 (2d Cir. 2025).

151. And strict scrutiny applies if there is "any 'indication that the statute was intended to suppress any ideas,'" *Turner*, 512 U.S. at 658 (citation omitted), an indication found throughout the Act and the Attorney General's regulations. Indeed, the regulations expressly require enforcement officials to consider (among other things) the "effects on covered minors" of the content a website publishes, whether that content might invite "repeated . . . engagement," whether such engagement is in the "best interests of covered minors," and whether the content might "influence[]" a minor's decision-making or be interpreted to impose "social pressure." Data & Design Rule at 2-6.

152. **Defendant cannot satisfy strict or intermediate scrutiny.** The State "bears the burden of proving the constitutionality of its actions." *FEC v. Cruz*, 596 U.S. 289, 305 (2022) (citation omitted).

153. Under strict scrutiny, the State must demonstrate that the Act is "the least restrictive means of achieving a compelling state interest." *Ams. for Prosperity Found. v. Bonta*, 594 U.S. 595, 607 (2021) (plurality opinion) (citation omitted). Strict scrutiny demands that "the curtailment of free speech must be actually necessary to the solution," and the State must "specifically identify" how the Act addresses an "actual problem in need of solving." *Brown*, 564 U.S. at 799 (cleaned up).

154. Under intermediate scrutiny, the State must establish that the Act advances "important governmental interests *unrelated to the suppression of free speech*" and does "not burden substantially more speech than necessary to further those interests." *Turner Broad. Sys., Inc. v. FCC* ("*Turner II*"), 520 U.S. 180, 189 (1997) (emphasis added).

155. Defendant cannot meet any level of First Amendment scrutiny.

156. Vermont's purposes for enacting the Act are impermissible under the First Amendment. The State's interest is not "unrelated to the suppression of free speech," *id.* at 189, as evidenced by its direct focus on the "impact that speech has on its listeners," *Boos*, 485 U.S. at 321, such as "emotional distress," "compulsive use," too much "engagement," and impacts on "decision making" or "choice." § 2449c; Data & Design Rule at 1-3. 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, 213-14 (1975). Where, as here, the "justification for the [restriction] is concern for the effect of the subject matter on young viewers," the restriction must satisfy strict scrutiny. *Playboy Ent. Grp.*, 529 U.S. at 811.

157. To the extent the State may invoke an interest in "privacy," the Act is "not drawn to serve that interest" when it "permits insurers, researchers, journalists, the State itself, and others to use [and collect minors'] information" without regulation. *Sorrell*, 564 U.S. at 572-73.

158. Nor is the Act tailored to an interest in privacy or any other non-speech interest. The Act is overinclusive because it governs many websites that do not pose any material risk of harm or privacy intrusion to minors (or even serve more than a tiny percentage of minors). It also applies to users who do not require or want the State's protection. "The State cannot force platforms to censor potentially sensitive, but protected, speech as to all users for the benefit of some subset of particularly susceptible users." *Griffin III*, 812 F. Supp. 3d at 922.

159. The Act also burdens substantially more speech than necessary. It sweeps in all manner of beneficial speech that poses no risk of harm to minors, including e-books, audiobooks, podcasts, music, educational websites, films, and blogs. And even as it requires websites to prevent harms, it eliminates their ability to tailor content to individual users, forcing blanket suppression rather than targeted protection.

160. The duty of care, § 2449c, is also ill-tailored. Because the duty is owed to "a" covered minor, § 2449c(b), a single minor's distress or "compulsive use" can trigger liability, forcing websites to calibrate their services for all users based on a conception of the most sensitive minor.

161. The Act is simultaneously underinclusive because it excludes from its coverage harms to children that might occur from exempt or offline activities, such as a data breach by a bank, medical provider, or government entity. Further, the Act allows minors to access even the most egregiously harmful content so long as the minor deliberately "search[es] for, or specifically

request[s]" that harmful content. § 2449i(2). "That is not how one addresses a serious social problem." *Brown*, 564 U.S. at 802.

162. "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"—which many already do; "(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-AADC I*, 113 F.4th at 1121; *see NetChoice v. Bonta* ("*Bonta-SB976*"), 761 F. Supp. 3d 1202, 1227 (N.D. Cal. 2024) (enjoining even content-neutral limits on "push notifications" because they would "restrict significant amounts of speech for little gain").

163. For all of these reasons and more, the Act fails any level of First Amendment scrutiny. Unless declared invalid and enjoined, the Act's speech restrictions will deprive Plaintiff, Plaintiff's members, and internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and internet users.

164. The Act's speech restrictions, on their face and as applied to NetChoice members and their services that may be covered by the Act (Amazon, Audible, Automattic, Discord, Dreamwidth, Goodreads, Google, IMDb, Meta, Netflix, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, X, and YouTube), should be declared unconstitutional, and their enforcement enjoined, as they threaten Plaintiff and its members with irreparable injury for which there is no adequate remedy at law.

COUNT II
42 U.S.C. § 1983
VIOLATION OF THE FIRST AMENDMENT TO THE U.S. CONSTITUTION
(§ 2449e (compelled "transparency"))

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

166. The freedoms protected by the First Amendment include not only the right to speak freely but also "the right to refrain from speaking at all." *Wooley*, 430 U.S. at 714. "The right to speak and the right to refrain from speaking are complementary components of the broader concept of 'individual freedom of mind.'" *Id.* (quoting *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 637 (1943)); *see also Riley*, 487 U.S. at 796-97 (First Amendment protects against "compelled speech and compelled silence"); *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 256 (1974) (statute "[c]ompelling editors or publishers to publish that which reason tells them should not be published" violated the First Amendment (cleaned up)); *Chiles v. Salazar*, 607 U.S. 627, 640 (2026) (reaffirming that "[i]n this Nation, no official—'high or petty'—may command our tongues or silence our voices" (citation omitted)).

167. Accordingly, the government cannot "compel a person to speak its message when he would prefer to remain silent" or "force an individual to include other ideas with his own speech that he would prefer not to include." *303 Creative*, 600 U.S. at 586.

168. "[T]his general rule, that the speaker has the right to tailor the speech, applies not only to expressions of value, opinion, or endorsement, but equally to statements of fact the speaker would rather avoid." *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos., Inc.*, 515 U.S. 557, 573 (1995); *see also McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995); *Riley*, 487 U.S. at 797-98.

169. A law "mandating speech that a speaker would not otherwise make" is a "content-based regulation of speech" because it "alters the content of the speech," *Riley*, 487 U.S. at 795, and is presumptively subject to strict scrutiny.

170. This provision is also subject to strict scrutiny because the Act's coverage definition is content-based.

171. The Act compels websites to speak "prominently" about their editorial decisions, including: (1) their "community standards"; (2) "the purpose of each algorithmic recommendation system" they use; (3) the "inputs" to those systems and how "each input" is "measured or determined," "weighed relative to the other inputs," and "influences the recommendation"; and (4) the "purpose" of "every feature of the service." § 2449e.

172. Such compelled "transparency" into the "reasons" for, and functioning of, a website's editorial "policies" cannot be squared with the First Amendment. *X Corp. v. Bonta*, 116 F.4th 888, 901-02 (9th Cir. 2024). "Requiring" a covered business "to disclose . . . its procedures with respect to [content recommendation systems] . . . would force that network to build and describe its framework for [curating content] around the *State's* definition, thereby burdening the networks' expressive activity of curating content." *Volokh*, 148 F.4th at 93.

173. The compelled speech requirements do not satisfy strict scrutiny, or any level of First Amendment scrutiny.

174. The Act's compelled speech requirements, on their face and as applied to NetChoice members and their services that may be covered by the Act (Amazon, Audible, Automattic, Discord, Dreamwidth, Goodreads, Google, Meta, Netflix, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, X, and YouTube), should be declared unconstitutional, and their enforcement enjoined, as they threaten Plaintiff's members with irreparable injury for which there is no adequate remedy at law.

COUNT III
42 U.S.C. § 1983
VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH AMENDMENTS TO THE U.S. CONSTITUTION
(§ 2449c (duty of care), § 2449d (monitoring and filtering), § 2449e (compelled "transparency"), § 2449f ("data" and "design" prohibitions) and accompanying regulations)

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

176. "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." *Fox Television Stations, Inc.*, 567 U.S. at 253. 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.

177. Where a law "threatens to inhibit the exercise of constitutionally protected rights"—for instance, if it "interferes with the right of free speech"—then "a more stringent vagueness test should apply." *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 499 (1982). Otherwise, vague laws risk chilling would-be speakers by forcing them "to steer far wider of the unlawful zone" than they would "if the boundaries of the forbidden areas were clearly marked." *Baggett*, 377 U.S. at 372 (citation omitted). For similar reasons, the "general rule disfavoring facial vagueness challenges does not apply in the First Amendment context," particularly for overbroad laws that "reach[] a substantial amount of constitutionally protected conduct." *Farrell v. Burke*, 449 F.3d 470, 496 (2d Cir. 2006) (citations omitted).

178. The Act here raises so many "vagueness problems" that "[i]t is hard to know where to begin." *Carolina Youth Action Project v. Wilson*, 60 F.4th 770, 786 (4th Cir. 2023).

179. **Duty of care.** The Act provides that a covered business that "processes a covered minor's data in any capacity owes a minimum duty of care to [a] covered minor." § 2449c(a). Yet the statutory text offers no ascertainable standard of conduct other than what websites should have known about the effects of speech on listeners. This is a negligence standard, but the Supreme

Court has held that liability even for unprotected true threats cannot be based on negligence. *See Counterman v. Colorado*, 600 U.S. 66, 79-80 & n.5 (2023).

180. The Act also does not explain what type, or how much, care would satisfy a covered business's "minimum duty." Indeed, although framed as a "duty of care," the Act defines that duty by outcome rather than conduct: A website's data use and design must "not result" in the specified harms. § 2449c(b). A website thus remains exposed to liability if a single covered minor experiences foreseeable distress or compulsive use. Websites cannot know in advance what conduct will satisfy the Act.

181. Worse, the duty "must be assessed as to any single child" across varying sensitivities, ages, backgrounds, and maturity levels, thereby creating a "particularly high" risk of "subjective enforcement." *Bonta-AADC II*, 170 F.4th at 764-65 (affirming injunction as to similar duty under California Age-Appropriate Design Code Act); *NetChoice v. Griffin*, 831 F. Supp. 3d 816, 829-30 (W.D. Ark. 2026) (Arkansas duty of care provision prohibiting "practices to evoke addiction or compulsive behaviors" in minors was impermissibly vague).

182. The Attorney General's implementing regulations only exacerbate this vagueness, adopting new vague terms, such as "engagement optimization," "asymmetrical friction," "disengagement controls," and "best interests of covered minors," all of which reserve essentially unbounded authority to the Attorney General to adopt new interpretations and applications based on "all relevant facts and circumstances." Data & Design Rule at 1-5.

183. Together, these ambiguities create a one-way ratchet in favor of censorship. Speech must be suitable for the most sensitive users, yet covered services face no penalty for removing too much content or too many features. Unable to know in advance what the State will deem "reasonably foreseeable" harm or precautions it will consider reasonable, or how any particular

minor will react, covered websites will have every incentive to suppress more speech to avoid liability—reducing internet audiences, including teens, to "reading only what is fit for children." *Butler v. Michigan*, 352 U.S. 380, 383 (1957).

184. **Emotional distress.** The Act defines "emotional distress" as "significant mental suffering or distress that may, but does not necessarily, require medical or other professional treatment or counseling." § 2449c(b)(1); 13 V.S.A. § 1061(2).

185. This definition provides no guidance as to how the "use of the personal data of a covered minor" or the "design of an online service" would lead to such "significant mental suffering or distress," or whether to apply the standard to minors generally or minors in different age ranges. The "definition of 'minor' . . . creates vagueness" because materials that might be distressing "for a three-year-old" would have different effects for a "16-year-old" and websites "cannot tell which of these minors should be considered." *ACLU v. Mukasey*, 534 F.3d 181, 205 (3d Cir. 2008). And even minors of the same age have differing sensibilities, which makes this standard fundamentally "unascertainable" because a "violation entirely depends upon the sensitivities of some unspecified user and a judge or jury's determination about what the platform 'should have known' about those sensitivities." *Griffin III*, 812 F. Supp. 3d at 928; *Bonta-AADC II*, 170 F.4th at 764-65 (invalidating California AADC's prohibition on data uses); *cf. Hustler Mag., Inc. v. Falwell*, 485 U.S. 46, 55 (1988) ("'outrageousness' . . . has an inherent subjectiveness about it").

186. **Compulsive use.** "Compulsive use" means "the repetitive use of a covered business's service that materially disrupts one or more major life activities of a minor, including sleeping, eating, learning, reading, concentrating, communicating, or working." § 2449a(8). The Act and implementing regulations do not say how much use is "repetitive"—does a mere 5, 15, or

30 minutes per day count? When does that use "materially disrupt[]" the specified "life activities," particularly where the impairment is not connected to any discernible physical or mental impairment (as in the disability context)? Is it enough that the user prefers to watch an online movie rather than go to sleep or do homework? If not, when do such ordinary behaviors cross the line to "compulsive"? What other "life activities" count as "major"? Who is the "minor" at issue? And who decides?

187. **Discrimination.** The duty of care also requires that a website's use of data and design "will not result in . . . discrimination against a covered minor" based on enumerated characteristics. § 2449c(b)(3). But neither the Act nor the regulations explain how a website's "design" could "result in" discrimination, or how websites should treat third-party speech that a minor or the Attorney General might view as discriminatory. This is precisely the kind of standardless prohibition that invites "seriously discriminatory enforcement." *Williams*, 553 U.S. at 304.

188. **"Personal data."** The term "personal data" is itself a vague term, rendering vague all of the statutory provisions that rely on it. The Act defines "personal data" as "any information" that is "linked or reasonably linkable, alone or in combination with other information" to an individual or their device. § 2449a(21)(A) (emphasis added). The Act does not define "linkable" or "other information." Nor does it explain how a covered business should assess whether particular "information" could "in combination with other information" be "linkable" to an "identified . . . individual[]" (or what degree of "linkability" is required). Indeed, this provision could be read in staggeringly broad fashion—to apply to practically any information created by an individual—given that nearly any information is potentially "linkable" to an individual "in

combination with other information" (such as the individual's name). *See Duhe v. City of Little Rock*, 902 F.3d 858, 864 (8th Cir. 2018).

189. **Reasonably likely to be accessed.** A website is "covered" by the Act if it is "reasonably likely to be accessed" by a minor, meaning it is "routinely accessed by an audience" composed of at least two percent minors, or the business "knew *or should have known* that at least two percent of [its] audience . . . includes minors." § 2449a(26). The Act does not define "routinely accessed" or "audience," again leaving websites guessing as to how frequently such access must occur (weekly? monthly?) and who counts as the website's "audience," whether all users and casual visitors, all routine users, all accountholders, or something else. The Act likewise supplies no time period in which the two percent threshold should be assessed (or reassessed) or grace period after such threshold is reached or as audiences fluctuate.

190. The constructive-knowledge criterion and data restrictions compound the ambiguity. The Attorney General may first choose what the undefined threshold means and *then* decide when a business *should have* anticipated that interpretation. And even while holding websites responsible for what they "should have known" about a tiny fraction of users, the Act *limits* websites' ability to discern or infer user age through its mandate "not [to] collect or process any personal data that is not reasonably necessary to provide" the service. § 2449a(26)(D). Yet because "personal data" includes "inferences," "assumptions," and "conclusions" about a minor, websites are held responsible for what they "should have known" while actively prohibited from drawing the "inferences" that would allow them to know it. 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. **Journalism exclusion.** The Act's ill-defined "journalism" exclusion adds further uncertainty by making coverage turn on an entity's "primary purpose" and workforce composition without defining those terms or explaining how they apply to mixed-purpose services that publish original journalism alongside commentary, social features, entertainment, or user-generated content. Nor does the Act define whose assessment of "primary purpose" matters—the website's, users', or someone else's. *See Griffin II*, 2025 WL 978607, at *15-16.

192. **Covered minor.** The Act's definition of "covered minor"—a term that appears throughout the Act's substantive provisions—is similarly vague because websites are left to guess at whether and when they must perform age assurance. Minors are "covered" if the website "labels [them] as a minor pursuant to age assurance methods in rules adopted by the Attorney General." § 2449a(12). But the Act does not explain when websites must perform such age assurance methods. Unhelpfully, the rule states that businesses must perform age assurance when "reasonably necessary," Age Assurance Rule at 1, without providing any inkling as to when such methods *are* reasonably necessary. And the rules, like the Act, simultaneously require the most "privacy-protective" age-assurance measures available and discourage websites from undertaking age assurance methods that require a business "to collect personal data where it can comply with [its] obligations by" simply "treating a user as a covered minor." *Id.* at 1-2. Yet a business could "treat[] a user as a covered minor" in virtually all cases, raising questions about when websites are even permitted to use personal data to conduct age assurance rather than reduce their entire user base to minors.

193. **"Necessary."** Many of the Act's requirements turn on whether using data is "necessary" or "strictly necessary" to deliver a service. *See* §§ 2449f(a)(1)-(2), 2449g(a)(1). Covered businesses have no way to know what will be deemed "necessary," let alone "strictly

necessary," because the answer to that question depends on how the service or feature is defined. For example, using data to personalize content is "necessary" to deliver the distinctive speech services that NetChoice members provide, including to publish age-appropriate content to minors, but the Act's text makes clear that Vermont does not share that assessment.

* * *

194. The Act's vague terms, separately and together, make it impossible for covered online services to understand their obligations and encourage "seriously discriminatory enforcement." *Williams*, 553 U.S. at 304. The State "cannot give the Judiciary uncut marble with instructions to chip away all that does not resemble David" while leaving covered services' users in Vermont "to bear constitutional deprivation in the meantime." *Griffin II,* 2025 WL 978607, at *17 (quoting *Percoco v. United States*, 598 U.S. 319, 337 (2023) (Gorsuch, J., concurring in the judgment)).

195. Unless declared invalid and enjoined, the Act's vague 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.

196. The Act on its face and as applied to NetChoice members and their services that may be covered by the Act (Amazon, Audible, Automattic, Discord, Dreamwidth, Goodreads, Google, IMDb, Meta, Netflix, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, X, and YouTube) should be declared unconstitutional, and its enforcement should be enjoined, as it threatens Plaintiff and its members with irreparable injury for which there is no adequate remedy at law.

COUNT IV
42 U.S.C. § 1983, 47 U.S.C. § 230
VIOLATION OF THE SUPREMACY CLAUSE OF THE U.S. CONSTITUTION
(§ 2449c (duty of care), § 2449d (monitoring and filtering requirements), § 2449e ("transparency"), § 2449f ("data" and "design" prohibitions) and accompanying regulations)

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

198. The Supremacy Clause provides that "[t]his Constitution, and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land . . . any Thing in the Constitution or Laws of any State to the Contrary notwithstanding." U.S. Const. art. VI, cl. 2.

199. Preemption derives from the Supremacy Clause, which "invalidates state laws that interfere with, or are contrary to federal law." *Hillsborough Cnty. v. Automated Med. Lab'ys, Inc.*, 471 U.S. 707, 712-13 (1985). Preemption arises when the application of state law would violate an "express preemption clause" of a federal statute, *Buono v. Tyco Fire Prods., LP*, 78 F.4th 490, 495 (2d Cir. 2023), and when a "state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *In re Methyl Tertiary Butyl Ether (MTBE) Prods. Liab. Litig.*, 725 F.3d 65, 97 (2d Cir. 2013) (quotation marks omitted).

200. In Section 230, Congress made it "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet[,] . . . *unfettered* by Federal or State regulation." 47 U.S.C. § 230(b) (emphasis added). Congress enacted this provision in recognition of the "staggering" amount of information communicated by online services, the "obvious chilling effect" of even the "specter" of liability in "an area of such prolific speech," and the infeasibility of screening "millions of postings for possible problems." *Force*, 934 F.3d at 63 (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997)).

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

202. These provisions bar laws that hold a website "liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content," *LeadClick Media*, 838 F.3d at 174, and how to "arrang[e] and distribut[e] third-party information." *Force*, 934 F.3d at 66. This includes when an "algorithm sorts, arranges, and distributes third-party content." *Doe 1 v. Twitter, Inc.*, 148 F.4th 635, 646 (9th Cir. 2025).

203. Multiple NetChoice members, including Amazon, Automattic, Discord, Dreamwidth, Goodreads, Google, IMDb, Meta, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, and X, operate "interactive computer service[s]" that disseminate "information provided by another information content provider." 47 U.S.C. § 230(c)(1), (f)(2). *See Force*, 934 F.3d at 64.

204. As to these members and any covered services, Section 230 bars the Act's provisions that impose liability based on traditional publishing functions.

205. Section 230 preempts, in whole or in part, the Act's "duty of care," § 2449c(a), because websites cannot know if they satisfy it without also considering how they "prioritize[] the dissemination of *one type of content over another*"—a traditional publishing function that Section 230 protects. *Pinckney*, 127 F.4th at 525 (emphasis added); *Doe 1 v. Twitter*, 148 F.4th at 646

(Section 230 bars laws "that 'attack the manner in which [a website] sorts, arranges, and distributes third-party content'").

206. Section 230 also preempts the monitoring, filtering, "data," and "design" provisions, which restrict: (1) the "display[]" of "media created or posted by" a minor, § 2449d(a)(1)(A)-(B); (2) "like[s]," "comment[s]," or other "feedback" on minors' posts, § 2449d(a)(1)(C); (3) messaging, connections, profiles, and notifications in connection with user-generated content, §§ 2449d(a)(1)(D)-(H), 2449f(a)(5); and (4) the use of minor-linked information to "select, recommend, or prioritize" the presentation of third-party speech, §§ 2449a(15), 2449f(a). *See Force*, 934 F.3d at 66 ("[A]rranging and distributing third-party information . . . is an essential result of publishing" that Section 230 protects); *Doe 1 v. Meta Platforms, Inc.*, 174 F.4th 1159, 1167-70 (9th Cir. 2026) (the "promotion of engagement-driven content through" a "personalized algorithm" is "publishing conduct" protected by Section 230); *Pinckney*, 127 F.4th at 526 ("acts of arranging and sorting content are integral to the function of publishing," even when done with data and "an algorithm").

207. Vermont attempted to avoid preemption under the Supremacy Clause by providing that "[n]othing in this subchapter shall be interpreted or construed to . . . impose liability in a manner that is inconsistent with 47 U.S.C. § 230." § 2449i(1). But this provision simply injects further incoherence into the Act. Section 230 provides that "*no liability may be imposed*" for protected publishing activity. 47 U.S.C. § 230(e)(3) (emphasis added). The Act imposes such liability. And where a savings clause would "nullify the 'clear and specific' substantive provisions of the" Act, *HIAS, Inc. v. Trump*, 985 F.3d 309, 325 (4th Cir. 2021), a "reviewing court must ignore [it] and read the [Act's] operative provision to mean what it says." *League of United Latin Am.*

Citizens v. Exec. Off. of the President, 780 F. Supp. 3d 135, 176 (D.D.C. 2025); *see also New York v. Trump*, 133 F.4th 51, 70-71 (1st Cir. 2025).

208. Unless declared preempted, the Act's regulation of online services will cause Plaintiff, its members, and internet users irreparable harm and violate federal law.

209. The Act on its face and as applied to NetChoice members and their services that may be covered by the Act (Amazon, Automattic, Discord, Dreamwidth, Goodreads, Google, IMDb, Meta, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, and X) should be declared preempted, and its enforcement should be enjoined as it threatens Plaintiff and its members with irreparable injury for which there is no adequate remedy at law.

COUNT V
42 U.S.C. § 1983, 15 U.S.C. §§ 6501-6506
VIOLATION OF THE SUPREMACY CLAUSE OF THE U.S. CONSTITUTION
(§ 2449d (monitoring and filtering requirements), § 2449f ("data" prohibitions) and accompanying regulations)

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

211. In COPPA, Congress created a nationwide regime to protect minors online while preserving the "extraordinary" benefits of the internet. *See* 144 Cong. Rec. S8482, S8482 (daily ed. July 7, 1998), 1998 WL 399521.

212. To achieve these dual aims, COPPA addresses the "collection, use, [and] disclosure" of data by any "online service" or "website" that operates "among the several States" and "collects or maintains personal information from or about" its "users" and "visitors." 15 U.S.C. §§ 6501(2), 6502(b)(1)(A)(ii).

213. Although Congress defined this threshold coverage broadly, Congress defined COPPA's regulatory requirements surgically, making nuanced judgments about how to protect minors without hampering the internet as a global medium. COPPA achieved "consensus" only after "revisions to [the] original bill that were worked out carefully" with "online industries" and

"first amendment organizations" to "preserve[] the interactivity" of the internet. 144 Cong. Rec. S11651, S11657 (daily ed. Oct. 7, 1998), 1998 WL 694765.

214. COPPA establishes a flexible notice-and-consent regime for websites "directed" to children or that have "actual knowledge" that particular users are children under 13. 15 U.S.C. § 6502(b)(1). Such websites must provide parents with notice and obtain consent to collect and use personal information. *Id.* § 6502(b)(1)(B)(ii). But COPPA does not require websites to disable or change their core services to accommodate non-consenting parents. Rather, where parents do not wish to consent, websites may "terminate service" to the child. *Id.* § 6502(b)(3).

215. To ensure federal uniformity, Congress adopted an express preemption provision, stating that no State may impose "liability for commercial activities or actions by [online services] in connection with an activity or action described in [COPPA] that is inconsistent with [COPPA's] treatment of those activities or actions." 15 U.S.C. § 6502(d). This broad language preempts any "state law that treats like conduct differently." *N.M. ex rel. Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1121 (D.N.M. 2020).

216. Congress also lodged implementation authority with the FTC, 15 U.S.C. §§ 6505, 6502(b)(2)(C), which has administered COPPA for nearly three decades with an eye to "maintaining children's access to the Internet, preserving the interactivity of the medium, and minimizing the potential burdens of compliance." COPPA Rule, 64 Fed. Reg. 59,888, 59,889 (Nov. 3, 1999). Last year, the FTC reaffirmed that commitment by carefully weighing the "benefits" of regulation against the "attendant burdens." COPPA Rule ("*2025 COPPA Rule*"), 90 Fed. Reg. 16,918, 16,928 (Apr. 22, 2025).

217. Vermont's Act regulates the same data processing activities as COPPA, and it treats those activities differently than COPPA in at least five ways.

218. **Conditions on data collection, processing, use, and sharing (§§ 2449c, 2449d, 2449f(a)).** COPPA *permits* websites to collect, process, use, "release," and make "publicly available" minors' "online contact information," "user name," "geolocation," and other information so long as (where applicable) they provide notice and obtain parental consent. 16 C.F.R. § 312.4(a), (c); *id.* § 312.2. Yet, even with parental consent, the Act *restricts* these same data activities, establishes "care" and "necessity" requirements, and expressly prohibits publication of contact information, location, and related data unless expressly requested by the minor.

219. **Personalization restrictions (§ 2449f(a)(4))**. COPPA permits websites to collect information "necessary to . . . *personalize the content on*, the website or online service" and conduct "passive tracking." *Id.* § 312.2 (emphasis added). The Act restricts using personal data of a minor to "select, recommend, or prioritize" content for a minor.

220. **"Design" practices (§ 2449f).** In its *2025 COPPA Rule*, the FTC specifically declined to adopt any prohibition of features that "encourage or prompt use of a website [or] . . . optimize user attention or maximize user engagement," including "notifications." COPPA Rule ("*2024 Proposed COPPA Rule*"), 89 Fed. Reg. 2034, 2045 (proposed Jan. 11, 2024). *2025 COPPA Rule*, 90 Fed. Reg. at 16,946 ("the Commission has decided not to adopt the proposed amendments"); 16 C.F.R. § 312.2. The Act and implementing regulations restrict such features and thus impose inconsistent treatment. *See, e.g.*, § 2449f(a)(4)-(5); Data & Design Rule at 1, 4-9.

221. **Age assurance (§ 2449a(12)).** The Act requires websites to use "age assurance methods" to "determine, estimate, or communicate" an age or age range before collecting or using personal data. COPPA, by contrast, only applies to users a website has "actual knowledge" are children, or to websites "directed to" such children. 16 C.F.R. § 312.2.

222. **Covered minors (§ 2449a(19)).** COPPA only regulates data collection and use for children under 13. *See* 15 U.S.C. § 6501(1). The Act regulates data collection and use for all minors "under 18 years of age."

223. For at least these reasons, the Act is preempted because it imposes liability for data practices in a manner "inconsistent" with the treatment of those activities under COPPA and frustrates Congress's objective of creating a uniform regime.

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

225. The Act on its face and as applied to NetChoice members and their services that may be covered by the Act (Amazon, Audible, Automattic, Discord, Dreamwidth, Goodreads, Google, IMDb, Meta, Netflix, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, X, and YouTube) should be declared preempted, and its enforcement should be enjoined, as it threatens Plaintiff and its members with irreparable injury for which there is no adequate remedy at law.

COUNT VI
42 U.S.C. § 1983
COMMERCE CLAUSE OF THE U.S. CONSTITUTION
(§§ 2449a-2449i and accompanying regulations)

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

227. The U.S. Constitution vests Congress with the power "[t]o regulate Commerce . . . among the several States." U.S. Const. art. I, § 8, cl. 3. This affirmative grant of power also includes a "negative command, known as the dormant Commerce Clause," under which states may not directly regulate out-of-state parties' out-of-state commerce, unduly burden interstate commerce, or discriminate against it. *Okla. Tax Comm'n v. Jefferson Lines, Inc.*, 514 U.S. 175, 179 (1995).

228. Although laws that regulate in-state conduct may pass muster despite out-of-state "effects," state laws that "directly regulate[]" purely out-of-state transactions are another matter. *Nat'l Pork Producers Council v. Ross*, 598 U.S. 356, 376 & n.1 (2023) (emphasis omitted); *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989) (state laws that "control conduct . . . wholly outside" the regulating state's jurisdiction are prohibited). "Because the internet does not recognize geographic boundaries, it is difficult, if not impossible, for a state to regulate internet activities without projecting its legislation into other States." *Am. Booksellers Found.*, 342 F.3d at 103 (cleaned up). Laws also violate the Commerce Clause if they impose burdens on interstate commerce that are "clearly excessive in relation to the putative local benefits." *See Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).

229. The Vermont Act directly regulates out-of-state conduct and imposes clearly excessive burdens that outweigh any Vermont-specific benefits.

230. As noted above, the Act's broad definition of "personal data" and narrow definitions of "de-identified data" and "publicly available information" ensure that the Act's regulation of data will have a global reach. Even if a website could accurately identify whether a user is legally a "Vermont resident," which is not possible, the Act does not confine its reach to transactions with residents actually located in the State of Vermont.

231. The Act's data restrictions directly regulate out-of-state conduct because they restrict any online activity anywhere so long as it is informed by data linkable to a device further linkable to a Vermont resident. That is true regardless of where the data is processed, where the covered minor is when the data is collected and used, whether the minor is the original source of that data, how much data is used and the volume of other data it may be aggregated with, and whether the use is made for general purposes (such as to improve services) or targeted to the

Vermont resident. *See* § 2449f (broadly prohibiting the collection, use, sale, sharing, or retention of data based solely on whether it is "linkable" to a Vermont resident's device without any other nexus to Vermont). This could include family members in other states (or around the world) and their devices and posts, a Vermont minor traveling for spring break, data originally collected when a Vermont minor lived in another state, and aggregated data sets used to improve a website's services but that do not meet the Act's stringent definition of de-identified data.

232. The Commerce Clause does not permit a state to control the flow and use of information anywhere in the world simply because that information can be traced back to a state, state resident, or a device owned by the family of a resident. If states could control information simply because it is "linkable" to someone in, or a device linkable to, their state, California could regulate photographs taken in Yosemite regardless of where those photographs may travel in interstate commerce. Texas could assert authority over photographs of the Empire State Building taken by a Coloradan simply because the camera belonged to a Texas resident. New Jersey could claim jurisdiction over the research of a Princeton academic—regardless of where that information may travel through the chain of commerce. But as courts have held, that is not the law—whether for speech, information, or physical products. *See Styczinski v. Arnold*, 46 F.4th 907, 913 (8th Cir. 2022) (law regulating a bullion "transaction anywhere in the world" with a Minnesota resident violated the Commerce Clause because a trader could "become subject to and violate Minnesota law without conducting a single transaction in Minnesota"); *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc) ("easily" invalidating law that regulated art sales by a California resident because it applied "even if the [art], the artist, and the buyer never traveled to, or had any connection with, California"); *Nat'l Shooting Sports Found. v. Bonta*, 718 F. Supp. 3d 1244, 1255-56 (S.D. Cal. 2024) (law violated the Commerce Clause where it regulated firearm

"transactions conducted [] entirely out of state—[where] the lawful participants never set foot in California").

233. The Act's "duty of care," "privacy" defaults, and data and design restrictions also impose burdens on interstate commerce that are clearly excessive relative to any local benefits. Online services operate in a national market reflecting the diverse and interstate nature of the customers they serve and the cross-border informational services they provide. *See, e.g.*, *United States v. MacEwan*, 445 F.3d 237, 244 (3d Cir. 2006) (once digital images "left the website server and entered the complex global data transmission system that is the Internet, the images were being transmitted in interstate commerce").

234. Even if it were possible for websites to develop state-specific "designs" of their services, with different rules for what user information could be collected and analyzed, when that information could be used, to whom it could be posted, and what harms and content should be avoided, such a regime would drastically impair the value of the internet, which derives its benefits from providing "relatively unlimited, low-cost capacity" for uniform cross-border "communication of all kinds." *Reno*, 521 U.S. at 870.

235. If every state were to adopt its own unique version of this Act's restrictions—including a state-specific duty of care, unique "design" requirements, granular default settings, and onerous restrictions on the use, presentation, and display of information—the information, contacts, content, and communications that online users see would depend on where they live. That in turn would fragment the internet—and interstate communication itself—along state lines. The prohibitive costs of navigating these divergent regulatory regimes would force thousands of smaller website operators, bloggers, and developers out of business, reduce the diversity of voices

and services available online, and radically alter the internet that undergirds our modern-day, global economy.

236. That is a textbook violation of the Commerce Clause.

237. The Act on its face and as applied to NetChoice, its members, and their covered services (Amazon, Audible, Automattic, Discord, Dreamwidth, Goodreads, Google, IMDb, Meta, Netflix, Pinterest, Reddit, Snap Inc., TikTok USDS Joint Venture LLC, Twitch, X, and YouTube) should be declared unconstitutional, and its enforcement should be enjoined, as it threatens Plaintiff and its members with irreparable injury for which there is no adequate remedy at law.

PRAYER FOR RELIEF

Plaintiff requests an order and judgment:

1. declaring that Vermont's Age-Appropriate Design Code Act is unlawful both on its face and as applied to Plaintiff's members and their covered services listed in each count;
2. declaring that the Act violates the First Amendment to the U.S. Constitution, as incorporated against the States by the Fourteenth Amendment;
3. declaring that the Act is void for vagueness under the First Amendment and the Due Process Clause of the Fourteenth Amendment to the U.S. Constitution;
4. declaring that the Act is preempted by 47 U.S.C. § 230;
5. declaring that the Act is preempted by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506;
6. declaring that the Act violates the Commerce Clause of the U.S. Constitution;
7. declaring that the unlawful portions of the Act are not severable from the rest of the Act;
8. entering judgment in favor of Plaintiff on each count;
9. enjoining Defendant and her agents, employees, and all persons acting under their direction or control from taking any action to enforce the challenged portions of the Act on their face and, at a minimum, against Plaintiff or its members and their covered services identified in each count;
10. 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

11. awarding Plaintiff all such other relief as the Court deems proper and just.

Dated: November 23, 2026

Respectfully submitted,

/s/ Matthew B. Byrne

Matthew B. Byrne
Gravel & Shea PC
76 St. Paul Street, 7th Floor
Burlington, VT 05402-0369
Telephone: (802) 658-0220
Fax: (802) 658-1456
mbyrne@gravelshea.com

Steven P. Lehotsky*
Jeremy E. Maltz*
Serena M. Orloff*
LEHOTSKY COHN LLP
200 Massachusetts Avenue, NW,
Suite 700
Washington, DC 20001
(512) 693-8350
steve@lehotskycohn.com
jeremy@lehotskycohn.com
serena@lehotskycohn.com

Meredith Pottorff*
Trey S. Campbell*
LEHOTSKY COHN LLP
700 Colorado Blvd., #407
Denver, CO 80206
(512) 693-8350
meredith@lehotskycohn.com
trey@lehotskycohn.com

**pro hac vice forthcoming*

Exhibit A

SUBJECT: CONSUMER PROTECTION –
PROHIBITED DATA AND DESIGN PRACTICES

ATTORNEY GENERAL – CONSUMER PROTECTION UNIT
ADOPTED PURSUANT TO 9 V.S.A. § 2449f
CONSUMER PROTECTION RULE ___
Effective date: January 1, 2027

CP ___ Definitions
CP ___ Applicability
CP ___ General Prohibition
CP ___ Foreseeability
CP ___ Compulsive Use
CP ___ Impairment of Autonomy
CP ___ Prohibited Practices
CP ___ Asymmetrical Interfaces
CP ___ Autoplay
CP ___ Behavioral Recommendation System
CP ___ Continuous Media Feeds
CP ___ Engagement-Based Notifications
CP ___ Push Notifications
CP ___ Reinforcement Mechanisms
CP ___ Social Pressure Features
CP ___ Illustrative Examples
CP ___ Circumvention
CP ___ Severability

CP ___ Definitions

(a) Terms used but not defined in this Rule have the meanings set forth in 9 V.S.A. § 2449a.

(b) "Behavioral data" means data reflecting a covered minor's activity, interactions, or engagement with an online service, product, or feature, including clicks, scrolls, dwell time, viewing history, and navigation patterns, but excluding preferences or characteristics inferred from such activity.

(c) "Engagement optimization" means techniques used to increase a covered minor's interaction, session duration, or frequency.

(d) "Express and unambiguous request" means a specific and contemporaneous request affirmatively initiated by a covered minor and not inferred from prior activity, behavioral data, or persistent interaction patterns.

(e) "Inferred preferences" means preferences, interests, or affinities predicted, derived, or estimated from a covered minor's personal data, behavioral data, prior activity, interactions, or engagement patterns.

(f) "Push notification" means any notification delivered to a covered minor outside active use of an online service, product, or feature.

CP Applicability

(a) This Rule applies to any covered business with respect to the design, development, and operation of any online service, product, or feature that is used by a covered minor.
(b) This Rule applies to a covered business with respect to a user who is a covered minor, as those terms are defined in 9 V.S.A. § 2449a. Nothing in this Rule shall be construed to alter the statutory standards governing when an online service, product, or feature is reasonably likely to be accessed by a minor or when a user is a covered minor.

CP General Prohibition

A covered business shall not implement data processing or design practices that lead to compulsive use or subvert or impair a covered minor's autonomy, decision making, or choice.

CP Foreseeability

(a) In determining whether a data processing or design practice leads to compulsive use or subverts or impairs a covered minor's autonomy, decision making, or choice, the Attorney General may consider evidence of the practice's actual or reasonably foreseeable effects on covered minors, based on all relevant facts and circumstances.

(b) Relevant evidence may include:

1. Internal testing, analytics, research, routinely collected metrics, or other evidence concerning the effects of the practice on covered minors;
2. Industry knowledge, guidance, standards, or commonly known effects associated with similar practices;
3. Prior similar practices or experiences demonstrating effects on covered minors;

4. Information available to the covered business concerning the effects of the practice before or after deployment or material modification; and
5. The nature, design, operation, and reasonably foreseeable effects of the practice, including any safeguards implemented to reduce compulsive use or impairment of autonomy.

(c) The factors in subsection (b) are evidentiary considerations relevant to determining whether a practice leads to compulsive use or subverts or impairs a covered minor's autonomy, decision making, or choice. This section does not establish an independent duty to conduct testing, perform a risk assessment, document an evaluation, or implement particular safeguards. A failure to undertake any such activity does not, standing alone, establish a violation of this Rule.

(d) An increase in engagement, session duration, or frequency of use, standing alone, does not establish compulsive use or impairment of autonomy. A practice does not violate this Rule solely because it incidentally increases engagement where its primary purpose and reasonably foreseeable effect are to enhance safety, accessibility, fraud prevention, security, or another function reasonably undertaken in the best interests of covered minors.

CP Compulsive Use

(a) A data processing or design practice leads to compulsive use where it causes or materially contributes to repetitive use that materially disrupts one or more major life activities of a covered minor, consistent with 9 V.S.A. § 2449a.

(b) In determining whether a data processing or design practice leads to compulsive use, the Attorney General may consider all relevant facts and circumstances, including:

1. Increases in time spent, frequency of use, or session length;
2. Repeated or habitual patterns of engagement;
3. The use of behavioral, psychological, or engagement-optimization techniques;
4. Internal testing, experimentation, A/B testing, product development, routinely collected metrics, or research concerning the practice's effects on engagement or disengagement;
5. Whether engagement occurs without a covered minor's express and unambiguous request; and
6. Whether the covered business's testing, analytics, or research demonstrates that the practice affects a covered minor's ability to disengage.

(c) Increased engagement, session duration, frequency of use, or re-engagement may be considered as evidence but does not, standing alone, establish compulsive use. No factor listed in subsection (b), standing alone, establishes a violation of this Rule.

CP ___ Impairment of Autonomy

(a) A data processing or design practice subverts or impairs a covered minor's autonomy, decision making, or choice where it materially steers, pressures, manipulates, obstructs, or imposes asymmetrical friction in a manner that meaningfully impairs the covered minor's ability to make or effectuate a choice.

(b) In determining whether a practice subverts or impairs autonomy, the Attorney General may consider:

1. Whether a covered minor is provided a clear, readily accessible, and substantially equivalent ability to decline, disengage from, or limit use of an online service, product, or feature;
2. Whether disengagement requires additional steps, effort, or time compared to continued engagement;
3. The clarity, timing, and visibility of a covered minor's controls; and
4. Whether a covered minor's decision-making is influenced without their awareness or intent.

(c) Differences in the number of steps, amount of effort, or time required to make or effectuate a choice may be considered as evidence but do not, standing alone, establish impairment of autonomy.

CP ___ Prohibited Practices

The following provisions identify data processing or design practices that, in the Attorney General's opinion, lead to compulsive use or subvert or impair a covered minor's autonomy, decision making, or choice. Except where a provision expressly implements a separate statutory prohibition, the requirements of this part shall be construed consistently with the standards set forth in CP ___ Compulsive Use and CP ___ Impairment of Autonomy. Examples in this Rule are illustrative and non-exhaustive; no example independently expands the operative prohibitions.

CP Asymmetrical Interfaces

(a) A covered business shall not design or deploy an interface that imposes asymmetrical friction in a manner that meaningfully impairs a covered minor's ability to decline, disengage from, or limit use of an online service, product, or feature.

(b) In determining whether an interface violates subsection (a), the Attorney General may consider whether the interface:

1. Hides, obscures, or makes exit or disengagement controls materially less accessible;
2. Requires materially greater steps, effort, or time to disengage than to continue engagement; or
3. Delays, obstructs, or otherwise interferes with a covered minor's ability to disengage.

(c) Differences in the number of steps, effort, or time required to disengage do not, standing alone, establish a violation of this section.

CP Autoplay

(a) A covered business shall not design or deploy an autoplay or auto-advancing media feature in a manner that leads to compulsive use or subverts or impairs a covered minor's autonomy, decision making, or choice.

(b) In determining whether a feature violates subsection (a), the Attorney General may consider whether it automatically initiates or advances media without a covered minor's direction, obscures a natural stopping point, or interferes with the covered minor's ability to stop or disengage.

(c) Automatic playback or advancement of media does not, standing alone, establish a violation of this section.

CP Behavioral Recommendation System

(a) A covered business shall not implement or deploy a system that uses personal data, behavioral data, or inferred preferences to select, recommend, rank, order, prioritize, or sequence media for a covered minor, except as permitted under 9 V.S.A. § 2449f(a)(4).

(b) In applying this section, the exceptions set forth in 9 V.S.A. § 2449f(a)(4), including media responsive to a covered minor’s express and unambiguous

request, privacy or accessibility settings, and search queries, shall be preserved.

CP Continuous Media Feeds

(a) A covered business shall not design or deploy a continuously loading or presenting media feed in a manner that leads to compulsive use or subverts or impairs a covered minor's autonomy, decision making, or choice.

(b) In determining whether a feed violates subsection (a), the Attorney General may consider whether the feed:

1. Automatically loads or continuously presents additional media without a discrete and intentional action by the covered minor beyond ordinary scrolling or navigation;
2. Removes, obscures, or materially diminishes natural stopping points; or
3. Interferes with the covered minor's ability to stop, decline additional media, or disengage.

(c) Continuous loading, scrolling, or navigation does not, standing alone, establish a violation of this section.

CP Engagement-Based Notifications

(a) A covered business shall not design, time, trigger, or deliver notifications using personal data, behavioral data, or inferred preferences in a manner that leads to compulsive use or subverts or impairs a covered minor's autonomy, decision making, or choice.

(b) In determining whether a notification practice violates subsection (a), the Attorney General may consider whether notifications:

1. Are triggered or timed based on a covered minor's prior activity, behavioral patterns, or inferred interests;
2. Repeatedly prompt a covered minor to resume or prolong use after disengagement;
3. Use urgency, social pressure, or behavioral prediction to encourage re-engagement; or
4. Interfere with the covered minor's ability to limit or disengage from the service.

(c) A notification does not violate this section solely because it informs a covered minor of new activity or media, responds to an express and unambiguous request, or provides transactional, safety, or account-related information.

CP Push Notifications

(a) A covered business shall not design, time, trigger, or deliver push notifications in a manner that leads to compulsive use or subverts or impairs a covered minor's autonomy, decision making, or choice.

(b) In determining whether a push-notification practice violates subsection (a), the Attorney General may consider whether the practice:

1. Uses a covered minor's personal data, behavioral data, or inferred preferences to optimize the timing or frequency of notifications for re-engagement;
2. Repeatedly prompts a covered minor to resume use after disengagement; or
3. Interferes with a covered minor's ability to limit notifications or disengage.

(c) Nothing in this section limits or modifies the prohibition in 9 V.S.A. § 2449f(a)(5) on sending push notifications to a covered minor between 12:00 midnight and 6:00 a.m.

CP Reinforcement Mechanisms

(a) A covered business shall not use the timing, triggering, or presentation of variable or intermittent rewards in a manner that leads to compulsive use or subverts or impairs a covered minor’s autonomy, decision making, or choice.

(b) A reward is not prohibited solely because it is variable or intermittent, including a score, level, achievement, badge, point, or other reward reflecting gameplay or completion of a user-selected activity.

CP Social Pressure Features

(a) A covered business shall not design or deploy a social-pressure feature in a manner that leads to compulsive use or materially impairs a covered minor's autonomy, decision making, or choice.

(b) In determining whether a feature violates subsection (a), the Attorney General may consider whether its design or operation:

1. Uses streaks, repeated prompts, or perceived obligations to pressure a covered minor to continue or resume use;
2. Creates artificial urgency or consequences for disengagement; or
3. Materially interferes with a covered minor's ability to decline, delay, or discontinue engagement.

(c) The presence of social interaction, popularity indicators, or information about other users' activity does not, standing alone, establish a violation of this section.

CP Circumvention

(a) A covered business shall not evade a prohibition of this Rule by modifying the design, implementation, timing, presentation, or technical operation of a data processing or design practice where the modified practice would itself violate an operative prohibition of this Rule.

(b) In determining whether a modified practice violates an operative prohibition of this Rule, the Attorney General may consider all relevant facts and circumstances, including:

1. Whether the modified practice causes or materially contributes to compulsive use;
2. Whether the modified practice materially steers, pressures, manipulates, obstructs, or imposes asymmetrical friction in a manner that meaningfully impairs a covered minor's ability to make or effectuate a choice;
3. Whether the modified practice achieves substantially the same prohibited effects through alternative design, technical, or operational means; and
4. Whether the modification changes the practice's form or delivery without materially changing its effects on covered minors.

(c) A practice does not violate this section solely because it resembles a prohibited practice, uses a similar technical mechanism, or produces increased engagement, session duration, or frequency of use. A violation must be established under an operative prohibition of this Rule.

CP Severability

If any provision of this Rule, or the application of any provision to any person or circumstance, is held invalid by a court of competent jurisdiction, the remaining provisions and applications shall remain in effect to the extent they can be given effect independently of the invalid provision or application.

Exhibit B

SUBJECT: CONSUMER PROTECTION –
AGE ASSURANCE PRIVACY

ATTORNEY GENERAL – CONSUMER PROTECTION UNIT
ADOPTED PURSUANT TO 9 V.S.A § 2449g
CONSUMER PROTECTION RULE __
Effective date: 1/1/2027

CP ___ Applicability
CP ___ Definitions
CP ___ Age Assurance Selection
CP ___ Graduated Escalation
CP ___ Accuracy and Error Evaluation
CP ___ Frequency and Reassessment
CP ___ Data Minimization in Age Assurance
CP ___ Linkability and Design
CP ___ Prohibited Uses, Retention, and Disclosure of Age Assurance Data
CP ___ Fallback and Accessibility
CP ___ Appeals Process
CP ___ Compliance and Oversight
CP ___ Illustrative Examples
CP ___ Severability

CP ___ Applicability

(a) This Rule governs the collection, use, processing, and deletion of personal data in age assurance processes or techniques used by covered businesses. This Rule does not mandate a particular technology or identity-based age verification method.

(b) This Rule applies where a covered business knows that a user is a covered minor as defined in 9 V.S.A. § 2449a. Nothing in this Rule alters the statutory standards governing when an online service, product, or feature is reasonably likely to be accessed by a minor or when a user is a covered minor.

(c) A covered business shall implement proportionate age assurance measures where age assurance is reasonably necessary to comply with any applicable obligations under 9 V.S.A. §§ 2449c–2449g. Nothing in this Rule requires a covered business to collect personal data where it can comply with those obligations by treating a user as a covered minor.

(d) Where age assurance is reasonably necessary, a covered business shall use a proportionate age assurance process or technique.

(e) Age assurance shall be conducted using a privacy-protective process or technique reasonably available that achieves the level of confidence appropriate to the applicable obligation, giving priority to user privacy and accessibility over accuracy, consistent with 9 V.S.A. § 2449g.

CP Definitions

(a) Terms used but not defined in this Rule have the meanings set forth in 9 V.S.A. § 2449a.

(b) "Age assurance" means a process or technique used to determine, estimate, or communicate the age or age range of a user, including whether the user is a covered minor. Methods may include self-declaration, estimation, credentials, privacy-preserving age signals, and combinations of methods; no method is inherently required or preferred.

(c) "Age assurance data" means personal data collected for the purpose of making an age-related determination, including personal data supplied to or obtained by an age assurance provider for that purpose. This term does not expand the statutory prohibition on uses of personal data collected for age assurance to an age-range determination generated by the process, but the determination remains subject to applicable law and the deletion exception in 9 V.S.A. § 2449g(a)(2).

(d) "Age signal" means an output indicating or communicating an age range or age-related status.

(e) "Error rate" means the frequency of incorrect age-related determinations, including adults classified as minors and minors classified as adults.

(f) "Fallback mechanism" means an alternative process or technique available where the primary age assurance process fails, produces an inconclusive result, or cannot reasonably be used.

(g) "Linkability" means the ability to associate a user across services, sessions, accounts, devices, or contexts, directly or indirectly.

(h) "Privacy-invasive age assurance" means a process or technique that, based on its design and operation, creates a material privacy risk considering the amount and sensitivity of personal data collected, transmission, retention, linkability, disclosure, secondary use, or persistent identification.

(i) "Proportionate age assurance" means an age assurance process or technique selected in light of the applicable statutory obligation, the reasonably necessary

level of confidence, and the priority afforded to privacy and accessibility under 9 V.S.A. § 2449g.

CP Age Assurance Selection

(a) Where age assurance is necessary to comply with an applicable statutory obligation, a covered business shall select a commercially reasonable and technically feasible process or technique in light of:

1. The applicable statutory obligation and the age-related determination needed for compliance;
2. The amount and sensitivity of personal data collected or processed;
3. Whether data is processed locally or transmitted, and the risks of retention, disclosure, linkability, or secondary use;
4. Accessibility and the burdens imposed on users, including users who cannot use a particular method;
5. More privacy-protective reasonably available alternatives; and
6. The level of confidence reasonably necessary for the age-related determination, giving priority to privacy and accessibility over marginal gains in accuracy.

(b) Depending on the circumstances, commercially reasonable and technically feasible processes or techniques may include self-declaration, existing age signals, privacy-preserving age credentials or tokens, estimation, or a combination of methods. This subsection identifies possible methods, not a preferred hierarchy or a requirement to collect additional personal data.

CP Graduated Escalation

(a) A covered business shall consider more privacy-protective reasonably available age assurance methods before selecting a method that creates greater privacy risks.

(b) In evaluating privacy impacts, the covered business shall consider the amount and sensitivity of personal data collected, whether raw personal data is transmitted, retention, linkability, disclosure, secondary use, persistent identification, accessibility, and user burden.

(c) No age assurance process or technique, including self-declaration, estimation, credential-based methods, biometric methods, device-based methods, or privacy-preserving credentials, is inherently required or preferred under this Rule.

(d) A covered business may use multiple processes or techniques where reasonably necessary, provided that each complies with applicable privacy, accessibility, minimization, and proportionality requirements.

(e) Before using a process or technique that materially increases privacy risks, a covered business shall consider whether a more privacy-protective reasonably available alternative can achieve the reasonably necessary level of confidence.

(f) A covered business shall maintain documentation reasonably sufficient to explain the basis for selecting a process or technique where the selection materially increases privacy risks.

CP Accuracy and Error Evaluation

(a) A covered business shall consider the known accuracy, error rates, and limitations of an age assurance process or technique used, including false positives (adults classified as minors) and false negatives (minors classified as adults).

(b) The evaluation shall take account of reasonably available information about material limitations, disproportionate errors, and accessibility barriers, without requiring collection or retention of personal data prohibited by 9 V.S.A. § 2449g.

(c) A covered business shall not use a process or technique where known error rates or limitations create a material risk that the process will not reliably perform the age-related determination for which it is used. In applying this subsection, privacy and accessibility shall be prioritized over accuracy consistent with 9 V.S.A. § 2449g; marginal improvements in accuracy alone do not require a more privacy-invasive method.

(d) Where available information indicates a material risk of incorrect classification, including adults incorrectly classified as minors, a covered business shall provide a reasonably accessible means to correct or contest a determination that materially affects access. In assessing accuracy, a covered business shall consider the effects of both false positives and false negatives, including burdens on adults incorrectly classified as minors.

CP Frequency and Reassessment

(a) A covered business shall not conduct age assurance more frequently than reasonably necessary to satisfy the applicable statutory obligation.

(b) A covered business shall not require repeated age assurance or reverification that results in unnecessary collection of personal data or imposes an unreasonable burden on users.

(c) Reverification may be undertaken where reasonably necessary because of a material change in circumstances, reliability concerns, fraud prevention, security, or compliance with applicable law.

(d) Continuous monitoring, persistent tracking, or repeated collection of personal data for age assurance shall not be used unless necessary for reliability, fraud prevention, security, a material change in circumstances, or compliance with applicable law. Any such practice remains subject to the statutory collection, use, and immediate-deletion restrictions.

(e) Nothing in this section authorizes retention of personal data that 9 V.S.A. § 2449g(a)(2) requires to be deleted.

CP Data Minimization in Age Assurance

(a) A covered business shall limit collection and processing of personal data for age assurance to the minimum reasonably necessary for the age-related determination required by the applicable statutory obligation.

(b) A covered business shall not collect personal data for age assurance where the determination can reasonably be made without collecting that data, including where compliance is achieved by treating the user as a covered minor.

(c) A covered business shall delete personal data collected for age assurance immediately after the age-related determination is made, except for the age range, consistent with 9 V.S.A. § 2449g(a)(2). This Rule creates no additional retention exception for auditing, fraud prevention, security, or compliance purposes.

(d) A covered business shall not use personal data collected for age assurance for a purpose prohibited by 9 V.S.A. § 2449g.

CP Linkability and System Design

(a) A covered business shall design and implement age assurance processes or techniques to minimize linkability across services, devices, accounts, and contexts.

(b) A covered business shall not use personal data collected for age assurance to enable cross-service identification, profiling, behavioral advertising, or other prohibited secondary uses.

(c) Age-related outputs shall disclose no more information than necessary for the applicable age-related determination, consistent with the statutory permission to retain an age range.

(d) This section does not authorize retention of underlying age assurance personal data after the age-related determination.

CP ___ Prohibited Uses, Retention, and Disclosure of Age Assurance Data

(a) A covered business shall use personal data collected for age assurance only for the age-related determination for which it was collected and as otherwise expressly permitted by 9 V.S.A. § 2449g.

(b) A covered business shall not use such data for advertising, profiling, personalized recommendations, engagement optimization, or inference of unrelated characteristics where such use is prohibited by 9 V.S.A. § 2449g.

(c) A covered business that uses a third party for age assurance remains responsible for compliance with applicable requirements of this Rule and 9 V.S.A. § 2449g.

(d) A covered business shall take reasonable steps to ensure that a third party processing personal data for age assurance does not retain, reuse, disclose, or combine that data in a manner prohibited by 9 V.S.A. § 2449g.

(e) The deletion requirement in CP ___ Data Minimization in Age Assurance applies regardless of whether the covered business or a third party performs the determination.

CP ___ Fallback and Accessibility

(a) Where an age assurance process or technique fails, produces an inconclusive result, or is not accessible to a user, a covered business shall provide an accessible alternative where one is available.

(b) A fallback mechanism shall minimize additional personal data collection and avoid requiring a more privacy-invasive process or technique where a more privacy-protective reasonably available alternative is sufficient.

(c) Nothing in this section requires a covered business to provide access in violation of another applicable law or prevents compliance by treating a user as a covered minor.

CP ___ Appeals Process

(a) A covered business shall provide an accessible means to contest or correct an age-related determination that materially affects a user's access to an online service, product, or feature.

(b) An appeal may be resolved through correction of information, automated reconsideration, or an alternative age assurance process or technique where that method provides a meaningful opportunity to correct the determination.

(c) Meaningful human review shall be available where automated reconsideration or an alternative process cannot reasonably resolve the dispute.

(d) An appeals process shall avoid unnecessary delays, barriers, and collection of additional personal data and shall not require a more privacy-invasive method where a reasonably available, more privacy-protective alternative is sufficient.

(e) Personal data collected during an appeal is subject to the collection, use, and deletion requirements of 9 V.S.A. § 2449g.

CP Compliance and Oversight

(a) A covered business shall maintain documentation reasonably sufficient to demonstrate compliance with this Rule, proportionate to the age assurance process or technique used and the associated privacy and accessibility risks.

(b) Documentation may address the basis for selecting the process or technique, reasonably available less privacy-invasive alternatives, known accuracy limitations, accessibility considerations, and arrangements with third parties, to the extent relevant.

(c) This section does not require retention of personal data collected for age assurance beyond the point permitted by 9 V.S.A. § 2449g(a)(2). Documentation should describe compliance without retaining prohibited underlying personal data.

(d) Failure to maintain a particular document does not create a presumption that the covered business violated a substantive provision of this Rule.

(e) A covered business remains responsible for compliance with this Rule when age assurance is performed by a third party.

CP Illustrative Examples

Examples in this Rule are illustrative and do not independently expand an operative prohibition.

CP Severability

If any provision of this Rule, or its application to any person or circumstance, is held invalid by a court of competent jurisdiction, the remaining provisions and

applications shall remain in effect to the extent they can be given effect independently.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Vermont

NetChoice

Plaintiff(s)

v.

Charity Clark, in her official capacity as the Vermont Attorney General

Defendant(s)

Civil Action No. 2:26-cv-444

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

Charity Clark
Vermont Attorney General
109 State Street, Pavilion Building
Montpelier, VT 05609

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Matthew B. Byrne, Esq.
Gravel & Shea PC
76 St. Paul Street, 7th Floor
P.O. Box 369
Burlington, VT 05402-0369
mbyrne@gravelshea.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 2:26-cv-444

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* Charity Clark, Vermont Attorney General was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: