UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

NETCHOICE, *Plaintiff*, v. ALAN WILSON, in his official capacity as the South Carolina Attorney General, *Defendant*.	Civil Action No. _____

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. South Carolina has enacted sweeping restrictions on free speech. The South Carolina Age-Appropriate Code Design Act ("Act") imposes an unlawful censorship regime that will fundamentally control how websites present speech and information to their users, what speech they present, and how hundreds of millions of Americans access that speech. *See* Ex. A (enacted legislative text).[1] Worse still, the Act requires websites to implement its vague and sweeping directives *immediately*, forcing thousands of websites into immediate non-compliance without any meaningful opportunity to understand the Act's requirements, consider options for compliance, or seek judicial relief.

2. The Act's central mandate is that websites "exercise reasonable care" in the speech they disseminate to prevent vaguely-defined "harm[s] to minors," such as "compulsive usage," "severe emotional distress," and "highly offensive" privacy intrusions. § 39-80-20(A). But

[1] This Complaint uses the term "service" or "website" to include all regulated "[c]overed online service[s]," § 39-80-10(4), including applications and other software. Unless otherwise noted, all statutory citations are citations to the South Carolina Code of Laws.

characterizing speech as a tort does not change the First Amendment. In both purpose and effect, this mandate imposes content-based restrictions on speech. As the Fourth Circuit recently recognized, websites cannot evaluate how to "design" and "operat[e]," *id.*, their websites to prevent the specified harms "without also demonstrating that the [website] prioritizes the dissemination of *one type of content over another*." *M.P. by & through Pinckney v. Meta Platforms Inc.*, 127 F.4th 516, 525 (4th Cir. 2025) (emphasis added).

3. The Act thus compels websites to act as the government's speech police, requiring them to make content-based judgments about lawful expression and forcing them to remove, downrank, or suppress lawful speech to avoid liability.

4. In addition to this generalized duty of "care," the Act imposes a number of specific prohibitions and requirements regulating so-called "design features" and other activities that websites rely on to organize and present speech. § 39-80-30(A). These rules direct websites to build an entirely different mode of presenting content through content-shaping controls that must be enabled by default for minors. They require websites to disable core discovery, engagement, and interaction features that disseminate speech. And—although the Act is anything but clear—the rules appear to compel services to change their design and expressive offerings for all users—both minors *and* adults. These minors and adults are among the millions of people who use NetChoice members' services to share billions of pieces of content annually on topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 870 (1997).

5. The Act also imposes strict liability on websites that "facilitat[e]" protected *commercial* speech for products that are prohibited for minors but perfectly lawful for adults. § 39-80-40(A)(B). This requires services to monitor and screen third-party advertising that flows through modern, often automated ad systems. And because perfect screening is not feasible in real-

time delivery systems, websites face immense pressure to block lawful ads and lawful speakers altogether.

6. Finally, the Act forces websites to stigmatize their own services by facilitating and submitting to intrusive third-party "audits" by which an outsider examines whether websites have sufficiently heeded the Act's content-based and highly subjective directives to restrict speech. § 39-80-70. The Act then compels websites themselves to issue "reports" of those audits and to provide them to the South Carolina Attorney General for public dissemination.

7. Like many States before it, South Carolina enacted its Act presumably under the auspices of protecting minors. But in fact it is a misguided attempt to regulate the *speech* minors engage with.

8. The First Amendment protects South Carolinians' right to receive information and ideas online regardless of the State's views of their social worth or whether those ideas might be too engaging for some minors or cause distress to others. The First Amendment protects among other things: speech that causes "anguish," *Snyder v. Phelps*, 562 U.S. 443, 456 (2011); speech that is "offensive" or "disagreeable," *Mahanoy Area Sch. Dist. v. Levy*, 594 U.S. 180, 205 (2021) (Alito, J., concurring); speech that "invites dispute," *Young v. Am. Mini Theaters, Inc.*, 427 U.S. 50, 63-64 (1976); and even speech that is "highly offensive" or "unwanted," *United States v. Playboy Ent. Grp.,* 529 U.S. 803, 811 (2000).

9. That is why federal courts across the country have rejected as unconstitutional many laws similar to this one. *See, e.g.*, *NetChoice, LLC v. Bonta*, 113 F.4th 1101 (9th Cir. 2024) ("*Bonta I*"); *NetChoice v. Murrill*, 2025 WL 3634112 (M.D. La. Dec. 15, 2025); *NetChoice v. Griffin*, 2025 WL 3634088, at *13 (W.D. Ark. Dec. 15, 2025) ("*Griffin III*"); *NetChoice v. Weiser*, 2025 WL 3101019 (D. Colo. Nov. 6, 2025); *NetChoice, LLC v. Bonta*, 770 F. Supp. 3d 1164 (N.D.

Cal. 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice, LLC v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025); *NetChoice, LLC v. Griffin*, 2025 WL 978607 (W.D. Ark. Mar. 31, 2025) ("*Griffin II*"); *Students Engaged in Advancing Tex. v. Paxton*, 2025 WL 455463 (W.D. Tex. Feb. 7, 2025) ("*SEAT*"); *Comput. & Commc'ns Indus. Ass'n v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024) ("*CCIA*").

10. The Act violates the First Amendment because it restricts covered websites' protected speech and editorial judgment. It regulates how covered services select, rank, recommend, and display speech to their users—all protected expression. *See Moody v. NetChoice, LLC*, 603 U.S. 707, 728-40 (2024); *Packingham v. North Carolina*, 582 U.S. 98, 104-07 (2017).

11. The Act also violates the First Amendment rights of website *users* because it blocks and burdens their ability to: (1) receive protected speech; (2) find speakers, communities, and information; and (3) engage in lawful discussion through features that help them find and interact with protected speech.

12. Although the State is free to voice concerns about how much time its citizens spend online, the First Amendment does not countenance "[b]road prophylactic rules in the area of free expression." *Riley v. Nat'l Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781, 801 (1988). Many of the Act's requirements regulate how covered services disseminate speech to both adults and minors. States lack authority to restrict lawful ideas in the name of protecting minors. *See Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 794-802 (2011); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 213-14 (1975). And where "[t]he overriding justification for [a] regulation is concern *for the effect of the subject matter on young viewers*," that law "is not justified without reference to the content of the regulated speech." *Playboy Ent. Grp.*, 529 U.S. at 813. For this reason alone, the Act is presumptively invalid.

13. The Act also creates an insurmountable vagueness problem. It defines its prohibitions in highly subjective terms that require websites to predict the potential effects of speech on listeners of different ages, preferences, and sensitivities. It leaves numerous key terms like "design features" undefined. § 39-80-30(A)(1). And it requires websites to guess as to what designs, algorithms, features, and content may subject them to liability.

14. The Act's ill-defined standards also give state officials nearly boundless enforcement discretion, forcing covered websites "to steer far wider of" any universe of speech South Carolina might be able to restrict "if the boundaries of the forbidden areas were clearly marked." *Baggett v. Bullitt*, 377 U.S. 360, 372 (1964). Government restrictions on speech "cannot be so vague as to set the censor adrift upon a boundless sea." *Interstate Cir., Inc. v. City of Dallas*, 390 U.S. 676, 684. (1968); *see United States v. Williams*, 553 U.S. 285, 304 (2008); *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012).

15. Several challenged provisions are also preempted by federal law.

16. Section 230 of the federal Communications Decency Act preempts the Act to the extent the Act imposes liability for monitoring, screening, and editorial decisions (or lack thereof) relating to third-party content. Congress protected websites from being held liable for information provided by third-party content providers, and it barred inconsistent state liability regimes. *See* 47 U.S.C. § 230(c)(1), (e)(3); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330-31 (4th Cir. 1997).

17. The Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-06, also preempts the Act's provisions that restrict websites' ability to use the data of minors. COPPA establishes a uniform, national framework that permits websites to collect and use minors' data if they provide notice to parents of children (under 13) and obtain verifiable parental consent. South

Carolina's Act, by contrast, imposes numerous additional restrictions on websites' data use that are inconsistent with, and preempted by, COPPA.

18. The Act also violates the Commerce Clause. As Congress recognized in both COPPA and Section 230, the "Internet . . . requires a cohesive national scheme of regulation." *ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999) (cleaned up). Indeed, "[g]iven the broad reach of the Internet, it is difficult to see how a blanket regulation of Internet material . . . can be construed to have only a local effect." *PSINet, Inc. v. Chapman*, 362 F.3d 227, 240 (4th Cir. 2004). Even if such a construction were possible here, "the burdens [the Act] imposes on interstate commerce are excessive in relation to the local benefits it confers." *Id.*

19. Finally, the Act also violates the Due Process Clause because it took effect *immediately* and imposed sweeping new duties without anything approaching a reasonable opportunity for covered services to understand and comply. These services now face immediate liability tied to vague, complex, service-wide design changes that require services to rebuild from the ground up. That rebuilding cannot occur overnight—or even in weeks. Due process requires time to learn a law's requirements and conform before this liability can attach. *See United States v. Locke*, 471 U.S. 84, 108 (1985); *Pac. Tel. & Tel. Co. v. City of Seattle*, 291 U.S. 300, 304 (1934). That is particularly true for this Act, which imposes treble damages and personal liability for company officers without any opportunity to cure.

20. The chill imposed by the Act is real, severe, and immediate. When other States have adopted similar laws forcing websites to censor speech on a dime, both NetChoice members and other websites have predictably decided the risk of liability is not worth it and shut down their expressive activities in those States. *See* Dreamwidth, *Mississippi legal challenge: beginning 1 September, we will need to geoblock Mississippi IPs* (Aug. 26, 2025), https://tinyurl.com/4dybyjts;

Groups.io, *Why access from Mississippi is currently blocked*, https://tinyurl.com/3xrj2wyc.

21. This Court should declare all these challenged provisions unlawful and enjoin them, both facially and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X).

PARTIES & STANDING

22. Plaintiff NetChoice is a District of Columbia nonprofit trade association for internet companies. NetChoice's mission is to promote online commerce and speech and to increase consumer access and options via the internet, while minimizing burdens that could prevent businesses from making the internet more accessible and useful. NetChoice's members are listed at NetChoice, About Us, https://perma.cc/5QXR-E9H7.

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

24. 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); *Citizens for Const. Integrity v. United States*, 57 F.4th 750, 759 (10th Cir. 2023); *Murrill*, 2025 WL 3634112, at *15-20; *Carr*, 789 F. Supp. 3d at 1213-15; *Yost*, 778 F. Supp. 3d at 939-40; *CCIA*, 747 F. Supp. 3d at 1029-31; *NetChoice, LLC v. Griffin*, 2023 WL 5660155, at *10 (W.D. Ark. Aug. 31, 2023) ("*Griffin I*").

25. Based on the Act's definitions, § 39-80-10, 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, *e.g.*, Amazon, Automattic, Discord,

Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc. and TikTok USDS Joint Venture LLC, X, and YouTube.

26. NetChoice also 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); *Fitch*, 134 F.4th at 805-07; *Murrill*, 2025 WL 3634112, at *15-20; *Yost*, 778 F. Supp. 3d at 946; *CCIA*, 747 F. Supp. 3d at 1031; *Griffin I*, 2023 WL 5660155, at *11-12.

27. Defendant Alan Wilson is the South Carolina Attorney General. Defendant is a South Carolina resident and is sued in his official capacity.

28. The Act gives the South Carolina Attorney General authority to enforce the Act. *See* § 39-80-80(A).

JURISDICTION & VENUE

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

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

31. This Court has personal jurisdiction over Defendant because he resides in and conducts a substantial proportion of his official business activities in South Carolina.

32. 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, South Carolina. Venue is proper in this Division under this Court's local rules. *See* Local Civ. Rule 3.01(A).

BACKGROUND

33. **Online services—including NetChoice's covered members—disseminate and facilitate vast amounts of protected speech.** The internet contains an enormous volume of protected speech. People use online services to read, watch, listen, and exchange ideas on subjects "as diverse as human thought," *Reno*, 521 U.S. at 852 (citation omitted), including politics, religion, art, science, and untold other interactions at the heart of daily life.

34. Internet users engage in this protected speech by sharing text, photos, videos, and commentary and by organizing, advocating, and building communities online.

35. Multiple Supreme Court decisions have held that the First Amendment protects online speech no less than other forms of speech. *See Packingham*, 582 U.S. at 104 ("While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular." (cleaned up)); *see also Moody*, 603 U.S. at 719 ("the First Amendment . . . does not go on leave when social media are involved").

36. A great deal of that protected speech occurs on NetChoice members' websites. Those websites disseminate user speech and enable sharing at massive scale. Users post text, images, audio, and video, and they also comment, react, and respond in real time. Other services offer video streaming, audio streaming, podcasts, and access to libraries of electronic books and information. In other words, people use these services to "gain access to information and communicate with one another." *Packingham*, 582 U.S. at 107.

37. The "social media" services alone disseminate and facilitate "billions of posts" of fully protected speech. *Moody*, 603 U.S. at 734. NetChoice members also "engage[] in expression" of their own through their "display" and "compiling and curating" of protected content "created by others." *Id.* at 728, 731, 740. NetChoice members exercise protected editorial judgment in how

they design their expressive services, including how they select, rank, recommend, and present speech to users. *See id.* at 728.

38. Regulations that burden websites' expressive choices therefore burden both users and websites as speakers and listeners alike. *Packingham*, 582 U.S. at 104-07.

39. **NetChoice members' covered websites use "data" to publish speech and engage in editorial functions.** Covered websites could not engage in these expressive activities without collecting and using some amount of data from their users. "An individual's right to speak is implicated when information he or she possesses is subjected to restraints on the way in which the information might be *used* or disseminated." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 568 (2011) (emphasis added; citation omitted).

40. Online data is much like the ink and paper necessary to publish newspapers—and the subscriber addresses necessary to distribute those newspapers. Put another way, it is a necessary part of disseminating protected speech to willing viewers and readers. It is also a building block in the further creation of speech.

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

42. *Data needed to deliver content.* Data collection is required simply to provide functional services and content to users at all. Information about a user's IP address, device type, operating system, screen resolution, browser type, language preferences, and time zone is necessary to determine where content should be disseminated and how to present it. An IP address acts like a digital mailing address, allowing packets of information to be routed to a particular device or server. Absent an IP address, content cannot be directed to an end recipient. Similarly,

other information—like a user's operating system and language preferences—allows formatting content in a way that will be decipherable to the user (*e.g.*, choosing the correct format of a video based on device type and screen resolution).

43. Many covered services also need user data to deter and detect malicious actors. For example, logging technical signals and changes on an account helps websites detect behavior that could signal a compromised account. Such logs also help users restore accounts. Without such data collection, services would be less functional and less secure.

44. *Information to access services.* Many websites have aspects that are optimized and available only for individuals who create an account. Some social media services, for example, permit non-members to view public portions of a user's profile, but not to view each post in detail. Allowing users to create accounts provides account holders with greater security, enhanced control, and more nuanced personalization features. But websites must collect information from users to create accounts, such as usernames, contact information, and passwords.

45. *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 and to support websites' efforts to deliver age-appropriate content. This aims to ensure that people see the content they want to see, in the order they want to see it, while avoiding or deprioritizing content they do not want to see or that is not appropriate for them.

46. The Supreme Court has recognized that personalized feeds—including the curated feeds of "Facebook" and "YouTube"—are protected expressive offerings because they incorporate editorial judgments, such as from a website's community guidelines and content moderation standards. *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.

47. Services beyond social media use personalization too. A video streaming service like Hulu might use personalization to recommend shows and movies based on prior watching habits and direct feedback from users such as "likes" or "dislikes" or preferences selected during account setup. Music streaming services do the same. Online news sources and e-reading services also use personalization to recommend articles and books based on content a user has engaged with. The same is true for e-commerce websites engaging in protected commercial speech whereby a customer who just bought (for example) peanut butter might see a recommendation for jelly.

48. Content curation through personalization allows users to see and engage with content that they may find most useful. This includes content from people they "follow" or "subscribe" to, recommended content from other people or accounts, alerts about developing events, and advertisements that help make the services viable. Without such curation, users could be lost in the potential "deluge" of content—which may not be useful, relevant, or appropriate to specific users, including minors. *Id.* at 719.

49. When moderating content, Amazon, Facebook, Instagram, Nextdoor, Pinterest, Reddit, TikTok, Tumblr, X, and YouTube sometimes use "algorithms," which the services "write . . . to implement" their "Community Standards" and similar policies. *Id.* at 734-35; *see* ECF 1, *TikTok Inc. v. Bonta*, 5:25-cv-09789-EJD (N.D. Cal. Nov. 13, 2025); ECF 6, *Google LLC et al. v. Bonta*, 5:25-cv-09795-EJD (N.D. Cal. Nov. 13, 2025); ECF 1, *Meta Platforms, Inc. v. Bonta*, 5:25-cv-09792-EJD (N.D. Cal. Nov. 13, 2025).

50. These algorithms are computer programs that help implement human editorial choices. A computer program using algorithms that provide human-programmed, expressive

"instructions" on "the conveying of information" to other humans is "'speech' for purposes of the First Amendment." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 447 (2d Cir. 2001). "Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer." *Id.* "[T]he fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions 'speech' for purposes of the First Amendment." *Id.* "Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection." *Id.* at 446 (citing *Miller v. California*, 413 U.S. 15, 34 (1973) ("The First Amendment protects works which, taken as a whole, have serious literary, artistic, political, or scientific value[.]")).

51. Importantly, websites and NetChoice members do not use personalization algorithms to "respond solely to how users act online—giving them the content they appear to want, without any regard to independent content standards." *Moody*, 603 U.S. at 736 n.5. Instead, websites write algorithms that personalize content while *also* "*implement[ing] th[eir community] standards*—for example, to prefer content deemed particularly trustworthy." *Id.* at 735 (emphasis added).

52. Indeed, each covered NetChoice member specifically designs, monitors, and manages their algorithms to reflect a multitude of ongoing human expressive judgments. These include judgments about what classifiers to use to increase or decrease the prominence of content; how to identify content that might not be appropriate to recommend widely, such as because it is low-quality, clickbait, or violent; how much new versus familiar content to present; how to implement community guidelines and content policies; and how to moderate content that might be more problematic with repeated exposure. Websites also decide on what type of feedback and

signals from users to integrate into their algorithms to make assessments about content quality and presentation and organization of content. These judgments are dynamic and iterative, reflecting affirmative and ongoing efforts to present a unique expressive offering.

53. **Existing options for parental control and oversight.** As multiple courts have recognized, parents have many existing and diverse choices to regulate and oversee whether and how their minor children use the internet. "[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." *Griffin II*, 2025 WL 978607, at *3 (collecting evidence); *e.g.*, *Bonta I*, 113 F.4th at 1121.

54. There are resources that collect all these parental tools in one place. *E.g.*, Internet Matters, *Parental Control Guides*, https://perma.cc/RN3U-ETA7.

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

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

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

58. Cellular and broadband internet providers offer families tools to block certain online services from certain devices. *See, e.g.*, Verizon, Verizon Smart Family, https://tinyurl.com/56nm4atf; AT&T, AT&T Secure Family, https://tinyurl.com/4dvkxcze; T-Mobile, Family Controls and Privacy, https://tinyurl.com/2xhr7k3.

59. Internet browsers also allow parents to control what online services their children may access. *See, e.g.*, Mozilla, *Block and unblock websites with parental controls on Firefox* (Aug.

11, 2022), https://tinyurl.com/3kwzt63a. Some browsers offer a "kids mode" or allow parents to see what online services their children are accessing the most. *See* Google, Safety Center, *Choose parental controls that are right for your family*, https://perma.cc/8PGR-7HEC. Parents can also use widely available browser extensions to reinforce these tools.

60. Wireless routers often have settings allowing parents to block particular websites, filter content, monitor internet usage, and control time spent on the internet. *See, e.g.*, Netgear, *Netgear Smart Parental Controls*, https://perma.cc/7U7S-JRAD; tp-link, *How to configure Parental Controls on the TP-Link Wi-Fi Router* (Oct. 21, 2025), https://perma.cc/UBZ7-72CU.

61. Devices allow parents to limit the time their children spend on the device, curtail the applications that can be used, filter online content, and control privacy settings. *See* ConnectSafely, *Set parental controls with the Amazon Kids Parent Dashboard*, Amazon News (Nov. 19, 2025), https://perma.cc/C87X-7RYG; Apple, *Use parental controls on your child's iPhone or iPad* (May 5, 2025), https://perma.cc/2P39-W8BA; Apple, *Use Screen Time on your iPhone or iPad* (May 13, 2025), https://perma.cc/CV6N-Z7H5; Google Family Link, *Help keep your family safer online*, https://perma.cc/5ZRD-SZTA; Microsoft, *Set up Microsoft Family Safety* (2026), https://tinyurl.com/mmret3x8; Samsung, *Manage Family groups and parental controls with your Samsung Account*, https://perma.cc/ABZ5-PSLR; Samsung, *Use Digital Wellbeing features on your Galaxy phone or tablet*, https://perma.cc/D6YV-VHDR; Android Help, *Manage how you spend time on your Android phone with Digital Wellbeing* (2026), https://perma.cc/FX2E-FR5F.

62. Many third-party applications also allow parents to control and monitor their children's online activities. *See, e.g.*, Benedict Collins, *Best Parental Control App of 2026: Expert Testing, Ranking and Reviews*, TechRadar (Jan. 8, 2026), https://perma.cc/8KL2-FN6P.

63. **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.

64. 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. *See* Amazon, *Parent Dashboard*, https://perma.cc/JZ76-LVSB. Grown-ups can opt in or out of digital features and control 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 in one central place. Parents can use the Dashboard to track what children are doing online. Usage information—including information for books, videos, skills, and apps—is all displayed for at-a-glance consideration. These quick insights help grown-ups understand what their kids are interested in, foster one-on-one conversations based on those findings, and can help with setting appropriate screen-time limits.

65. Parents and guardians can also use supervision tools on Facebook and Instagram to set daily time limits for their teens or limit use during select days and hours; set reminders to close the apps; 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; approve or deny their teens' requests to change default safety and privacy settings to a less strict state; and see their teen's settings for account privacy, messaging, and sensitive content. *See, e.g.*, Instagram, Help

Center, *Parental Supervision* (2026), https://tinyurl.com/356rttjy; Facebook, Help Center, *Safety Resources for Parents* (2026), https://tinyurl.com/yu9mvvv5.

66. Facebook and Instagram also provide teens with tools to set their own time limits and set scheduled breaks. *See, e.g.*, Meta, *Giving Teens and their Parents More Ways to Manage Their Time on Our Apps* (June 27, 2023), https://perma.cc/GFA9-BRNT. Moreover, Meta has announced that minors under 18 will automatically be placed into Facebook and Instagram "Teen Accounts" which default to the strictest privacy settings and have limitations on who can contact minors, the content minors can see, and the time of day minors can receive notifications. Via Teen Accounts, parents will have added supervision features, including ways to get insights into who their minors are chatting with and seeing topics their minors are looking at. Minors under 16 need a parent's permission to change any of these Teen Accounts settings to be less strict. *See, e.g.*, Instagram, *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents* (Sept. 17, 2024), https://perma.cc/T62T-KN2S; Meta, *We're Introducing New Built-In Restrictions for Instagram Teen Accounts, and Expanding to Facebook and Messenger* (Apr. 8, 2025), https://tinyurl.com/3py5jbm9.

67. Pinterest is running an experiment on reminders during the school day that remind minor users who "open the Pinterest app during the school day" to "put down [their] phone[s], pause notifications, and focus on school." Pinterest, Help Center, *Resources for parents and care-givers of teens* (2026), https://perma.cc/8AA7-UGHT.

68. 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. *See* Snapchat Support, *What is Family Center?*, https://perma.cc/QB66-JEEY.

69. TikTok has a "family pairing" feature that allows parents to, among other things, set a screen time limit, restrict exposure to certain content, decide whether their teen's account is private or public, turn off direct messaging, and decide who can comment on their teen's videos.

70. 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. YouTube, *Exploration starts here: Choices for every family*, https://perma.cc/JXU2-HGXK. YouTube has also developed features and policies directed at promoting digital wellbeing among teens and children, such as turning auto-play off by default, refining its recommendation systems so teens are not repeatedly exposed to potentially harmful content, and reminding teens to take a break or go to bed. *Id.*

71. YouTube also offers a standalone "YouTube Kids" service that is a filtered version built specifically to let children under the age of 13 explore curated age-appropriate content. YouTube also offers additional tools for parents and caregivers to moderate the content children see. *See* YouTube Kids, *A safer online experience for kids*, https://perma.cc/GCS7-JRCM. In addition to other tools, YouTube Kids allows parents to control their children's privacy settings and 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." *See* YouTube For Families Help, *Limit screen time on YouTube Kids* (2026), https://perma.cc/AKV6-N66N.

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

73. Instagram encourages teens via prompts and safety notices to be cautious in conversations with adults, even those to whom they are connected. And Instagram Teen Accounts take this a step further by restricting direct messaging from people teens do not follow or are not connected to, regardless of the user's age. *See* Instagram, Help Center, *About Instagram Teen Accounts*, https://tinyurl.com/nhhd5a8j.

74. 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. Facebook and Instagram take steps to limit adults from messaging teens to whom they are not connected. *See, e.g.*, Meta, *Introducing Stricter Message Settings for Teens on Instagram and Facebook* (Jan. 25, 2024), https://perma.cc/KR5S-JCQP.

75. 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. *See* TikTok, Safety Center, *Guardian's Guide* (Feb. 6, 2026), https://tinyurl.com/fb2rf2cb. For 16- and 17-year-olds, TikTok also turns off direct messaging by default. *See id.*

76. Finally, YouTube and other members do not offer private messaging between users at all.

77. All NetChoice members prohibit minors under 13 from accessing their main services. Some NetChoice members offer separate experiences for users under 13 geared for that age group. TikTok also offers a separate experience specifically designed for users under 13 that has heightened protections and that does not offer the ability to post, to 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. *See* YouTube For Families Help, *Important info for parents about YouTube kids* (2026), https://perma.cc/YT9K-XDRR; YouTube Help, *What is a pre-teen supervised experience on YouTube?* (2026), https://perma.cc/KKF5-G5MN. These services allow parents to select content settings, set screen time limits, and otherwise oversee their children's use of the services.

78. **Covered websites' dedication to beneficial user experiences and user security.** NetChoice's members expend vast resources to improve their services and curate 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. *See* Malena Dailey, *By The Numbers: What Content Social Media Removes And Why* 13 (2021), https://perma.cc/M9VV-CFC4. "Facebook and YouTube" "cull and 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.

SOUTH CAROLINA AGE-APPROPRIATE CODE DESIGN ACT

79. The South Carolina Legislature passed HB 3431, the Age-Appropriate Code Design Act, on January 26, 2026. The Act became law after Governor McMaster signed it on February 5, 2026. The Act did not include any legislative findings. *See* HB 3431 § 1-4.

80. The Act took *immediate* effect after becoming law. *See id.* § 4 ("This act takes effect upon approval by the Governor."). It seeks to regulate content and expressive activities on covered websites and requires such websites to entirely reconfigure their expressive offerings.

81. Coming into compliance with the Act's multiple and onerous requirements would take most covered entities *at least* six months, if not many more—if it were possible at all.

82. **Covered services.** The Act regulates certain "[o]nline service[s]," which the Act defines as "any service, product, or feature that is accessible to the public on the internet including, but not limited to, a website or application. An online service may include any service, product, or feature that is based in part or in whole on artificial intelligence." § 39-80-10(9).[2]

83. A "[c]overed online service" is any "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that": (1) "owns, operates, controls, or provides an online service that conducts business in South Carolina"; (2) "is *reasonably likely to be accessed by minors*"; (3) "determines the purposes and means of the processing of consumer's *personal data* alone, or jointly with its affiliates, subsidiaries, or parent company"; and (4) either

> (A) has annual gross revenues in excess of twenty-five million dollars, adjusted every odd-numbered year to reflect changes in the Consumer Price Index;

[2] An "[o]nline service" does not include: "(a) a telecommunications service, as defined in 47 U.S.C. Section 153; (b) a broadband internet access service as defined in 47 C.F.R. Section 54.400; or (c) the sale, delivery, or use of a physical product." § 39-80-10(9)(a)-(c).

> (B) annually buys, receives, sells, or shares the personal data of fifty thousand or more consumers, households, or devices alone or in combination with its affiliates, subsidiaries, or parent company; or
>
> (C) derives at least fifty percent of its annual revenue from the sale or sharing of consumers' personal data.

§ 39-80-10(4)(a) (emphases added). "Covered online service" also includes "(i) an entity that controls or is controlled by a business that shares a name, service mark, or trademark that would cause a reasonable consumer to understand that two or more entities are commonly owned; and (ii) a joint venture or partnership composed of businesses in which each business has at least a forty percent interest in the joint venture or partnership." § 39-80-10(4)(b).

84. "Minor" means a consumer who is less than eighteen years of age. § 39-80-10(8). The Act does not define "consumer." But it defines "user" as "an individual who uses the covered online service and who is located in South Carolina." § 39-80-10(20).

85. A user is "[k]nown to be a minor" when "the covered online service has actual knowledge that a particular consumer is a minor. For purposes of this Act, actual knowledge includes all information and inferences known to the covered online service relating to the age of the individual including, but not limited to, self-identified age, and including any age the covered online service has attributed or associated with the individual for any purpose including, but not limited to, marketing, advertising, or product development purposes." § 39-80-10(7) (emphasis added).

86. If the user is known to be a minor, the covered online service must treat the particular individual as a minor. § 39-80-10(17)(b).

87. If the service is "directed to children," the service must treat all users as minors unless the service has actual knowledge that a user is not a minor. § 39-80-10(17)(a)(ii), (b).

88. "Reasonably likely to be accessed by a minor" means it is "reasonable to expect that the covered online service would be accessed by an individual minor or by minors based on the covered online service meeting either of the following criteria": (i) the individual user "is known to the covered online service to be a minor," or (ii) if the service "is directed to children as defined by the Children's Online Privacy Protection Act," 15 U.S.C. §§ 6501–06 ("COPPA"), "and the Federal Trade Commission rules implementing that act." § 39-80-10(17)(a). The phrase "known to the covered online service to be a minor" appears only in the Act's coverage definitions, apparently extending that part of the Act's definition—and the Act's onerous requirements—to *any* online service that has knowledge of even one minor user.

89. The Act imposes its most sweeping defaults and restrictions when a service "know[s]" a user is a minor. But the Act defines "know[]" broadly to include all "information" and "*inferences*" "known" to the website. This could be interpreted to encompass data the website possesses *anywhere* in its digital systems, even if no employee or system has *actually identified* the user as a minor. The Act thus forces covered services to consider when they will be deemed to have "actual knowledge" of a user's age, how to avoid liability for treating undetected minors as adults, and also how they will avoid treating large numbers of *adults* as minors. § 39-80-10(7); § 39-80-10(17)(b). The Act also forces services that are "directed to children" to treat *every* user as a minor unless they have "actual knowledge" the user is not a minor. This requires those services to either childproof *all* offerings for the youngest users or implement mechanisms to affirmatively sort adults from minors. § 39-80-10(17)(a)(ii), (b). In practice, and to avoid liability, these requirements could effectively require covered services to deploy some level of age-verification or age-estimation systems across their services to determine which users must be placed into the Act's default-restricted experience—or else treat all users as minors.

90. "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 "publicly available data." § 39-80-10(11).

91. **"Reasonable Care" requirement for covered services to "prevent" content from causing "harm to minors." § 39-80-20.** The Act requires websites to exercise "reasonable care" to prevent "harm" to minors, including (but not limited to) harms from "covered design features." § 39-80-20(A). This provision necessarily requires covered services to evaluate the underlying content they disseminate and make value-laden judgments about whether that speech should be removed or otherwise censored.

92. Specifically, the Act requires that covered services "shall exercise reasonable care in *the use of a minor's personal data and the design and operation of the covered online service including, but not limited to, covered design features*, to prevent the following *harm* to minors": (1) *compulsive usage* of the covered online service; (2) severe psychological harm including, but not limited to, anxiety, depression, self-harm or suicidal ideations; (3) severe emotional distress; (4) highly offensive intrusions on the minor's reasonable privacy expectations; (5) identity theft; (6) discrimination against the minor on the basis of race, ethnicity, sex, disability, or national origin; and (7) material financial or physical injury. § 39-80-20(A) (emphases added). The Act provides that "harm" under this section is "limited to those [harms] for which liability is permitted under 47 U.S.C. Section 230." § 39-80-20(B).

93. The Act enumerates features like "infinite scroll" and "autoplay" as potential vectors for "harms." § 39-80-10(3). "Covered design feature" means "any feature or component

of a covered online service that will encourage or increase a minor's frequency, time spent, or activity on a covered online service including, but not limited to," "infinite scroll," "auto-playing videos," "any design feature that emulates gameplay . . . that motivate or cause more frequent or more extensive use" (*e.g.*, streaks, badges, rewards), "quantification of engagement" such as showing "how many likes, comments, clicks, views, or reactions any user-generated item has received," "notifications and push alerts," "in-game purchases," and "appearance-altering filters." *Id.* "Compulsive usage" means "the persistent and repetitive use of a covered online service that substantially limits one or more of a user's major life activities including, but not limited to, sleeping, eating, learning, reading, concentrating, communicating, or working." § 39-80-10(1).

94. These definitions again are inseparable from the *content* the user is "scroll[ing]" or "playing." § 39-80-10(3). A user would not encounter harm from scrolling a service that was devoid of content, and indeed it is nonsensical to even attempt imagining such a service. The harms the Act describes, such as "compulsive usage" and "severe emotional distress" also presumably would not occur on websites that solely presented math lessons or religious studies—unless, of course, a minor was struggling with math, applied religious principles so strictly as to cause anxiety, or happened to be obsessively interested in either math or religion.

95. **Mandatory settings disabling personalization for minors by default and offering adults the option to disable personalization. §§ 39-80-30(B), 39-80-40(F).** The Act requires covered services both to offer a separate, non-personalized version of their services and to make this non-personalized version the default experience for minors. It also restricts any form of "profiling" for known minors "unless profiling is necessary to providing the covered online service with which a minor has knowingly requested and is limited to only the aspects of the covered online service with which a minor is actively and knowingly engaged." § 39-80-30(F).

96. Specifically, the Act requires that covered services "must provide to a user the option to opt out of *personalized recommendation systems*, except for optimizations based on the user's *expressed preferences*. A covered online service must establish this option as a default setting for any individual the covered online service knows to be a minor." § 39-80-30(B) (emphases added). "Personalized recommendation system" means "a fully or partially automated system used to suggest, promote, or rank content, including other users, hashtags, or material from others based on the personal data of users." § 39-80-10(12). "Expressed preferences" means "a freely given, considered, specific, and unambiguous indication of a user's preferences regarding the user's engagement with a covered online service." § 39-80-10(6)(a). Further, "expressed preferences" "cannot be based on the user's time spent engaging on the covered online service, nor on the usage of features that do not indicate explicit preference, such as comments made, posts reshared, or similar actions that are commonly taken on disliked media." § 39-80-10(6)(b).

97. Similarly, "[a] covered online service shall not" use "any form of automated processing of personal data to evaluate, analyze, or predict" a user's "personal preferences," "interests" or other aspects about a user, unless such a prediction "is necessary to providing the covered online service with which a minor has knowingly requested and is limited to only the aspects of the covered online service with which a minor is actively and knowingly engaged." § 39-80-30(F). The Act calls such predictions "[p]rofil[ing.]" § 39-80-10(15).

98. These broad mandates will block minors' access to protected expression as a default rule, because they force covered services to turn off systems that "suggest, promote, or rank content" for known minors—even though those systems are both how users find speakers, topics, and communities they want to see, read, and listen to and how covered services' expressive choices are executed. § 39-80-10(12); § 39-80-30(B). Covered services will also apparently need to treat

routine personalization as prohibited "[p]rofil[ing]" unless a minor has "knowingly requested" it, which will push services to deny minors those tools rather than risk liability. § 39-80-10(15); § 39-80-30(F).

99. The Act does not just affect minors. Even for adults, it forces covered services to build and maintain new opt-out settings across their services, which will require substantial engineering time, new compliance processes, and ongoing employee time to implement, monitor, and audit these systems for all users, including adults. §§ 39-80-30(B), 39-80-40(F).

100. **Mandatory "tools" restricting minors' access to certain content by default and offering adults the option to restrict certain content. § 39-80-30(A), (C).** The Act requires covered services to build "easily accessible" user controls that disable or limit a wide range of ordinary features that shape how users find, view, and engage with protected First Amendment expression online. § 39-80-30(A). These tools affect core speech-facilitating and speech-disseminating functions, including features like "auto-playing videos," "game-play," and the display of engagement metrics such as counts of "like[s]," "comment[s]," and "reaction[s]." *See* § 39-80-10(3). For minors, the Act requires that covered services ensure that these features are switched off by default, forcing minors into a stripped-down experience that reduces their access to protected First Amendment expression.

101. Specifically, the Act requires that covered websites "must provide a user or visitor to the service with easily accessible and easy-to-use tools to: (1) disable design features including, but not limited to, all covered design features, that are not necessary to provide the covered online service by allowing users to opt out of the use of all such design features or any combination of such design features; (2) limit the amount of time the user spends on the covered online service; (3) limit[], at the level of the user's choosing, the financial value of purchases and transactions on

the covered online service if such purchases and transactions have not been disabled; (4) block, disable, and render nonvisible messaging, requests, reactions, likes, comments, or other contact from account holders that are not already among the minor's existing connected accounts; (5) restrict the visibility of the minor's account and information posted by the minor to only users with *connected accounts*; (6) block, disable, and render nonvisible quantification of engagement including, but not limited to, providing a visible count of how many likes, comments, clicks, views, or reactions regarding any item generated by the user; (7) disable search engine indexing of a user's account profile such that the account only shows within searches initiated by a user with a connected account; (8) prohibit any other individual from viewing the user's connections to other users . . . ; and (9) restrict the visibility of the user's location information to only those with whom the user specifically shares such information and provide notice when the minor's precise geolocation information is being tracked or shared." § 39-80-30(A) (emphasis added). "Connected account" means "an account . . . that is directly connected to: (a) the user's account; or (b) an account that is directly connected to the user's account." § 39-80-10(2).

102. For known minors, "[a] covered online service must establish, implement, and maintain" all of these tools as "settings" that are enabled by "default." § 39-80-30(C). These requirements force covered services to turn off their core expressive offerings by default and disable the very functions that make them attractive to their audiences: functions that allow minors to discover speakers, receive recommendations, participate in public discussion, and engage with expression in real time.

103. The "tool" requirements also compel services to redesign their services around a dense litany of mandated controls, including sweeping limits on who can interact with a minor, what feedback the minor can see, how the minor can be found, and what information the minor

can access through ordinary browsing and search. § 39-80-30(A), (C). Those defaults will predictably block minors from lawful speech and lawful speakers. Meanwhile, the Act imposes significant engineering and compliance burdens across the entire service, because these tools must be built, integrated, tested, maintained, and enforced at scale. This will pressure services to change their core design and operations for everyone, including adults. § 39-80-30(A), (C).

104. **Prohibition on "facilitating" certain advertisements to minors. § 39-80-60(B).** The Act also makes it unlawful for a covered online service to facilitate certain advertisements to minors. This prohibition reaches advertising that originates with third parties and is published with automated self-service tools, not just ads the website creates, sells, or directly screens itself.

105. Although NetChoice members expend significant resources to ensure such ads are appropriate for minors, they do not—and could not—manually screen every possible third-party ad. In practical terms, this requirement will force services to police each and every ad by monitoring and screening all ad content to avoid liability. As with many of the Act's other requirements, this again invites overbroad suppression, because the safest course for a covered online service is to block or restrict entire categories of ads and ad-delivery mechanisms rather than attempt continuous fine-grained judgments about who might be a minor and what content might be covered.

106. Specifically, the Act prohibits covered services "from facilitating ads directed to minors for products prohibited for minors including, but not limited to, narcotic drugs, tobacco products, gambling, and alcohol to users the covered online services know are minors." § 39-80-60(B).

107. Again, many covered services, including NetChoice members, already firmly prohibit age-inappropriate advertisements of this sort. But the Act creates strict liability. With

automated auctions, self-serve advertising tools, and real-time delivery across many intermediaries, a covered service cannot perfectly monitor, at the moment an ad is served, what a particular ad contains, why it was delivered to a user, what user sees it, or whether upstream actors in the ad-delivery process are using prohibited criteria.

108. This prohibition thus forces covered services to monitor, screen, and suppress lawful messages to avoid liability. It will predictably lead to overblocking, reduced access to information for minors and adults alike, and chilled speech for advertisers and speakers who cannot reliably predict how the Act will be applied.

109. **Requirement compelling services to issue a public report. § 39-80-70.** The Act also compels covered services to publish third-party speech on highly controversial issues, including messages they might not agree with and messages that could stigmatize their services and editorial choices.

110. Specifically, the Act requires covered services to "issue a public report prepared by an independent third-party auditor that contains a detailed description of the covered online service as it pertains to minors, including its covered design features, its use of personal data, and its business practices as they pertain to minors." *Id.* These reports must include: "(1) the purpose of the covered online service; (2) the extent to which the covered online service is likely to be accessed by minors; (3) an accounting of the total number and types of reports generated pursuant to Section 39-80-60(A) and assessment of how those reports were handled, if known; (4) whether, how, and for what purpose the covered online services collects or processes minors' personal data and sensitive personal data; (5) the design safety for minors, the privacy protections for minors, and the parental tools that the covered online entity has adopted; (6) whether and how the covered online service uses covered design[] features; (7) the covered online service's process for handling

data access, deletion, and correction requests for a minor's data; (8) age verification or estimation methods used; and (9) description of algorithms used by the covered online service." *Id.*

111. These mandatory reports compel covered services to speak to third-party auditors and then to publish third-party speech about contested, policy-laden subjects that shape public perception of their services. *See X Corp. v. Bonta*, 116 F.4th 888, 894 (9th Cir. 2024) (compelled reports on content-moderation policies and practices likely violated the First Amendment). These mandatory reports also compel publication of subjective judgments about "design safety," "privacy protections," "parental tools," "age verification or estimation," and even "description of algorithms," along with narratives about how the service operates "as it pertains to minors." § 39-80-70(A). Because the report must be "prepared by an independent third-party auditor" ("in consultation with experts on minors' use of covered online services") and then publicly issued by the service, the Act essentially makes the service a mouthpiece for outsiders' assessments and potential critiques. § 39-80-70(A)-(B). That compelled speech will predictably chill design and editorial choices, and it will pressure services to change how they operate to avoid reputational harm that these reports could create.

112. **Enforcement. § 39-80-80**. The South Carolina Attorney General "shall enforce" the Act, § 39-80-80(A), and a "covered online service shall be liable for treble the financial damages incurred as a result of a violation of" the Act, § 39-80-80(B). Further, "[t]he officers and employees of a covered online service may be held personally liable for wilful and wanton violations" of the Act. § 39-80-80(C). The Act imposes this liability without specifying what connection (if any) these officers and employees must have to the alleged violation.

113. This enforcement scheme leaves covered services guessing about exposure and remedies. The Act says the Attorney General "shall enforce" it, yet the enforcement provisions

hinge on "treble" "financial *damages*" without saying who sues or what counts as damages. § 39-80-80(B) (emphasis added). This uncertainty could allow the Attorney General to argue for treating alleged noncompliance as an "unfair or deceptive act" under the South Carolina Unfair Trade Practices Act, § 39-5-20. This would allow him to seek sweeping injunctive relief and restitution-style orders. § 39-5-50(a)-(b). The Attorney General could also pursue civil penalties of up to $5,000 per violation, and up to $15,000 per violation of an injunction. § 39-5-110(a)-(b).

114. In light of these penalties—including *personal liability*—guessing wrong about what the Act means (or about what the South Carolina Attorney General interprets the Act to mean) is prohibitively expensive—not to mention ruinous for employees and officers. Many services will not or cannot risk it. Instead they will (1) self-censor by banning users who could be minors; (2) refrain from publishing content to certain users; (3) disable editorial features that control the publication and curation of content on their services; (4) forego efforts to connect their customers with suggested content or other users; or (5) shut down altogether.

CLAIMS

115. For all claims below, NetChoice raises challenges as applied to NetChoice's covered members, including those specified in paragraphs 20 and 21. NetChoice also raises facial challenges to the provisions in their entirety and as applied 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) (analyzing First Amendment challenge "to the extent of [the] reach" defined by Plaintiff).

116. Each First and Fourteenth Amendment challenge set forth below raises the rights of both NetChoice members and those who use or could prospectively use NetChoice members' websites. *See, e.g.*, *Am. Booksellers*, 484 U.S. at 392-93 (holding that bookstore could raise the

First Amendment rights of customers); *Yost*, 778 F. Supp. 3d at 940, 946; *NetChoice, LLC v. Bonta*, 692 F. Supp. 3d 924, 939 (N.D. Cal. 2023); *Griffin I*, 2023 WL 5660155, at *9-12.

COUNT I
42 U.S.C. § 1983
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT
("REASONABLE CARE" STANDARD, § 39-80-20(A))
(FACIAL AND AS-APPLIED CHALLENGES)

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

118. 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.

119. "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)).

120. Laws are content-based if they draw distinctions based "on the message a speaker conveys." *Id.* And 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.* (cleaned up) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)).

121. The Act requires covered online services to "exercise reasonable care in the use of a minor's personal data and the design and operation of the covered online service including, but not limited to, covered design features, to prevent" several enumerated "harm[s] to minors." § 39-80-20(A). This "reasonable care" standard necessarily requires covered online services to evaluate

the content on their websites and, if it is "reasonable" to do so, to remove content that could be considered "harm[ful]" to minors. *See* § 39-80-20(A).

122. Although several of the harms the Act enumerates are ambiguous and undefined, virtually none of them can be evaluated without making content-based judgments about the speech a website disseminates.

123. To decide what a service must "prevent," the service must assess what speech might contribute to "anxiety, depression, self-harm or suicidal ideations," "severe emotional distress," or "compulsive usage." § 39-80-20(A). News reports on climate change, famine, or genocide might not make the cut. Videos of classical ballet dancers could be removed for fear they might encourage eating disorders. Articles and research about vaccines and safety might be removed as well. The potential for censorship is endless. *See Playboy Ent. Grp.*, 529 U.S. at 811-12 (where "[t]he overriding justification for the regulation is concern for the effect of the subject matter on young viewers," the law "is not justified without reference to the content of the regulated speech" (cleaned up)); *Griffin III*, 2025 WL 3634088, at *8 (enjoining similar "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"); *see also Pinckney*, 127 F.4th at 525 (rejecting similar theory under common law tort principles because accepting such a theory would require an online service to "prioritize[] the dissemination of *one type of content over another*." (emphasis added)).[3]

124. Underscoring that the Act regulates content, the Act specifies that it does not "require a covered online service to prevent or preclude any user from *deliberately and*

[3] *Pinckney* is a Section 230 case, but the court's logic demonstrates that both covered online services and state enforcement officials would have to consider content (and make content-based judgments) to determine if a service has complied with the Act.

independently searching for or specifically requesting content, or accessing resources and information regarding the prevention or mitigation" of harm. § 39-80-20(C) (emphasis added).

125. This carveout would have no meaning if the Act's duty of care did not otherwise require websites to restrict content. First Amendment protections are not limited to speech that an audience "deliberately and independently" searches for. *Id.* The carveout is also internally inconsistent, because it disclaims any duty for content a minor "deliberately and independently" searches for—even though the Act would otherwise treat exposure to that very same content as a source of "harm." *Id.*

126. Regardless, the Act's unsupported assumption that users will know to deliberately search for and "request" specific pieces of content among the "billions" of posts and videos online, *Moody*, 603 U.S. at 734, ignores the protected role that covered websites play in disseminating protected speech on the internet. The assumption also overlooks the fact that writers, performers, and other content creators are unlikely to continue to *create* protected speech if viewers have no opportunity to see that speech unless they "deliberately and independently search[]" for it. *Id.*

127. South Carolina lacks a "free-floating power to restrict the ideas to which children may be exposed." *Brown*, 564 U.S. at 794, 799 (holding California could not bar minors from purchasing video games because they were violent). "Speech . . . cannot be suppressed solely to protect the young from ideas or images that a legislative body thinks unsuitable for them." *Erznoznik*, 422 U.S. at 213-14.

128. "While the First Amendment 'leaves undisturbed States' traditional power to prevent minors from accessing' some legitimately harmful speech, states cannot overly burden access to speech in their efforts to protect children." *NetChoice v. Brown*, 2025 WL 3267786, at *1 (D. Md. Nov. 24, 2025) (quoting *Free Speech Coal., Inc. v. Paxton*, 606 U.S. 461, 478 (2025)).

129. It is irrelevant that the Act characterizes its restrictions in terms of "design feature[s]" and "operation[s]." § 39-80-20(A). Even when viewed through the prism of these features—such as "auto-playing videos" and "gameplay," § 39-80-10(3)—the harm analysis still cannot be conducted independent of the *content* those features and operations carry. The analysis will differ depending on whether, for example, covered websites display algebra tutorials, guided meditations, violent movies, or any of countless other options. The Act thus impermissibly targets disfavored "subject matter" and that subject matter's "effect on young viewers." *Playboy Ent. Grp.*, *Inc.*, 529 U.S. at 812-13.

130. By imposing the "reasonable care" mandate on websites that facilitate, curate, and disseminate enormous amounts of third-party speech, the Act also impermissibly "deputizes covered businesses into serving as censors for the State." *Bonta I*, 113 F.4th at 1118 (citing *Interstate Cir., Inc.*, 390 U.S. at 678, 684).

131. Finally, the Act also triggers heightened scrutiny to the extent that it effectively compels age verification or age estimation as a condition of accessing and disseminating broad categories of fully protected speech. Although the Act's requirements for "known minors" are not clear, websites might determine that they cannot effectively protect themselves from the risk of liability unless they can differentiate minors from adults (or the Attorney General might adopt that interpretation). This would force users to submit to the burden of age verification and potentially forfeit anonymity as a condition of accessing fully protected speech, thus triggering strict scrutiny. *See Free Speech Coal., Inc.*, 606 U.S. at 482-83, 495.

132. In short, because the Act targets disfavored content and could effectively require age-verification to fully protect against the risk of liability, it is subject to heightened scrutiny and must be narrowly tailored.

133. The Act fails that scrutiny—and all other forms of heightened First Amendment scrutiny. Defendant cannot show that this standard "furthers a compelling interest *and is narrowly tailored to achieve that interest*." *Reed*, 576 U.S. at 171 (cleaned up; emphasis added).

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

135. The Act is overinclusive because, in practice, it governs many websites that do not pose any material risk of harm to minors—and would cover a website if even one known minor accessed the service. *See* § 39-80-10(17)(a)(i).

136. Further, because reasonable minds will disagree not only about the types of content that *are* harmful, but also about what it means to exercise "reasonable care" in the presentation or removal of protected speech, services will inevitably err on the side of removing or deprioritizing all content that *any* user could subjectively consider to be controversial or disturbing. "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*, 2025 WL 3634088, at *8. "Instead, the burden of avoiding that speech should 'normally fall upon the viewer to avoid further bombardment of (his) sensibilities simply by averting (his) eyes.'" *Id.* (cleaned up) (quoting *Erznoznik*, 422 U.S. at 210-11) (finding similar requirement "substantially overinclusive").

137. The Act is also wildly *underinclusive*, indeed irrational. Even as the Act directs websites to exercise "reasonable care" in the content they serve to minors, it hamstrings websites' ability to do that by significantly restricting personalization, one of websites' tools for ensuring

that minors receive age-appropriate content. Further, the Act allows minors to access even the most egregiously harmful content so long as the minor "search[es] for or specifically request[s]" that harmful content. § 39-80-20(C). Any argument that the State has a compelling interest in protecting minors is fatally undercut if a minor can overcome that interest with a simple search. The Act also leaves entirely *unaddressed* the same harms if they occur through offline activities or on websites that do not qualify as a covered online service.

138. Unless declared invalid and enjoined, the Act's requirement that covered services monitor and restrict fully protected speech based on a vague and content-based "reasonable care" standard will deprive Plaintiff's members and internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and internet users.

139. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 II
42 U.S.C. § 1983, 47 U.S.C. § 230, AND
***EX PARTE YOUNG* EQUITABLE CAUSE OF ACTION**
PREEMPTION UNDER THE SUPREMACY CLAUSE OF THE CONSTITUTION,
("REASONABLE CARE" STANDARD, § 39-80-20(A))
(FACIAL AND AS-APPLIED CHALLENGES)

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

141. Title 47 U.S.C. § 230 ("Section 230") also preempts the Act's requirement that covered online services "exercise reasonable care . . . to prevent [enumerated] harm[s] to minors," including "compulsive usage" and emotional distress, § 39-80-20(A)(1), (3), to the extent that doing so requires covered online services to monitor and censor content posted by third parties.

142. In Section 230, Congress protected websites' "exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content" generated by third parties. *Zeran*, 129 F.3d at 330. Congress adopted Section 230 to preserve and reinforce First Amendment protections for online services in light of the unique challenges of the medium. *E.g.*, *Bennett v. Google, LLC*, 882 F.3d 1163, 1166 (D.C. Cir. 2018).

143. 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).

144. 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).

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

146. Multiple NetChoice members operate "interactive computer service[s]" that disseminate "information provided by another information content provider." *Id.* § 230(c)(1), (f)(2). In fact, NetChoice members disseminate billions of posts of third-party content. *See Moody*, 603 U.S. at 734.

147. NetChoice members cannot evaluate whether their "design," "operation," or "use of . . . personal data" satisfies the "reasonable care" standard under § 39-80-20(A), "without also

demonstrating that the [website] prioritizes the dissemination of *one type of content over another*." *Pinckney*, 127 F.4th at 525 (emphasis added).

148. The Act thus requires covered services to monitor and police third-party speech, in violation of Section 230. The Act would also penalize websites for their exercise of traditional editorial functions.

149. Indeed, South Carolina manifestly understood that this requirement would conflict with Section 230, as the Legislature attempted to avoid the Supremacy Clause by providing that "harm" as "defined in this section is limited to those for which liability is permitted under [Section 230], including as that provision is amended or repealed in the future." § 39-80-20(B). But this provision simply injects further confusion and incoherence into the Act. Section 230 does not describe specific harms for which liability is permitted; rather, it provides a general presumption that "*no liability may be imposed*" for the dissemination of third-party content. 47 U.S.C. § 230(e)(3) (emphasis added).

150. In any event, South Carolina's feeble "attempt to immunize the [Act] from review through a savings clause" that "would nullify the 'clear and specific' substantive provisions of the" Act must be rejected. *HIAS, Inc. v. Trump*, 985 F.3d 309, 325 (4th Cir. 2021). Courts have "repeatedly rejected the argument that simply including 'consistent with applicable law' or a similar boilerplate phrase inoculates an otherwise unconstitutional [law] from judicial review." *PFLAG, Inc. v. Trump*, 766 F. Supp. 3d 535, 562 (D. Md. 2025).

151. Accordingly, the Act is preempted to the extent that it regulates NetChoice members' exercise of traditional editorial functions.

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

153. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 III
42 U.S.C. § 1983
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT
(RESTRICTIONS ON PERSONALIZATION, §§ 39-80-30(B), 39-80-40(F))
(FACIAL AND AS-APPLIED CHALLENGES)

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

155. Plaintiff members exercise expressive choices and engage in expressive conduct in the way they build their websites to disseminate billions of posts of protected speech.

156. "Laws enacted to control or suppress speech may operate at different points in the speech process." *Citizens United v. FEC*, 558 U.S. 310, 336 (2010). The Supreme Court has therefore recognized that "regulation of a medium [of expression] inevitably affects communication itself." *City of Ladue v. Gilleo*, 512 U.S. 43, 48 (1994).

157. Plaintiff members' decisions about "whether—*and, if so, how*—to convey posts having a certain content or viewpoint" is protected expression. *Moody*, 603 U.S. at 738 (emphasis added). "Those [editorial] choices rest on a set of beliefs about which messages are appropriate and which are not (or which are more appropriate and which less so). And in the aggregate they give the [social media] feed a particular expressive quality." *Id.*

158. The choice to personalize content in the first place is a protected editorial decision. And websites' design, implementation, and oversight of personalization algorithms each involve

numerous, ongoing expressive judgments about the kinds of speech offerings websites want to provide to their users.

159. NetChoice members use information collected from their users—along with a range of other expressive considerations—to deliver content that will be most beneficial to their users, that their users want to see, and that comport with members' values, beliefs, and editorial choices. For example, in addition to user information, services might assign content "scores" or ratings based on content quality, interactive feedback, recommendations, community guidelines, and their own content moderation and review activities. These selection, scoring, ranking, and organization processes reflect ongoing discretionary decisions and human-driven editorial judgments that are quintessential aspects of publishing speech and are protected by the First Amendment.

160. Online services that personalize content for users "are in the business, when curating their feeds, of combining 'multifarious voices' to create a distinctive expressive offering. The individual messages may originate with third parties, but the larger offering is the platform's. . . . And in the aggregate they give the feed a particular expressive quality." *Moody*, 603 U.S. at 738 (citation omitted).

161. The Act's requirement that covered online services "must provide to a user the option to opt out of personalized recommendation systems," § 39-80-30(B), directly infringes on a covered online service's choice in how to "combin[e] 'multifarious voices' to create a distinctive expressive offering." *Moody*, 603 U.S. at 738.

162. Similarly, the Act prohibits online services from exercising their First Amendment right to collect and utilize a minor's data to provide that minor with an experience curated to their "personal preferences, interests, . . . behavior, location, or movements," what the Act calls "profil[ing]," § 39-80-10(15), unless such profiling is "necessary to providing the covered online

service with which [sic] a minor has knowingly requested"—and even then only as to "aspects of the covered online service with which a minor is actively and knowingly engaged." § 39-80-40(F). The Act does not define what it means to be "necessary" to provide a covered service. Indeed, personalization *is* a necessary feature for many covered features because it helps users find relevant, appropriate content and makes the service useful. But the subtext of the Act makes clear that South Carolina believes such personalization is *not* necessary.

163. Although the meaning of all of these terms is vague and inherently subjective and open to interpretation, what is clear is that covered websites that engage in personalization will need to fundamentally reshape their services. For example: they will need to offer an alternative user interface; present that new interface by default for known minors; and obtain express and "knowing[]" requests from known minors to use personalized features that would help deliver content that matches the minor's interests. *See* § 39-80-40(F). This will significantly affect how services present content. It will also require websites to expend significant resources building and testing new systems, designing new interfaces and presentations of content, and reallocating or hiring new staff (among other compliance costs).

164. As discussed above, this prohibition also entirely *undercuts* the Act's purported goal of protecting minors because it removes one of the most important tools websites have for ensuring that minor users receive age-appropriate content.

165. The Act's prohibition on how Plaintiff's member websites may use data to communicate fully protected speech and expressive conduct with minors, § 39-80-40(F), and its requirement that covered websites must create a version of their service with an "off-switch" for protected speech, § 39-80-30(B), each violate the First Amendment.

166. These restrictions also violate the First Amendment rights of covered websites' users because they burden access to lawful and protected speech.

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

168. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT
(RESTRICTIONS ON DEFAULT TOOLS, § 39-80-30(A), (C))
(FACIAL AND AS-APPLIED CHALLENGES)

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

170. Covered websites, including Plaintiff's members, exercise protected expressive judgment by providing features to communicate with their users, organize and present content, and allow their users to communicate with each other.

171. The number and type of features that websites decide to offer is itself an expressive choice.

172. The speech that websites "engage in when they make decisions about *how to construct and operate* their platforms . . . is protected speech" under the First Amendment. *Reyes*, 2024 WL 4135626, at *8 (emphasis added).

173. Choices made by expressive services about how to present content to the public are "the product of a wealth of choices about whether—*and, if so, how*—to convey posts having a certain content or viewpoint." *Moody*, 603 U.S. at 738 (emphasis added).

174. The Act would require covered services to provide all users the ability to alter and undermine these expressive choices by, among other things, "disabl[ing]" them unless "necessary"; "limit[ing] the amount of time the user spends on [them]"; blocking, disabling, and rendering nonvisible "messaging, requests, reactions, likes, comments, or other contact" from unconnected accounts; "restrict[ing] the visibility of [a] minor's account and information posted by the minor to only users with connected accounts"; blocking, disabling, and rendering nonvisible "quantification of engagement"; "disabl[ing] search engine indexing of a user's account profile"; and "prohibit[ing] any other individual from viewing the user's connections to other users, regardless of the nature of the connection." § 39-80-30(A)(1)-(2), (4)-(8).

175. The Act requires covered websites to turn on by default for minor users all the requirements in § 39-80-30(A). § 39-80-30(C).

176. These requirements impermissibly interfere with covered online services' right to present a distinctive speech offering to willing users on their websites.

177. These requirements also violate the First Amendment rights of covered websites' users, because they burden users' access to protected First Amendment speech.

178. For example, "[l]ike counts are 'speech with a particular content,'" so telling a website that "it cannot tell the minor [service user] the number of likes or feedback that the [minor's] post has received" "is content discrimination" that triggers and fails strict scrutiny. *NetChoice, LLC v. Bonta*, 152 F.4th 1002, 1016 (9th Cir. 2025) ("*Bonta II*") (enjoining a similar state law's similar requirements).

179. The Act violates the First Amendment to the extent it interferes with protected, expressive decisions like a website's choice to display "likes, comments, clicks, views, or reactions regarding any item generated by the user." *See, e.g.*, § 39-80-30(A)(6). This is particularly true where the Act mandates that these protected features be defaulted "off." § 39-80-30(C). It is also true for adults by mandating that sites offer "easy-to-use tools" to disable their expressive choices. § 39-80-30(A).

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

181. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 V
42 U.S.C. § 1983
VOID FOR VAGUENESS UNDER THE FIRST AND FOURTEENTH AMENDMENTS
(ALL CHALLENGED SPEECH RESTRICTIONS,
§§ 39-80-20, 39-80-30(A)-(C), 39-80-40, 39-80-60)
(FACIAL AND AS-APPLIED CHALLENGES)

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

183. 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." *Williams*, 553 U.S. at 304.

184. Standards of vagueness are more stringent where First Amendment interests are at play. *See Fox Television Stations, Inc.*, 567 U.S. at 253-54. "When a statute 'is capable of reaching expression sheltered by the First Amendment, the [vagueness] doctrine demands a greater degree

of specificity than in other contexts.'" *Ctr. for Individual Freedom, Inc. v. Tennant*, 706 F.3d 270, 280 (4th Cir. 2013) (alteration in original) (quoting *Smith v. Goguen*, 415 U.S. 566, 573 (1974)).

185. Here, all the Act's challenged speech provisions described in these Counts are impermissibly vague and thus violate the First and Fourteenth Amendments.

186. To begin, all of the Act's challenged speech restrictions are invalid because they turn on inherently subjective and abstract definitions.

187. For example, "compulsive usage" turns on whether use "substantially limits" "major life activities," but it provides no workable standard for when a feature crosses the line. § 39-80-10(1).

188. "Covered design feature" hinges on whether a feature "will encourage or increase" a minor's "frequency, time spent, or activity," but those verbs will vary among users and contexts and have no fixed and ascertainable meaning. § 39-80-10(3). And the Act's "reasonable care" requirements are not even limited to those undefined "covered design[] features." *Id.* Instead they encompass a broader (and likewise undefined) set of choices websites make when they disseminate expression. Regardless, whether a minor develops "compulsive usage" under the Act will inevitably depend, in whole or in part, on the content the minor views on the service, because no minor would foreseeably develop "persistent and repetitive" use that "substantially limits" "major life activities" if the service displayed only irrelevant or uninteresting material, such as dictionary text, random strings of words, or long excerpts of legislative coverage. § 39-80-10(1); § 39-80-20(A)(1). But a minor could easily spend hours engaging with compelling and beneficial content, such as science lessons, music performances, sports highlights, or other educational or cultural material, and that response would depend on individual tastes and circumstances. § 39-80-10(1). A person of ordinary intelligence cannot know, *ex ante*, whether a particular design practice or

feature will cause "compulsive usage" or "severe psychological harm," because the Act offers no workable, objective way to predict those outcomes across millions of minors with widely varying ages, maturity, and susceptibilities, and those reactions will vary based on factors a website cannot know. § 39-80-20(A)(1)-(3); § 39-80-10(1).

189. "Gamification" sweeps in any feature that "emulates gameplay" and "motivate[s] or cause[s]" more use, again with no clear boundary. § 39-80-10(3).

190. "Expressed preferences" demands a "freely given, considered, specific, and unambiguous" indication while excluding common signals that communicate that assent, thus leaving unclear what qualifies. § 39-80-10(6).

191. And "known to be a minor" expands "actual knowledge" to "all information and *inferences*" relating to age, including ages "attributed or associated" "for any purpose," which once again makes the trigger for liability itself uncertain. § 39-80-10(7); § 39-80-10(17)(b).

192. The Act's challenged speech restrictions also impose substantive requirements that are themselves unconstitutionally vague.

193. The Act requires that covered websites shall exercise "reasonable care in the use of a minor's personal data and the design and operation of the covered online service including, but not limited to, covered design features, to prevent . . . harm[s] to minors." § 39-80-20(A). The "reasonable care," § 39-80-20(A), standard creates no ascertainable standard of conduct other than imposing liability based on the "impact that speech has on its listeners," *Playboy Ent. Grp.*, 529 U.S. at 811. This will require covered services to guess how billions of posts of content will affect millions of their minor users. The Act provides no guidance on how covered online services are supposed to execute those predictions. Specifically, the Act fails to define the necessary link between a website's "operation" and "covered design features" and the Act's enumerated harms.

Further, the Act does not explain what type, or how much, of any given action a covered service might take that would satisfy the "reasonable care" standard. Nor could it because this term is highly subjective, context-dependent, and personalized.

194. Because covered websites have no way of definitively knowing what content the State will find harmful, and whether their efforts are "reasonable," websites are incentivized to remove more speech to protect against liability. The Act thus creates a "one-way ratchet" in favor of censorship because covered services will never be penalized for removing more content or features, but they might be penalized for delivering such content to minors.

195. Beyond the "reasonable care" standard, some of the "harm[s]" that covered services must "prevent" are also impermissibly vague. *See* § 39-80-20(A)(1)-(7).

196. Covered online services have no way to ensure that the content and features on their sites will not be deemed to result in "harm," no matter how they modify their operations or design features. *See Bonta I*, 113 F.4th at 1122 (finding impermissible vagueness where "the relevant provisions are worded at such a high level of generality that they provide little help to businesses in identifying which of those practices or designs may actually harm children"); *Griffin III*, 2025 WL 3634088, at *13 ("The Supreme Court has therefore consistently struck down laws that restricted otherwise protected speech based solely on its impact on the feelings and conduct of others.").

197. Consider "compulsive usage." § 39-80-20(A)(1). The line between a covered online service's effective design (on the one hand) and impermissibly causing "compulsive usage" (on the other) is undefined. It is entirely vague when a computer game becomes "too fun" such that a website offering that game violates a law against "compulsive usage."

198. The same vagueness concern applies to other of the Act's identified harms, like "severe psychological harm," § 39-80-20(A)(2), and "severe emotional distress." § 39-80-20(A)(3). Certainly, an online reading group discussing Anne Frank's *The Diary of a Young Girl* would cause some level of emotional and psychological distress, but covered services have no way to know whether this content rises to the level of "severe" "psychological harm" or "emotional distress" such that a service is failing to "exercise reasonable care" by allowing the group to continue. Further, as discussed above, the level of distress that might arise from different content and features is likely user-specific and age-specific, meaning there is no standard metric by which covered online services can assess compliance.

199. Additionally, it is unclear how covered online services are to evaluate whether the use of personal data will result in "highly offensive intrusions on the minor's reasonable privacy expectations." § 39-80-20(A)(4). Neither "highly offensive" nor the "reasonable privacy expectations," *id.*, of minors are defined. And the Supreme Court has said that privacy expectations for minors of different ages may well be different. *See Reno*, 521 U.S. at 865-66.

200. The Act's blunderbuss approach to age, grouping toddlers with those a day shy of legal adulthood, goes against the Supreme Court's guidance, which has emphasized the importance of "tak[ing] into account juveniles' differing ages and levels of maturity" in the First Amendment context. *Am. Booksellers*, 484 U.S. at 396. Yet the Act flattens all minors—including young people a day shy of their eighteenth birthday—into a single mass and requires covered entities to evaluate what might cause "harm" to any of those "minors" based on the lowest common denominator.

201. When combined with the Act's vague categories of harm, South Carolina's sweeping definition of "minor" multiplies the sheer number of indeterminate analyses covered entities must engage in and heightens the confusion about what those analyses will require. The

resulting uncertainty will encourage covered entities to assess the risks and implement content restrictions based on the most sensitive and youngest users, defaulting to the most restrictive possible understandings of the Act to avoid liability.

202. Of course, South Carolina already prohibits discrimination through its separate, generally applicable antidiscrimination law. *See* § 1-13-20 (declaring "the practice of discrimination against an individual because of race, religion, color, sex, age, national origin, or disability as a matter of state concern and declares that this discrimination is unlawful"). Yet the Act adds to those existing requirements with an additional, vague command, seemingly untethered to—or at least distinct from—those existing prohibitions.

203. South Carolina's effort to avoid Section 230 by defining "harm" in terms of "liability . . . permitted" under Section 230, § 39-80-20(B) injects further uncertainty and incoherence into the Act's statutory scheme. First, Section 230 forecloses virtually *any* liability for protected third-party content, so this part of the Act's scheme undercuts the plain text that surrounds it. Second, this aspect of the duty would require regulated entities to guess at how courts will resolve hotly-litigated legal questions about Section 230's scope and risk significant liability if they are incorrect. This uncertainty entirely undercuts the purpose and protection of Section 230. Third, by indexing websites' duty of care to issues of federal law—and incorporating a hope that Congress might amend or change that law in the future—this provision fails to give regulated entities sufficiently concrete guidance to structure their activities *now*.

204. The Act's other substantive requirements also turn on undefined standards that invite arbitrary enforcement. The "tools" requirement compels services to offer tools to disable design features "that are not necessary to provide the covered online service," but the Act never defines what is "necessary" or what "design features" means. This leaves covered services unsure

whether core expressive functions count as optional or required. § 39-80-30(A)(1). The same undefined "necessary" limitation appears again in the profiling restriction, where liability turns on whether profiling is "necessary to providing the covered online service" that a minor has "knowingly requested." § 39-80-30(F). The data provisions likewise rely on undefined concepts, including mandates about what is "easy-to-use" and "easily accessible," again with no objective criteria to determine compliance. § 39-80-30(A); § 39-80-40(F). Covered websites have no way to know what any of this means.

205. Finally, all of the Act's challenged speech restrictions are unconstitutionally vague because their enforcement relies on an unconstitutionally vague enforcement standard.

206. The Act provides that the Attorney General "shall enforce" it, that a covered service is "liable for treble the financial damages incurred" from a violation, and that "officers and employees" may be "personally liable" for "wilful and wanton violations." § 39-80-80. It does so without clearly identifying what conduct triggers damages, how damages would be measured for many mandates, or what enforcement theory will be used. That uncertainty magnifies the constitutional defect because covered services facing vague speech restrictions must predict not only what the Act requires, but also what penalties the State will pursue if they guess wrong. As a result, services will predictably disable speech-facilitating features, suppress lawful content, and restrict access for users who could be minors to avoid ruinous damages and the threat of *personal* liability for their employees. § 39-80-80.

207. All this ambiguity "is so standardless that it authorizes or encourages seriously discriminatory enforcement." *Williams*, 553 U.S. at 304. South Carolina has unlimited discretion to identify content it disfavors and bring an enforcement action against a website for disseminating

that content because, in the State's view, the website failed to "exercise reasonable care" in permitting the "harm[ful]" content on its website. § 39-80-20.

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

209. That South Carolina used the term "reasonable" to qualify covered online services' duties under the Act does not cure the ambiguity. If anything, it *amplifies* the vagueness problems by tethering liability for protected speech to inherently subjective, highly controversial, and ever-changing norms. *See Bonta I*, 113 F.4th at 1120 (explaining that whether online services might result in harm to minors presented "highly controversial issues of public concern").

210. In the tort context, whether behavior is "reasonable" in a particular context has been defined by hundreds of years of case law and often requires a jury trial to resolve definitively. The concept is further constrained by elements of foreseeability, proximate causation, and legally cognizable harm. The Act here transposes the concept of "care" onto protected expression—a context in which it has no historical application or clear meaning (and indeed is highly controversial)—and omits the mens rea, causation, and harm requirements. § 39-80-20(A).

211. Courts have repeatedly rejected efforts to transplant common-law tort concepts to speech. *See Snyder v. Phelps*, 562 U.S. 443, 458 (2011) ("outrageous" was too "malleable" a standard to impose liability for speech); *Hustler Mag., Inc. v. Falwell*, 485 U.S. 46, 47 (1988) ("'[o]utrageousness' . . . has an inherent subjectiveness about it"). And the Supreme Court has recently rejected holding defendants liable for their speech under a "negligence" standard, *i.e.*, imposing culpability for "a bad mistake"; instead it has required the more demanding "recklessness" standard, which requires "a deliberate decision" by the defendant to endanger someone. *Counterman v. Colorado*, 600 U.S. 66, 79-80 (2023) (cleaned up); *see id.* at 79 n.5.

212. The First Amendment forbids States from imposing liability for disseminating even *unprotected* speech unless the publishers know the nature of the allegedly unprotected speech. *Smith v. California*, 361 U.S. 147, 152 (1959). Negligence is not enough. *Counterman*, 600 U.S. at 79 & n.5. That is why courts have rejected liability for disseminating speech based on reactions not already subsumed within well-defined First Amendment exceptions (such as defamation and fighting words). *See, e.g.*, *Herceg v. Hustler Mag., Inc.*, 814 F.2d 1017, 1020, 1022-24 (5th Cir. 1987); *McCollum v. CBS, Inc.*, 202 Cal. App. 3d 989, 1000-01 (1988).

213. 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.

214. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 VI
42 U.S.C. § 1983
VIOLATION OF THE FIRST AMENDMENT, AS INCORPORATED AGAINST THE STATES BY THE FOURTEENTH AMENDMENT
(COMPELLED SPEECH VIA THIRD PARTY AUDITOR, § 39-80-70)
(FACIAL AND AS-APPLIED CHALLENGES)

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

216. It "is well-established that the First Amendment protects 'the right to refrain from speaking at all.'" *Bonta I*, 113 F.4th at 1117 (quoting *Wooley v. Maynard*, 430 U.S. 705, 714 (1977)). That is true even when the government does not compel *public* speech. The "Supreme Court has recognized the First Amendment may apply even when the compelled speech need only

be disclosed to the government." *Id.* at 1117-18. Likewise, it is true when the government compels private entities to disseminate the speech of others. *E.g.*, *Hurley v. Irish-Am. Gay, Lesbian and Bisexual Grp. of Boston, Inc.*, 515 U.S. 557, 575-76 (1995); *Pacific Gas & Elec. Co. v. Pub. Utils. Comm'n*, 475 U.S. 1, 11-12 (1986) (plurality op.); *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 258 (1974).

217. The Act's third-party audit requirements, § 39-80-70, violate the First Amendment both facially and as applied to NetChoice's covered members.

218. Section 39-80-70 requires websites to speak to third-party auditors, facilitate those audits, and "issue a public report prepared by [the] independent third-party auditor that contains a detailed description" of the service "as it pertains to minors," including the service's "purpose," the extent to which it is accessed by minors, how the service handles and protects data, the number of harm reports received by the service, "whether and how the service uses covered design features," and the "age verification or estimation methods" and "algorithms" used by the service (among a few others). § 39-80-70.

219. Laws compelling companies to convey "policy views on intensely debated and politically fraught topics . . . and . . . how the company . . . applie[s] its policies," are subject to strict scrutiny. *X Corp.*, 116 F.4th at 901-02 (mandatory reports requiring the company to "*implicitly* opin[e] on whether and how certain controversial categories of content should be moderated" were likely unconstitutional (emphasis added)). The Ninth Circuit has therefore held that California's similar compelled-speech and censorship requirements violate the First Amendment. *Bonta I*, 113 F.4th at 1116-22 ("It is . . . well-established that the forced disclosure of information, even purely commercial information, triggers First Amendment scrutiny.").

220. A law "[m]andating speech that a speaker would not otherwise make" is a "content-based regulation of speech" subject to strict scrutiny because it "alters the content of the speech." *Riley*, 487 U.S. at 795.

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

222. Specifically, the Act requires covered websites to embrace (by themselves "issu[ing]") the opinions of outside auditors addressing all manner of sensitive topics on the websites' safety for minors, including the website's "design safety," "privacy protections," and an "assessment" of how "reports [documenting harms to minors] were handled." § 39-80-70(A).

223. The Act thus necessarily operates as a content-based regulation because it alters the content of speech—specifically, § 39-80-70(A)(3) requires covered online services to broadcast to the public, where, despite a website's best efforts, its service was involved in harm to a minor.

224. What is worse, the third-party audit detailing those harms "must be submitted to the Attorney General who *shall* post it in a prominent place on his internet website." § 39-80-70(A) (emphasis added).

225. Both by requiring covered entities to "issue" the reports and by requiring websites to convey the reports to the South Carolina Attorney General for public posting and consumption, the Act thus "[r]equir[es] a company to *publicly* condemn itself," which is "more constitutionally offensive." *Nat'l Ass'n of Mfrs. v. SEC*, 800 F.3d 518, 530 (D.C. Cir. 2015) (emphasis added; quotations omitted).

226. Because the audit is content-based and compels speech, it triggers strict scrutiny.

227. The audit requirement fails strict scrutiny.

228. The audit requirement also fails all other forms of heightened First Amendment scrutiny, including intermediate scrutiny and scrutiny of laws that compel commercial speech.

229. Unless declared invalid and enjoined, the Act's compelled speech requirements will deprive Plaintiff's members and internet users of their fundamental First Amendment rights and will irreparably harm Plaintiff, its members, and internet users.

230. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 VII
42 U.S.C. § 1983, 47 U.S.C. § 230, AND
***EX PARTE YOUNG* EQUITABLE CAUSE OF ACTION**
PREEMPTION UNDER THE SUPREMACY CLAUSE OF THE CONSTITUTION,
(FACILITATING ADS, § 39-80-60(B))
(FACIAL AND AS-APPLIED CHALLENGES)

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

232. Some of Plaintiff's covered members offer advertising services to third parties.

233. The Act prohibits covered online services "from facilitating ads directed to [known] minors" for products that are illegal for minors, such as narcotic drugs, alcohol, and gambling. § 39-80-60(B).

234. The Act's use of "facilitat[e]," means it is not enough for covered online services to themselves abstain from showing prohibited advertisements to children. Nor is it enough for covered services to prohibit such advertisements by third party advertisers. Rather, covered services must *definitively ensure* that third parties never publish such ads, otherwise the covered service would be "facilitating" those ads, even if unintentionally.

235. But Section 230's "language establishes broad immunity from any cause of action that would make service providers liable for information originating with a third-party user of the service," so long as the claims "are based on the interactive computer service provider's publication of a third party's speech." *Pinckney*, 127 F.4th at 524 (cleaned up).

236. The Act mandates that Plaintiff members view and evaluate the content of third-party ads to see if the content relates to activities that are unlawful for minors (even if lawful for adults).

237. Plaintiff members make extensive efforts to avoid advertising age-restricted and illegal products to minors. But the Act requires much more. It requires perfect monitoring of third parties to ensure compliance, because even one failure could create massive institutional and personal liability. Thus "it is reasonable to expect that companies will adopt broad definitions that do encompass such plainly protected" advertisements. *CCIA*, 747 F. Supp. 3d at 1040.

238. Moreover, the Act lacks any mens rea requirement, so it imposes a strict liability regime on covered services both to monitor the content on their services and to prevent *all* prohibited ads. § 39-80-60(B).

239. Section 230 says that covered online services shall not be held liable for third-party speech, including advertisements, on their platforms.

240. South Carolina's Act says the opposite, that covered services *are* strictly liable for some third-party speech on their platforms, even if websites are actively trying to avoid such advertisements.

241. South Carolina's Act thus directly conflicts with Section 230 and is expressly preempted by Section 230.

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

243. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, 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 VIII
42 U.S.C. § 1983, 15 U.S.C. §§ 6501, ET SEQ.
***EX PARTE YOUNG* EQUITABLE CAUSE OF ACTION**
PREEMPTION UNDER THE SUPREMACY CLAUSE OF THE CONSTITUTION
(§§ 39-80-20, 39-80-40, 39-80-60)
(FACIAL AND AS-APPLIED CHALLENGES)

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

245. Sections 39-80-20 (mandating "reasonable care" to prevent "harm[s]" to minors), 39-80-40 (regulating collection and use of minors' data), and 39-80-60 (regulating advertisements to minors) of the Act are preempted by COPPA.

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

247. COPPA and the COPPA Rule regulate websites that are "directed to children" or have "*actual knowledge* [they are] collect[ing] [personal information] from a child." 15 U.S.C. § 6501(4)(B) (emphasis added). COPPA prohibits such data collection unless websites "[p]rovide notice on the website or online service of what information" they collect and how they use and

disclose it, 16 C.F.R. § 312.3(a), and "obtain verifiable parental consent." *Id.* § 312.5(a)(1). COPPA does not impose other conditions or substantive restrictions on the use of minors' data.

248. COPPA says that "[n]o State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is *inconsistent* with the treatment of those activities or actions under this section." 15 U.S.C. § 6502(d) (emphasis added).

249. In general, COPPA's "treatment" in connection with the use of minors' data is to require notice and parental consent for children under 13. *Id.* § 6501(1). Congress chose not to regulate teenagers from 13 to 17 years of age. And for younger children, Congress chose to place the decision-making where it should be—with parents and guardians. COPPA does not impose other conditions or substantive restrictions.

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

251. The Act's various regulations of teenagers (minors aged 13 to 17)—their personal data (§ 39-80-20(A)), the online tools and communicative features teenagers are allowed to see (§ 39-80-30(A)), the information allowed to be collected from them (§ 39-80-40), and the advertisements covered online services and third parties may show teenagers (§ 39-80-60)—are thus "inconsistent" with Congress's preemptive determination to regulate only interactions with minors younger than 13.

252. Additionally, as a condition of using minors' data, South Carolina's Act imposes several substantive requirements that COPPA does not. For example, the Act requires services to determine what content *might*, at some time in the future, cause harm to an unspecified minor and to remove or deprioritize that content so minors cannot see or use it, § 39-80-20(A).

253. Because COPPA would permit covered online services to use minors' data without these requirements, the Act is inconsistent with and preempted by COPPA.

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

255. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, 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 IX
42 U.S.C. § 1983
VIOLATION OF THE COMMERCE CLAUSE OF THE U.S. CONSTITUTION
(TITLE 39, SECTION 80)
(FACIAL AND AS-APPLIED CHALLENGES)

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

257. 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, or discriminate against interstate commerce. *Okla. Tax Comm'n v. Jefferson Lines, Inc.*, 514 U.S. 175, 179 (1995).

258. Even laws that regulate evenhandedly and do not discriminate against other States are unconstitutional if they impose burdens on interstate commerce that are clearly excessive in relation to the putative local benefits. *See Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970). The Commerce Clause likewise prohibits States from regulating activities, including speech, when

the "practical effect of the regulation is to control conduct" that occurs "wholly outside" the regulating State's jurisdiction. *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989).

259. As the Supreme Court recently explained, while laws that regulate in-state conduct with some extraterritorial effect may pass constitutional muster, 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). Indeed, both the Supreme Court and the Fourth Circuit have long held the latter unconstitutional. *See Edgar v. MITE Corp.*, 457 U.S. 624, 640, 642 (1982) (controlling plurality opinion) (explaining that the Commerce Clause "precludes the application of a state statute to commerce that takes place wholly outside of the State's borders"); *Ass'n of Accessible Medicines v. Frosh*, 887 F.3d 664, 669, 670-72 (4th Cir. 2018) (holding a Maryland law unconstitutional because it regulated "conduct that occur[red] entirely outside Maryland's borders").

260. 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"); *United States v. Carroll*, 105 F.3d 740, 742 (1st Cir. 1997) ("Transmission of [information] by means of the Internet . . . constitutes transportation in interstate commerce." (citing *United States v. Thomas*, 74 F.3d 701, 706-07 (6th Cir. 1996))); *United States v. Runyan*, 290 F.3d 223, 239 (5th Cir. 2002) ("Internet transmission, in and of itself, constitutes interstate transportation sufficient to [constitute] interstate commerce").

261. Online services would be far less useful to interstate commerce if website operators were required to develop entirely different services—with different content, different interfaces,

different communication functionalities, different visibility, different sharing restrictions, and different expressive features—in each State. *See Am. Booksellers Found. v. Dean*, 342 F.3d 96, 104 (2d Cir. 2003) (internet communications "fall[] within the class of subjects that are protected from State regulation because they 'imperatively demand a single uniform rule'" (cleaned up)).

262. For these reasons, both the Fourth Circuit and this Court have invalidated laws prohibiting online dissemination of information that is harmful to minors. *See PSINet*, 362 F.3d at 240; *Se. Booksellers Ass'n v. McMaster*, 371 F. Supp. 2d 773, 787-88 (D.S.C. 2005) (permanently enjoining a South Carolina law that prohibited the online dissemination of "harmful material to minors" because "[g]iven the broad reach of the Internet, it is difficult to see how a blanket regulation of Internet material . . . can be construed to have only a local effect").

263. Because the internet is an inherently borderless technology, "[h]aphazard and uncoordinated state regulation can only frustrate the growth of cyberspace," which is why the "Internet . . . requires a cohesive national scheme of regulation." *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 182-83 (S.D.N.Y. 1997).

264. Congress recognized the interstate nature of the internet when it enacted Section 230 and COPPA. In Congress's words: the internet has "flourished, to the benefit of all Americans, with a minimum of government regulation." 47 U.S.C. § 230(a)(4). To "promote the continued development of the Internet," Congress declared 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*." *Id.* § 230(b) (emphasis added).

265. That hands-off federal policy has worked: The internet has grown tremendously over the past few decades, fostering "a revolution of historic proportions." *Packingham*, 582 U.S. at 105. The online services regulated by this Act have facilitated trillions of dollars in commerce,

provided hundreds of millions of Americans with access to information, and helped billions of people across the globe communicate almost instantaneously.

266. This Act's far-reaching and proscriptive mandates are fundamentally inconsistent with that cohesive national scheme. Indeed, if other States follow South Carolina's lead, online information, contacts, content, communications, and features available to users will depend on the State they reside in and the internet will be fragmented by state lines.

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

268. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 X
42 U.S.C. § 1983
VIOLATION OF THE FOURTEENTH AMENDMENT'S DUE PROCESS CLAUSE
(TITLE 39, CHAPTER 80)
(FACIAL AND AS-APPLIED CHALLENGES)

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

270. South Carolina's Act became law and took *immediate effect* upon the Governor's signature on February 5, 2026. *See* HB 3431 § 4 ("This act takes effect upon approval by the Governor.").

271. Covered online services had almost no opportunity to analyze the Act's requirements, consider compliance options, or conform their conduct to the Act's requirements before it became effective. Nor does the Act provide for a cure period before liability can be incurred. No exigencies or change in circumstances even remotely required South Carolina to take immediate action or demand compliance immediately.

272. The Act therefore puts covered online services to an impermissible choice: either cease to engage in First Amendment "protected speech," *Moody*, 603 U.S. at 738-39, or continue with longstanding operations that previously were lawful but suddenly violate this new Act. *See Packingham*, 582 U.S. at 109 (The "State may not enact this complete bar to the exercise of First Amendment rights on websites integral to the fabric of our modern society and culture."). The Due Process Clause bars a State from putting citizens to that Hobson's choice.

273. "In altering substantive rights through enactment of rules of general applicability, a legislature generally provides constitutionally adequate process simply by enacting the statute, publishing it, *and, to the extent the statute regulates private conduct*, affording those within the statute's reach a reasonable opportunity *both to familiarize themselves with the general requirements imposed and to comply with those requirements*." *United States v. Locke*, 471 U.S. 84, 108 (1985) (emphases added) (citing *Anderson Nat'l Bank v. Luckett*, 321 U.S. 233, 243 (1944); *N. Laramie Land Co. v. Hoffman*, 268 U.S. 276, 283 (1925)).

274. "The demands of due process are satisfied if a reasonably clear definition is afforded *in time to give the taxpayer an opportunity to comply*." *Pac. Tel. & Tel. Co. v. City of Seattle, Wash.*, 291 U.S. 300, 304 (1934) (emphasis added); *see also Planned Parenthood Great Nw., Haw., Alaska, Ind., & Ky., Inc. v. Cameron*, 599 F. Supp. 3d 497, 501-02 (W.D. Ky. 2022) (granting TRO "based on the impossibility of compliance" where law likely violated due process "[b]y taking effect immediately, without providing Plaintiff and other abortion providers time to comply"); *Jones v. United States*, 121 F.3d 1327, 1329-30 (9th Cir. 1997) (finding 11 months satisfied the requirement that "[i]n order to comply with due process in connection with [a new enactment], the government was required to 'afford the citizenry a reasonable opportunity to familiarize itself with [the Act's] terms and to comply'" (citation omitted)); *Herschfus v. City of*

Oak Park, 718 F. Supp. 3d 707, 717 (E.D. Mich. 2024) (assuming that due process would require a "reasonable time to . . . bring [activities] . . . into compliance" with regulatory requirements and finding such requirement met by "a full year" of notice).

275. In addition to covered online services, the immediate liability under the Act violates the First Amendment rights of users in addition to the rights of the covered online services. So NetChoice members here can raise the protected free-speech interests of their users to challenge the general "abridg[ment of] expression that the First Amendment was meant to protect." *First Nat. Bank of Bos. v. Bellotti*, 435 U.S. 765, 776, 780 (1978) (free speech has "always been viewed as fundamental components of the liberty safeguarded by the Due Process Clause, . . . and the Court has not identified a separate source for the right when it has been asserted by corporations").

276. In addition to protected liberty interests, NetChoice members also have protected property interests in the operation of their businesses, and those property interests independently warrant due process protections. "A business is an established property right entitled to protection under the Fourteenth Amendment." *S. Allegheny Pittsburgh Rest. Enters., LLC v. City of Pittsburgh*, 806 F. App'x 134, 139 (3d Cir. 2020) (cleaned up). "If a plaintiff has a property interest and [a court] deem[s] it deserves protection, [the court] review[s] the procedures (that is, the process) constitutionally needed to assure protection and whether they were provided." *Id.*

277. The Act's immediate effective date here violated NetChoice members' right to due process to protect their property interests in their covered online services. *See Loudermill v. Cleveland Bd. of Educ.*, 721 F.2d 550, 560 (6th Cir. 1983), *aff'd and remanded*, 470 U.S. 532 (1985) ("federal due process rights, which may not be the same as state procedural guarantees, must be accorded before a state deprives one of a property interest").

278. Unless declared invalid and enjoined, the Act will deprive Plaintiff's members and internet users of their fundamental due process rights and will irreparably harm Plaintiff, its members, and internet users.

279. The Act on its face and as applied to NetChoice members and their covered services (Amazon, Automattic, Discord, Dreamwidth, Duolingo, Google, Meta, Netflix, Nextdoor, Pinterest, Reddit, Snap Inc., TikTok Inc., TikTok USDS Joint Venture LLC, and X) 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 the South Carolina Age-Appropriate Code Design 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 §§ 39-80-20(A), 39-80-30(A)-(C), 39-80-40(F), 39-80-70, violate the First Amendment to the Constitution, as incorporated against the States by the Fourteenth Amendment, both facially and to the extent they compel speech, interfere with protected editorial discretion, and restrict the collection and use of information for the purposes of curating, recommending, and delivering protected speech to users, and as applied to Plaintiff's members and their covered services listed in each count;

3. declaring that the Act as a whole and as to specific sections (§§ 39-80-20, 39-80-30(A)-(C), 39-80-40, 39-80-60) are void for vagueness under the First Amendment and the Due Process Clause of the Fourteenth Amendment to the Constitution, as incorporated against the States by the Fourteenth Amendment, both on their face and as applied to Plaintiff's members and their covered services listed in each count;

4. declaring that §§ 39-80-20, 39-80-60(B) are preempted by 47 U.S.C. § 230 both on their face and as applied to Plaintiff's members and their covered services listed in each count, to the extent that they apply to the dissemination of third-party speech;

5. declaring that §§ 39-80-20(A), 39-80-40, 39-80-60 of the Act are preempted by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06, both on their face and as applied to Plaintiff's members and their covered services listed in each count;

6. declaring that the South Carolina Age-Appropriate Code Design Act violates the Commerce Clause of the United States Constitution both on its face and as applied to Plaintiff's members and their covered services listed in each count;

7. declaring that the South Carolina Age-Appropriate Code Design Act violates the Due Process Clause of the Fourteenth Amendment to the Constitution, as incorporated against the States by the Fourteenth Amendment, both on its face and as applied to Plaintiff's members and their covered services listed in each count to the extent it requires immediate compliance without any meaningful opportunity to comply;

8. declaring that the unlawful portions of the South Carolina Age-Appropriate Code Design Act are not severable from the rest of the Act;

9. entering judgment in favor of Plaintiff and Plaintiff's members listed in each count;

10. enjoining Defendant and his 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;

11. 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

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

Dated: February 9, 2026

Respectfully submitted,

/s/ Lucy Dinkins

Lucy Dinkins
Jim May
Kathleen Stoughton
WYCHE, P.A.
807 Gervais St.
Suite 301
Columbia, SC 29211
(803) 254-6544
ldinkins@wyche.com
jmay@wyche.com
kstoughton@wyche.com

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

Joshua P. Morrow*
LEHOTSKY KELLER COHN LLP
7500 Rialto Blvd.
Suite 1-250
Austin, TX 78735
josh@lkcfirm.com

**pro hac vice forthcoming*

Exhibit A

South Carolina General Assembly
126th Session, 2025-2026

Download This Bill in Microsoft Word format

H. 3431

STATUS INFORMATION

General Bill
Sponsors: Reps. W. Newton, Wooten, Pope, Martin, Pedalino, McCravy, Bernstein, Guffey, Govan, T. Moore, Erickson, Bradley, Robbins, Calhoon, M.M. Smith and Crawford
Document Path: LC-0072SA25.docx

Introduced in the House on January 14, 2025
Introduced in the Senate on February 26, 2025
Last Amended on January 14, 2026
Passed by the General Assembly on January 21, 2026

Summary: South Carolina Social Media Regulation Act

HISTORY OF LEGISLATIVE ACTIONS

Date	Body	Action Description with journal page number
12/5/2024	House	Prefiled
12/5/2024	House	Referred to Committee on Judiciary
1/14/2025	House	Introduced and read first time (House Journal-page 199)
1/14/2025	House	Referred to Committee on Judiciary (House Journal-page 199)
1/29/2025	House	Member(s) request name added as sponsor: Bernstein, Guffey, Govan
2/4/2025	House	Member(s) request name added as sponsor: T. Moore, Erickson, Bradley
2/11/2025	House	Member(s) request name added as sponsor: Robbins
2/13/2025	House	Committee report: Favorable with amendment Judiciary (House Journal-page 25)
2/18/2025	House	Member(s) request name added as sponsor: Oremus, Hartz, Calhoon, M.M. Smith
2/18/2025		Scrivener's error corrected
2/19/2025	House	Member(s) request name removed as sponsor: Oremus
2/18/2025	House	Member(s) request name removed as sponsor: Hartz
2/19/2025	House	Requests for debate-Rep(s). Bamberg, Cromer, Gilreath, Edgerton, Magnuson, Morgan, King, Hart, Gilliaard, Rivers, White
2/19/2025	House	Member(s) request name added as sponsor: Crawford
2/19/2025	House	Amended (House Journal-page 29)
2/19/2025	House	Read second time (House Journal-page 29)
2/19/2025	House	Roll call Yeas-90 Nays-17 (House Journal-page 56)
2/20/2025	House	Read third time and sent to Senate (House Journal-page 32)

Date	Body	Action Description with journal page number
2/20/2025	House	Roll call Yeas-89 Nays-14 (House Journal-page 32)
2/21/2025		Scrivener's error corrected
2/26/2025	Senate	Introduced and read first time (Senate Journal-page 10)
2/26/2025	Senate	Referred to Committee on Labor, Commerce and Industry (Senate Journal-page 10)
4/24/2025	Senate	Committee report: Favorable with amendment Labor, Commerce and Industry (Senate Journal-page 11)
5/1/2025	Senate	Committee Amendment Adopted
5/1/2025	Senate	Amended
5/1/2025	Senate	Read second time
5/1/2025	Senate	Roll call Ayes-39 Nays-0
5/5/2025		Scrivener's error corrected
5/6/2025	Senate	Amended (Senate Journal-page 36)
5/6/2025	Senate	Read third time and returned to House with amendments (Senate Journal-page 36)
5/6/2025	Senate	Roll call Ayes-45 Nays-0 (Senate Journal-page 36)
5/12/2025		Scrivener's error corrected
1/14/2026	House	Senate amendment amended (House Journal-page 105)
1/14/2026	House	Returned to Senate with amendments (House Journal-page 105)
1/14/2026	House	Roll call Yeas-112 Nays-0 (House Journal-page 116)
1/21/2026	Senate	Concurred in House amendment and enrolled (Senate Journal-page 29)
2/3/2026		Ratified R 100
2/5/2026		Signed By Governor

View the latest legislative information at the website

VERSIONS OF THIS BILL

12/5/2024
2/13/2025
2/18/2025
2/19/2025
2/21/2025
4/24/2025
5/1/2025
5/5/2025
5/6/2025
5/12/2025
1/14/2026

NOTE: THIS IS A TEMPORARY VERSION. THIS DOCUMENT WILL REMAIN IN THIS VERSION UNTIL FINAL APPROVAL BY THE LEGISLATIVE COUNCIL.

(R100, H3431)

AN ACT TO AMEND THE SOUTH CAROLINA CODE OF LAWS BY ADDING CHAPTER 80 TO TITLE 39 SO AS TO PROVIDE THAT A COVERED ONLINE SERVICE SHALL EXERCISE REASONABLE CARE IN THE USE OF MINORS' PERSONAL DATA, TO PROVIDE FOR CERTAIN REQUIREMENTS FOR COVERED ONLINE SERVICES, TO RESTRICT THE AMOUNT OF PERSONAL DATA OF A MINOR THAT MAY BE COLLECTED, TO PROVIDE FOR PARENTAL CONTROLS, TO PROVIDE FOR AN ANNUAL REPORT, AND TO PROVIDE FOR ENFORCEMENT.

Be it enacted by the General Assembly of the State of South Carolina:

Age-Appropriate Code Design

SECTION 1. Title 39 of the S.C. Code is amended by adding:

CHAPTER 80

Age-Appropriate Code Design

Section 39-80-10. As used in this chapter:

(1) "Compulsive usage" means the persistent and repetitive use of a covered online service that substantially limits one or more of a user's major life activities including, but not limited to, sleeping, eating, learning, reading, concentrating, communicating, or working.

(2) "Connected account" means an account on a covered online service that is directly connected to:

(a) the user's account; or

(b) an account that is directly connected to the user's account.

(3) "Covered design feature" means any feature or component of a covered online service that will encourage or increase a minor's frequency, time spent, or activity on a covered online service including, but not limited to:

(a) infinite scroll or any design feature that automatically loads and displays content other

than what the user prompted, requested, or searched for;

(b) auto-playing videos or any design feature in which videos automatically begin playing when a user navigates to or scrolls through a set of videos;

(c) gamification or any design feature that emulates gameplay including, but not limited to, streaks, badges, or rewards, that motivate or cause more frequent or more extensive use of a covered online service;

(d) quantification of engagement including, but not limited to, providing a visible count of how many likes, comments, clicks, views, or reactions any user-generated item has received;

(e) notifications and push alerts;

(f) in-game purchases or any design feature in which digital items or tokens are purchased with virtual currency or other forms of payment, including where the purchased digital item can be shared with another user; or

(g) appearance-altering filters.

(4)(a) "Covered online service" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that owns, operates, controls, or provides an online service that conducts

business in this State, is reasonably likely to be accessed by minors, determines the purposes and means of the processing of consumer's personal data alone, or jointly with its affiliates, subsidiaries, or parent company and either:

(A) has annual gross revenues in excess of twenty-five million dollars, adjusted every odd-numbered year to reflect changes in the Consumer Price Index;

(B) annually buys, receives, sells, or shares the personal data of fifty thousand or more consumers, households, or devices alone or in combination with its affiliates, subsidiaries, or parent company; or

(C) derives at least fifty percent of its annual revenue from the sale or sharing of consumers' personal data; and

(b) "Covered online services" include:

(i) an entity that controls or is controlled by a business that shares a name, service mark, or trademark that would cause a reasonable consumer to understand that two or more entities are commonly owned; and

(ii) a joint venture or partnership composed of businesses in which each business has at least a forty percent interest in the joint venture or partnership.

(5) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(6)(a) "Expressed preferences" means a freely given, considered, specific, and unambiguous indication of a user's preferences regarding the user's engagement with a covered online service.

(b) Expressed preferences cannot be based on the user's time spent engaging on the covered online service, nor on the usage of features that do not indicate explicit preference, such as comments made, posts reshared, or similar actions that are commonly taken on disliked media.

(7) "Known to be a minor" means the covered online service has actual knowledge that a particular consumer is a minor. For purposes of this act, actual knowledge includes all information and inferences known to the covered online service relating to the age of the individual including, but not limited to, self-identified age, and including any age the covered online service has attributed or associated with the individual for any purpose including, but not limited to, marketing, advertising, or product development purposes.

(8) "Minor" means a consumer who is less than eighteen years of age.

(9) "Online service" means any service, product, or feature that is accessible to the public on the internet including, but not limited to, a website or application. An online service may include any service, product, or feature that is based in part or in whole on artificial intelligence. "Online service" does not mean any of the following:

(a) a telecommunications service, as defined in 47 U.S.C. Section 153;

(b) a broadband internet access service as defined in 47 C.F.R. Section 54.400; or

(c) the sale, delivery, or use of a physical product.

(10) "Parent" has the same meaning as defined in the Children's Online Privacy Protection Act, 15 U.S.C. Sections 6501-6506 and the Federal Trade Commission rules implementing that act.

(11)(a) "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.

(b) "Personal data" does not include publicly available data.

(12) "Personalized recommendation system" means a fully or partially automated system used to suggest, promote, or rank content, including other users, hashtags, or material from others based on the personal data of users.

(13)(a) "Precise geolocation information" means any data that identifies a user's present or past location within a radius of one thousand one hundred eighty feet, the present or past location of a device that links or is linkable to a user, or any data that is derived from a device that is used or intended to be used to locate a user within a radius of one thousand one hundred eighty feet by means of technology that includes a global positioning system that provides latitude and longitude coordinates.

(b) "Precise geolocation information" does not include the content of communications or any data generated or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(14) "Process" means the performance of an operation, or a set of operations, by manual or automated means on personal data including, but not limited to, collecting, using, storing, disclosing, analyzing, deleting, sharing, or modifying personal data.

(15) "Profile" means any form of automated processing of personal data to evaluate, analyze, or predict certain aspects relating to a user including, but not limited to, a user's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(16)(a) "Publicly available data" means data that is lawfully made available from federal, state, or local government records, or data that a business has a reasonable basis to believe is lawfully made available to the general public by the individual or from widely distributed media or data made available by a person to whom the individual has disclosed the data if the individual has not restricted the data to a specific audience.

(b) "Publicly available data" does not mean biometric data collected by a covered online service about a minor without the minor's knowledge.

(17)(a) "Reasonably likely to be accessed by a minor" means it is reasonable to expect that the covered online service would be accessed by an individual minor or by minors based on the covered online service meeting either of the following criteria:

(i) the individual is known to the covered online service to be a minor as defined in Section 39-80-10(7); or

(ii) the covered online service is directed to children as defined by the Children's Online Privacy Protection Act, 15 U.S.C. Sections 6501-6506 and the Federal Trade Commission rules implementing that act.

(b) Where subitem (a)(i) is met, the covered online service must treat the particular individual as a minor. Where subitem (a)(ii) is met, the covered online service must treat all individuals using or visiting the covered online service as minors, except where the covered online service has actual knowledge that the individual is not a minor.

(18) "Sensitive personal data" means personal data that reveals:

(a) an individual's social security number, driver's license, state identification card, or passport number;

(b) an individual's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

(c) an individual's precise geolocation information;

(d) an individual's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership;

(e) the contents of an individual's mail, email, text messages, or other forms of communications that perform similar functions, including shared images and videos, unless the business is the intended recipient of the communication;

(f) an individual's genetic data;

(g) biometric data for the purpose of uniquely identifying an individual; or

(h) personal data concerning an individual's health.

(19)(a) "Targeted advertising" means displaying advertisements to an individual where the advertisement is selected based on personal data obtained or inferred from that individual's activities over time and across nonaffiliated websites or online applications to predict the individual's preferences or interest.

(b) "Targeted advertising" does not include:

(i) advertisements based on activities within a covered online service's own internet websites or online applications;

(ii) advertisements based on the context of an individual's current search query, visit to an internet website, or use of an online application;

(iii) advertisements directed to an individual in response to the individual's request for information or feedback; or

(iv) processing personal data solely to measure or report advertising frequency, performance, or reach.

(20) "User" means with respect to a covered online service an individual who uses the covered online service and who is located in South Carolina.

Section 39-80-20. (A) A covered online service shall exercise reasonable care in the use of a minor's personal data and the design and operation of the covered online service including, but not limited to, covered design features, to prevent the following harm to minors:

(1) compulsive usage of the covered online service;

(2) severe psychological harm including, but not limited to, anxiety, depression, self-harm or suicidal ideations;

(3) severe emotional distress;

(4) highly offensive intrusions on the minor's reasonable privacy expectations;

(5) identity theft;

(6) discrimination against the minor on the basis of race, ethnicity, sex, disability, or national origin; and

(7) material financial or physical injury.

(B) "Harm" defined in this section is limited to those for which liability is permitted under 47 U.S.C Section 230, including as that provision is amended or repealed in the future.

(C) Nothing in this section may be construed to require a covered online service to prevent or preclude any user from deliberately and independently searching for or specifically requesting content, or accessing resources and

information regarding the prevention or mitigation of the harm described in this section.

(D) The provisions contained in this chapter do not apply to:

(1) a federal, state, tribal, or local government entity in the ordinary course of its operations;

(2) personal data that is controlled by a covered online service that is:

(a) required to comply with:

(i) Title V of the federal Gramm-Leach-Bliley Act;

(ii) the federal Health Information Technology for Economic and Clinical Health Act; or

(iii) regulations promulgated pursuant to Section 264(C) of the Health Insurance Portability and Accountability Act of 1996;

(b) in compliance with the information security requirements of the statutes or regulations identified in subitem (a);

(3) information including, but not limited to, personal data collected as part of a clinical trial subject to the federal policy for the protection of human subjects pursuant to human subject protection requirements of the U.S. Food and Drug Administration;

(4) the requirements of this chapter are in addition to and may not limit or restrict in any way the application of other laws including, but not limited to, statutes, regulations, and common law of South Carolina. In the event of a conflict between this chapter and one or more other laws, the law that affords the greatest protection to minors shall control.

Section 39-80-30. (A) A covered online service must provide a user or visitor to the service with easily accessible and easy-to-use tools to:

(1) disable design features including, but not limited to, all covered design features, that are not necessary to provide the covered online service by allowing users to opt out of the use of all such design features or any combination of such design features;

(2) limit the amount of time the user spends on the covered online service;

(3) limits, at the level of the user's choosing, the financial value of purchases and transactions on the covered online service if such purchases and transactions have not been disabled;

(4) block, disable, and render nonvisible messaging, requests, reactions, likes, comments, or other contact from account holders that are not already among the minor's existing connected accounts;

(5) restrict the visibility of the minor's account and information posted by the minor to only users with connected accounts;

(6) block, disable, and render nonvisible quantification of engagement including, but not limited to, providing a visible count of how many likes, comments, clicks, views, or reactions regarding any item generated by the user;

(7) disable search engine indexing of a user's account profile such that the account only shows within searches initiated by a user with a connected account;

(8) prohibit any other individual from viewing the user's connections to other users, regardless of the nature of the connection; and

(9) restrict the visibility of the user's location information to only those with whom the user specifically shares such information and provide notice when the minor's precise geolocation information is being tracked or shared.

(B) A covered online service must provide to a user the option to opt out of personalized recommendation systems, except for optimizations based on the user's expressed preferences. A covered online service must establish this option as a default setting for any individual the covered online service knows to be a minor.

(C) A covered online service must establish, implement, and maintain as default settings for any individual the covered online service knows to be a minor the safeguards described in subsection (A).

Section 39-80-40. (A) Covered online services shall only collect, use, or share the minimum amount of a minor's personal data necessary to provide the specific elements of the covered online service with which a minor has knowingly engaged. Such personal data may not be used for reasons other than those for which it was collected. Minors' personal data collected for age verification or estimation cannot be used for other purposes and must be deleted after use.

(B) A covered online service shall only retain a minor's personal data as long as necessary to provide the specific elements of an online service with which a minor has knowingly engaged.

(C) Covered online services may not facilitate targeted advertising to minors.

(D) Precise geolocation information of minors cannot be collected by default unless necessary to the provision of the covered online service. An obvious notice to the minor must be provided when precise geolocation information is being collected or used.

(E) A covered online service must provide users with accessible and easy-to-use tools to prevent notifications and push alerts to an individual during specified times. To comply with this requirement, a covered online service must offer the user the option to prevent notifications and push alerts to an individual the covered online service knows is a minor between the hours of ten p.m. and six a.m. seven days a week year round and between the months of August and May between the hours of eight a.m. and three p.m. Monday through Friday in the minor's local time zone.

(F) A covered online service shall not profile an individual the covered online service knows is a minor, unless profiling is necessary to providing the covered online service with which a minor has knowingly requested and is limited to only the aspects of the covered online service with which a minor is actively and knowingly engaged.

(G) Settings for the protections required under this section must be set at the highest level of protection by default.

(H) If a covered online service allows parental monitoring or is required to provide parental monitoring by law, then it must provide obvious notice to the minor when they are being monitored.

Section 39-80-50. (A) Covered online services must provide parents with accessible and easy-to-use tools to help parents protect and support minors using the covered online services and these shall be on by default for any individual the covered online service knows to be a minor.

(B) The parental tools provided by the covered online services shall provide to the parents the ability to:

(1) manage the minor's account settings and change and control the minor's privacy and account settings; and

(2) restrict a minor's purchases and other financial transactions.

(C) Among the parental tools provided by covered online services shall be one to enable parents to view the total time spent on a covered online service by a user the covered online service knows is a minor and allow the parent to place limits on the minor's use of the covered online service. The parental tools provided by covered

online services must also offer parents the ability to restrict a minor's use of the covered online service during times of day specified by the parents, including during school hours and at night.

(D) Covered online services must notify a minor when any of the tools described in this section are in effect and what settings have been applied.

Section 39-80-60. (A) Covered online services shall establish mechanisms for parents, minors, and schools to report harm to minors on covered online services, especially those harms that pose an imminent threat to a minor.

(B) Covered online services are prohibited from facilitating ads directed to minors for products prohibited for minors including, but not limited to, narcotic drugs, tobacco products, gambling, and alcohol to users the covered online services know are minors.

(C) Covered online services are prohibited from using dark patterns.

(1) Use of dark patterns by a covered online service shall constitute an unlawful trade practice under Section 39-5-20 of the South Carolina Unfair Trade Practices Act.

(2) A covered online service that violates the provisions of this section are subject to the provisions, penalties, and damages of the South Carolina Unfair Trade Practices Act.

(D) Each covered online service that utilizes personalized recommendation systems is required to describe in its terms and conditions, in a clear, conspicuous, and easy-to-understand manner, how the systems are used to provide information to minors and information regarding how minors or their parents can opt out of or control the systems.

(E) Covered online services are required to provide comprehensive, clear, conspicuous, and easy-to-understand information in a prominent location describing the design safety for minors, the privacy protections for minors, and the parental tools that the covered online service has adopted pursuant to this chapter. Such disclosure must also include a clear, conspicuous, and easy-to-understand explanation of how minors and parents may utilize those design safety measures, privacy protections, and tools.

Section 39-80-70. (A) Annually, on or before July first, the covered online service must issue a public report prepared by an independent third-party auditor that contains a detailed description of the covered online service as it pertains to minors, including its covered design features, its use of personal data, and its business practices as they pertain to minors. The public report must be submitted to the Attorney General who shall post it in a prominent place on his internet website. Each report must include:

(1) the purpose of the covered online service;

(2) the extent to which the covered online service is likely to be accessed by minors;

(3) an accounting of the total number and types of reports generated pursuant to Section 39-80-60(A) and assessment of how those reports were handled, if known;

(4) whether, how, and for what purpose the covered online services collects or processes minors' personal data and sensitive personal data;

(5) the design safety for minors, the privacy protections for minors, and the parental tools that the covered online entity has adopted;

(6) whether and how the covered online service uses covered designed features;

(7) the covered online service's process for handling data access, deletion, and correction requests for a minor's data;

(8) age verification or estimation methods used; and

(9) description of algorithms used by the covered online service.

(B) Independent auditors that prepare reports required under this section are required to follow inspection and consultation practices designed to ensure that reports are comprehensive and accurate, and that the reports are prepared in consultation with experts on minors' use of covered online services.

(C) Covered online services are required to provide independent auditors that prepare reports required under this section full and complete cooperation and access to information and operations required to ensure that the report is comprehensive and accurate.

Section 39-80-80. (A) The Attorney General shall enforce the provisions contained in this chapter.

(B) A covered online service shall be liable for treble the financial damages incurred as a result of a violation of this chapter.

(C) The officers and employees of a covered online service may be held personally liable for wilful and wanton violations of this chapter.

Conflict

SECTION 2. The requirements of this act are in addition to and shall not limit or restrict in any way the application of other laws including, but not limited to, statutes, regulations, and common law of this State. In the event of a conflict between this act and one or more other laws, the law that affords the greatest protection to minors shall control.

Severability

SECTION 3. If any section, subsection, paragraph, subparagraph, sentence, clause, phrase, or word of this act is for any reason held to be unconstitutional or invalid, such holding shall not affect the constitutionality or validity of the remaining portions of this act, the General Assembly hereby declaring that it would have passed this act, and each and every section, subsection, paragraph, subparagraph, sentence, clause, phrase, and word thereof, irrespective of the fact that any one or more other sections, subsections, paragraphs, subparagraphs, sentences, clauses, phrases, or words hereof may be declared to be unconstitutional, invalid, or otherwise ineffective.

Time effective

SECTION 4. This act takes effect upon approval by the Governor.

Ratified the 3rd day of February, 2026.

_____

President of the Senate

_____

Speaker of the House of Representatives

Approved the _____ day of _____2026.

_____

Governor

----XX----

This web page was last updated on February 3, 2026 at 4:28 PM