April 6, 2026

Rhode Island Senate Committee on Artificial Intelligence and Emerging Technologies
82 Smith Street
Providence, RI 02903

Re: SB 2968 – "RHODE ISLAND SOCIAL MEDIA REGULATION ACT" (Oppose)

Dear Chair Gu, Vice Chair Burke, and Members of the Senate Committee on Artificial Intelligence and Emerging Technologies:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 2968, which would impose broad bans on access to social media services. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the intrastate provision of digital services therefore can have a significant, nationwide impact on CCIA members. CCIA firmly believes that children are entitled to security and privacy online. Our members have designed and developed parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.[2] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[3]

However, protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Lawful speech cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors.[4] While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).
[3] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[4] *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–14 (1975). *See also FCC v. Pacifica Found.* 438 U.S. 726, 749–50 (1978); *Pinkus v. United States*, 436 U.S. 293, 296–98 (1978).

The U.S. Supreme Court has repeatedly struck down laws containing speech restrictions intended to prevent harm to minors.

In 1997, the Supreme Court held that "the First Amendment does not tolerate" laws that "reduce[] the adult population ... to reading only what is fit for children."[5] Yet SB 2968 effectively does exactly this: in order to restrict access to content potentially harmful to children, the proposed bill would restrict both children and adults' access to such content. The First Amendment applies to teens as well as adults,[6] and includes their right to speak anonymously online.[7] Nor may states require parental consent to view such content; the Court has likewise rejected the argument that "the state has the power to prevent children from hearing or saying anything without their parents' prior consent."[8] Accordingly, the proposed bill unconstitutionally undermines established free speech protections for users of all ages.

For these reasons, the vast majority of lower courts that have ruled on the issue have held that the First Amendment does not permit states to require age verification to access protected speech.[9] For example, a Louisiana federal court recently struck down a similar age verification mandate, noting that "The Act's age-verification and parental-consent requirements fail strict and intermediate scrutiny. Even if the Court accepts that Defendants have a compelling interest 'in protecting the physical and psychological well-being of minors,' Defendants have not established a causal relationship between social media use and health harms to minors."[10]

The bill's coverage definition also poses constitutional problems: SB 2968 covers online services based in part on whether they "provide[] news, sports, entertainment, or other content that is preselected by the provider and not user generated". Multiple federal courts have found this method of designating covered services to violate the First Amendment's prohibition on content-based speech restrictions. As a Virginia federal court recently explained, a law that "creates exemptions for news, sports, [or] entertainment... creates a content-based restriction" on speech.[11] It further held that "creat[ing] an exemption for content preselected by the provider and not generated by users... favors provider-selected speech over user generated speech.... precisely the type of speaker preference the Supreme Court declared should be treated as content-based."[12] Several other federal courts have found such content-based regulation of digital service to be unconstitutional as well.[13]

---

[5] *Reno v. ACLU*, 521 U.S. 844, 888 (1997) (cleaned up).
[6] *See, e.g.*, *id.* at 855-56.
[7] *See, e.g.*, *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *20-21 ((W.D. Ark. Mar. 31, 2025).
[8] *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 n. 3 (2011).
[9] *See, e.g.*, *NetChoice v. Jones*, No. 1:25-cv-02067, 2026 WL 561099 (E.D. Va. Feb. 27, 2026); *CCIA v. Paxton*, No. 25-cv-01660, 2025 WL 3754045 (W.D. Tex. Dec. 23, 2025); *SEAT v. Paxton*, No. 25-cv-01662, 2025 WL 3731733 (W.D. Tex. Dec. 23, 2025); *NetChoice v. Murrill*, No. 25-231, 2025 WL 3634112 (M.D. La. Dec. 15, 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025); *Griffin*, 2025 WL 978607; *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024); *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).
[10] *Murrill*, 2025 WL 3634112 at *72.
[11] *Jones*, 2026 WL 561099 at *18 (cleaned up) (quoting *Reed v. Town of Gilbert, AZ*, 576 U.S. 155, 170 (2015)).
[12] *Id.*
[13] *See, e.g.*, *Murrill*, 2025 WL 3634112 at *62; *Yost*, 778 F. Supp. 3d at 953; *Griffin*, 2025 WL 978607 at *22-24.

The bill's requirements undermine privacy and competition.

SB 2968 contains many requirements that undermine privacy for all users. While well-meaning, age verification mandates inherently require collecting sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[14] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[15]

Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[16] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes. Compounding these problems, the bill requires covered online services to retroactively verify the ages of existing users as well as prospective ones, which unnecessarily increases the risk of malicious actors accessing the data submitted.

The proposed bill further undermines privacy by requiring covered services to "allow the parent or guardian to view… All posts the Rhode Island minor account holder makes under the social media platform account; and… All responses and messages sent to or by the Rhode Island minor account holder in the social media platform account." These provisions remove much of younger internet users' autonomy to speak with their friends, read, or research new information. Such excessive monitoring has been shown to negatively affect young people's mental health and development.[17] This provision is therefore at odds with the bill's ostensible goal of protecting young users online.

SB 2968 also requires that covered services prohibit minors from accessing their accounts between 10:30 p.m. and 6:30 a.m. Such requirements inevitably require that covered services track when it is nighttime in a given device's location. This requirement therefore effectively mandates location-based tracking of minors' devices, thus undermining the privacy of the very population the bill is designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly offer users the option to turn off notifications themselves.

---

[14] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.

[15] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.

[16] *See, e.g.*, Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.

[17] *See, e.g.*, Hannah Quay-de la Valle, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, Ctr. for Democracy & Tech. (May 5, 2022), https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/ (finding that "Monitoring programs, if not carefully implemented, can stifle growth and leave students vulnerable to the chilling effect, placing their mental health at risk").

The more data a service is forced to collect, the greater risk it poses to small business sustainability.[18] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification methods, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[19]

The Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.[20] For these reasons, a group of 438 privacy and data security scientists has recently urged policymakers to institute a moratorium on age verification requirements until better solutions emerge.[21] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

To avoid restricting teens' access to information, SB 2968 should regulate users under 13 rather than 18 in accordance with established practices.

SB 2968 defines a "minor" as an individual under 18. Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, a 16-year-old conducting research for a school project can be expected to come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. We would suggest changing the definition of "known minor" to a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard.[22] This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

If enacted, SB 2968 may result in denying services to all users under 18, limiting their access to needed supportive communities.

The bill's lack of narrowly tailored definitions could incentivize businesses to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. Requiring businesses to deny access to social networking sites or other online resources may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For minors in unsafe households or from minority

---

[18] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[19] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023) at 10, https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[20] *Online Age Verification: Balancing Privacy and the Protection of Minors,* CNIL (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.
[21] Joint Statement of Security and Privacy Scientists and researchers on Age Assurance (Mar. 9, 2026), https://csa-scientist-open-letter.org/ageverif-Feb2026.
[22] *See* 15 U.S.C. § 6501(1).

groups who may not have local peers with shared experiences, digital services can provide vital communities for support and resources.[23]

The connected nature of social media has led some to allege that online services may negatively impact teenagers' mental health. However, researchers explain existing evidence does not support this theory and repeats a 'moral panic' argument frequently associated with new technologies and modes of communication. Instead, social media effects are nuanced,[24] individualized, reciprocal over time, and gender-specific. Indeed, as an Ohio court noted when striking down a similar law last year, "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation."[25]

As explained above, CCIA believes that an alternative to solving these complex issues is to work with businesses to continue their ongoing private efforts to implement mechanisms such as daily time limits or child-safe searching so that parents can have control over their own child's social media use.

The bill's private right of action would result in the proliferation of frivolous lawsuits and questionable claims, and exorbitant statutory damages.

Creating a new private right of action would open the doors of state courthouses to plaintiffs advancing costly, time-intensive claims based on subjective criteria. Furthermore, as it is difficult to establish broadly applicable guidelines for when a party is "aggrieved" by a violation of this bill, resolving such claims during early stages of litigation will be difficult if not impossible. These new dynamics would significantly affect litigants' incentives. If defendants are routinely forced past the motion to dismiss phase and into full discovery, the cost of litigation itself becomes a coercive force, encouraging settlements unrelated to the strength of the legal claims. Moreover, these costs would be passed on to Rhode Island residents, disproportionately impacting smaller businesses and startups across the state.[26]

While we share the concerns of the sponsor and the Committee regarding online youth safety, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate your consideration of these comments and stand ready to provide additional information as you consider proposals related to technology policy.

Respectfully submitted,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association

---

[23] *The Importance of Belonging: Developmental Context of Adolescence*, Boston Children's Hospital Digital Wellness Lab (Oct. 2024), https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/.
[24] Amy Orben et al., *Social Media's Enduring Effect on Adolescent Life Satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[25] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).
[26] Trevor Wagener, *State Regulation of Content Moderation Would Create Enormous Legal Costs for Platforms*, Broadband Breakfast (Mar. 23, 2021), https://broadbandbreakfast.com/trevor-wagener-state-regulation-of-content-moderation-would-create-enormous-legal-costs-for-platforms/.