**March 31, 2026**

New York Senate Committee on Internet and Technology
Legislative Office Building
198 State Street
Albany, NY 12247

## Re: S 4609 – "Stop Online Predators Act" (Oppose)

Dear Chair Gonzalez and Members of the Senate Committee on Internet and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose S 4609 in advance of the hearing on April 1. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and 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 Inst., *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).

## U.S. courts have 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 S 4609 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 do states have the authority to require parental consent for viewing 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 bills unconstitutionally undermine established free speech protections for users of all ages. As the bill's legislative findings now recognize, the First Amendment applies to teens as well as adults,[9] and includes their right to speak anonymously online.[10]

For these reasons, most 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.[11] As a Louisiana federal court recently held when striking down a similar law, "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."[12]

## S 4609's method of designating covered services violates the First Amendment.

The bill's coverage definition also poses constitutional problems: S 4609 covers online services and applications based in part on whether they "presents the user with content generated by other users". 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, "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

[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.*, *id.* at 855-56.
[10] *See, e.g.*, *Griffin*, 2025 WL 978607 at *20-21.
[11] *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).
[12] *Murrill*, 2025 WL 3634112 at *72 (cleaned up).

treated as content-based."[13] Several other federal courts have found such content-based regulation of digital service to be unconstitutional as well.[14]

## Age verification and parental consent requirements undermine user privacy for users of all ages.

S 4609 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.[15] 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.[16] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[17] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes.

The more data a service is forced to collect, the greater risk it poses to consumer privacy and 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] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

---

[13] *Jones*, No. 1:25-cv-02067 at *18 (cleaned up) (quoting *Reed v. Town of Gilbert, AZ*, 576 U.S. 155, 170 (2015)).
[14] *See, e.g.*, *Murrill*, 2025 WL 3634112 at *62; *Yost*, 778 F. Supp. 3d at 953; *Griffin*, 2025 WL 978607 at *22-24.
[15] *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/.
[16] 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/.
[17] *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.
[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.

## Restricting access to the internet for younger users limits their access to information and supportive communities.

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 example, since children of certain minority groups may not live in areas where they can easily connect with others who relate to their unique experiences, an online meeting place to share such experiences and find support can have positive impacts.[21]

Empirical findings regarding social media's impact on young users are much more nuanced than S 4609's introductory legislative findings suggest. When the U.S. Surgeon General released the advisory entitled *Social Media and Youth Mental Health* referenced in these findings, many were quick to highlight only the harms and risks it detailed, as did the original version of this bill. However, as the legislative findings now acknowledge, the advisory is much more complex and also discusses many potential benefits of social media use among children and adolescents. It concludes, for instance, that social media provides young people with communities and connections with others who share identities, abilities, and interests.[22] It can also provide access to important information and create spaces for self-expression. Research further details that social media can especially benefit marginalized youth, including racial, ethnic, sexual, and gender minorities, as online peer support can mitigate the stresses they face.[23]Indeed, as an Ohio court noted when striking down a law age-gating social media services last year, "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation."[24]

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.

## To avoid restricting teens' access to information, S 4609 should regulate users under 13 rather than 16 in accordance with established practices.

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, if a 15-year-old is conducting research for a school project, it is expected that they would 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 scope of covered users to be minors under the

---

[21] *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/.
[22] Off. of the Surgeon Gen., U.S. Department of Health & Human Services, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, *Social Media Has Both Positive and Negative Impacts on Children and Adolescents* (2023), https://www.ncbi.nlm.nih.gov/books/NBK594763/.
[23] *Id.*; *see also* Jennifer Marino et al., *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, J. Med. Internet Rsch. (Sept. 22, 2021), https://www.jmir.org/2022/9/e38449.
[24] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).

age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard.[25] 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.

## S 4609 contains requirements that are not well-defined.

S 4609 contains several provisions that are vague, subjective, or not well-defined. Most privacy laws that prohibit the use of "dark patterns" do so only in highly specific contexts, such as to obtain consent.[26] S 4609, however, prohibits the use of "dark patterns" without the necessary context, defining the term as "deploy[ing] any mechanism or design which intentionally inhibits the purpose of this article, subverts user and/or parent choice or autonomy, or renders it more difficult for a user and/or parent to exercise " Deciding when design features "subvert[] user choice and autonomy " is far more subjective than determining when such features impair the choice to provide consent. This requirement should therefore be specific to the consent context.

Furthermore, the bill requires operators to use "commercially reasonable age verification methods", but does not specify which methods are "commercially reasonable." Nor does the bill specify how "size, financial resources, and technical capabilities" will determine which age verification methods are "technically feasible" for a given digital service. These subjective requirements do not provide covered services sufficient clarity to know if they are violating the law, risking inconsistent application and arbitrary enforcement.

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

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

[25] *See* 15 U.S.C. § 6501(1).
[26] *See, e.g.*, Texas Data Privacy and Security Act § 541.001(6)(C); Connecticut Data Privacy Act § 42-515(7)(C).