



January 29, 2026

Washington Senate Business, Trade, and Economic Development Committee

Attn: Alina Cole

416 Sid Snyder Ave SW

Olympia, WA 98504

Re: SB 6111 – "Washington protecting children online act" (Oppose)

Dear Chair Kauffman and Members of the Senate Business, Trade, and Economic Development Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 6111. 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.

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 6111 effectively does exactly this: in order to restrict access to content potentially harmful to

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).

⁵ *Reno v. ACLU*, 521 U.S. 844, 888 (1997) (cleaned up).

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

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."⁷ Accordingly, the proposed bills unconstitutionally undermine 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.⁸ 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."⁹

The bill further violates the First Amendment by imposing content-based restrictions on speech, as it regulates a digital service that "Primarily functions to provide a user with access to news, sports, commerce, [or] online video games" differently from others. As the above Louisiana court explained, such a law regulates a digital service "with reference to what it is not.... Classification of websites under the Act therefore requires consideration of their content—that is, whether their content is "predominant[ly] or exclusive[ly]" socially interactive.¹⁰ Several other federal courts have found such content-based regulation of digital service to be unconstitutional as well.¹¹

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

SB 6111 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.¹² Requiring individuals to share

⁶ See, e.g., *id.* at 855-56.

⁷ *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 n. 3 (2011).

⁸ See, e.g., *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. Griffin*, No. 5:25-CV-5140 (W.D. Ark. Dec. 15, 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); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 (W.D. Ark. Mar. 31, 2025); *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024); *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).

⁹ *Murrill*, 2025 WL 3634112 at *72.

¹⁰ *Id.* at *62.

¹¹ See, e.g., *Yost*, 778 F. Supp. 3d at 953; *Griffin*, 2025 WL 978607 at *22-24, *NetChoice v. Bonta*, 770 F. Supp. 3d 1164, 1190-91 (N.D. Cal. 2025).

¹² 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/>.

sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.¹³

Such dangers are far from hypothetical: Several of the most devastating data breaches in recent years are directly attributable to age verification requirements.¹⁴ 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 more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.¹⁵ 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.”¹⁶

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.¹⁷ 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 6111 should regulate users under 13 rather than 18 in accordance with established practices.

SB 6111 defines a “known minor” as an individual under 17. Due to the nuanced ways in which children under the age of 17 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-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 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.¹⁸ 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.

¹³ 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/>.

¹⁴ 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>.

¹⁵ 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>.

¹⁶ *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.

¹⁷ *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>.

¹⁸ See 15 U.S.C. § 6501(1).

The bill's requirements are not well-defined.

SB 6111 requires covered services to “make commercially reasonable efforts to develop and implement a strategy to prevent or mitigate the known minor’s exposure to content that promotes or facilitates” a broad list of defined harms, including “patterns of use that indicate substance abuse”. However, it is unclear what obligations this provision confers in practice, leaving covered services unable to know whether they are violating the law. The bill does not specify what constitutes “commercially reasonable efforts,” or what would constitute sufficient mitigation of exposure to these harms. Furthermore, it does not specify when a “pattern of use” would “indicate” substance abuse, nor does it clarify whether this provision refers to use of the digital service or use of substances. Consequently, covered entities will have no way of knowing what measures they need to institute, or how they are to know whether they are succeeding. Defining covered services’ obligations using such vague and subjective terms risks arbitrary and inconsistent application of the law.

If enacted, SB 6111 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 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.¹⁹

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers’ mental health. However, researchers explain that this theory is not well supported by existing evidence and repeats a ‘moral panic’ argument frequently associated with new technologies and modes of communication. Instead, social media effects are nuanced,²⁰ 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.”²¹

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.

* * * * *

¹⁹ *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/>.

²⁰ 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>.

²¹ *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).



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,

Aodhan Downey
State Policy Manager, Western Region
Computer & Communications Industry Association