March 27, 2026

Minnesota Senate Commerce and Consumer Protection Committee
Minnesota Senate Building
95 University Avenue W
Saint Paul, MN, 55155

Re: SB 1857 – "Minor Access to Chatbots" (Oppose)

Dear Chair Klein and Members of the Senate Commerce and Consumer Protection Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 1857. 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] While CCIA shares the goal of increasing online safety, the bill raises the following concerns:

SB 1857's vague and subjective definitions would create compliance uncertainty.

Many of the bill's definitions are not sufficiently clear for businesses to ensure compliance. For example, the bill broadly defines "AI companion" to include any AI system that "is accessible to the general public and primarily simulates human conversation through text, audio, or visual interaction." This open-ended, subjective definition risks scoping in businesses such as customer service chatbots that answer support questions, productivity tools that use conversation interfaces, wellness applications that respond to user prompts about goals or progress, and other products and services without the capabilities this bill contemplates. The definition of "AI companion system," which is defined in the bill as "artificial intelligence systems that are specifically designed, marketed, or optimized to form ongoing social or emotional bonds with individuals, whether or not such systems also provide information, complete tasks, or assist with specific functions" remains broad enough to capture widely used conversational interfaces, including AI tutors, language apps and research tools.

[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).

Similarly, it is difficult to objectively determine when a given output meets many of the listed criteria, such as tools that "express or invite emotional attachment" or "behave in a way that a reasonable user would consider excessive praise" These vague terms do not allow businesses to determine in advance whether their products and services comply with the law. Precise narrowing is required to focus any regulation solely on the intended targets.

Moreover, consumer-facing digital services have already built considerable consensus around mitigating content- and conduct-related risks to users and other parties. Most of the leading firms in industry have committed to meet best practice standards for online safety, which are embedded in a recently published 2025 international standard.[3]

To avoid restricting teens' access to information, SB 1857 should regulate users under 13 rather than 18 in accordance with established practices.

SB 1857 defines "minor" as an individual less than 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, 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 scope of covered users to be minors under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard.[4] 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.

Age verification raises significant privacy concerns.

SB 1857 risks effectively forcing covered providers to institute age verification to ensure compliance. This approach creates significant problems. Every approach to age determination presents trade-offs between accuracy and privacy[5]—in addition to significant costs, especially for startups[6]—and there is no one-size-fits-all approach. Different services consider various factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility, and should be able to choose the method that they believe will best protect their users. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains guiding principles for age assurance and discusses how digital services have used such principles to develop best practices.[7]

---

[3] ISO/IEC 25389:2025, *Information technology — The safe framework* (Edition 1, June 2025), https://www.iso.org/standard/90106.html.
[4] *See* 15 U.S.C. § 6501(1).
[5] Kate Ruane, *CDT Files Brief in* NetChoice v. Bonta *Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[6] Engine, *More than just a number: How determining user age impacts startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf.
[7] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

Determining a user's age inherently requires collecting additional sensitive data from those users, and any document capable of verifying a user's age will likely contain sensitive information. 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.[8]

SB 1875 risks creating a fragmented regulatory environment.

The bill would also contribute to a growing panoply of state artificial intelligence laws that impose inconsistent and potentially conflicting obligations on interstate digital services. Artificial intelligence systems are developed, trained, and deployed on a national and global scale. Prescriptive state-level mandates risk becoming outdated quickly, complicating compliance, and discouraging investment in jurisdictions that adopt rigid or punitive frameworks. A fragmented regulatory approach threatens that position by making it more difficult for companies to deploy new services and features in the state.

The bill's private right of action would result in the proliferation of costly and questionable claims based on subjective criteria.

SB 1857 permits an individual to "bring a civil action for damages, statutory damages not to exceed $1,000, injunctive relief, and costs and reasonable attorney fees." By creating a new private right of action, this measure would open the doors of state courthouses to plaintiffs advancing costly, time-intensive claims based on subjective criteria. The vague standards noted above necessitate fact-intensive inquiries that make courts reluctant — or unable — to dismiss claims until more facts can be gathered in the discovery phase. 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 Minnesotans, disproportionately impacting smaller businesses and startups across the state.[9] CCIA therefore recommends granting the state exclusive enforcement authority and adding a right to cure period to ensure that such costly litigation arises only when necessary, mirroring New Hampshire's recent shift.[10]

* * * * *

While we share concerns about protecting child safety online, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We

[8] *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.
[9] 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/.
[10] *CCIA Applauds New Hampshire House Members for Improving Flawed AI Bill*, CCIA (May 23, 2025), https://ccianet.org/news/2025/05/ccia-applauds-new-hampshire-house-members-for-improving-flawed-ai-bill/.

appreciate your consideration of these issues and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Tom Mann
State Policy Manager, South
Computer & Communications Industry Association