April 2, 2026

The Honorable Brian Kemp
Governor of Georgia
206 Washington Street, Suite 203
Atlanta, GA 30334

Re: SB 540 - "AI Companion Chatbots" (Oppose)

Dear Governor Kemp:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto of SB 540. 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] However, while CCIA shares the goal of increasing online safety for minors, SB 540 introduces significant constitutional, operational, and privacy concerns that would negatively impact Georgia residents and businesses.

The bill's requirements undermine user privacy for users of all ages.

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.[3] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[4] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes.

---

[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] 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/.

[4] *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.

While well-meaning, the bill's requirements will inevitably lead to the collection of sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[5] Furthermore, the more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.[6] 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."[7]

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] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

SB 540's coverage requirement is unconstitutionally vague.

SB 540 covers content based in part on whether it is "harmful to minors", a term the bill does not define. Several federal courts have held that such framing does not enable operators to know what content is being regulated and thus violates the Fourteenth Amendment's Due Process Clause. Most recently, the US Court of Appeals for the Ninth Circuit invalidated a similarly worded regulation, holding that such a law "does not provide any guidance as to the breadth of conduct that 'material[] detriment[] to the physical health, mental health, or well-being of a child may reach".[9] Other federal courts have blocked analogous regulations on vagueness grounds as well.[10]

SB 540's vague definitions would create compliance uncertainty.

Besides posing constitutional challenges, many of the bill's definitions are not clear enough for businesses to ensure they are in compliance. The bill's definition of "AI companion chatbot" contains open-ended and subjective phrases such as "designed to simulate a sustained human or human-like relationship with a user", which could scope in businesses that should fall

[5] *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/.
[6] 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.
[7] *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.
[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] *NetChoice v. Bonta*, No. 25-2336 at *36 (9th Cir. Mar. 12, 2026).
[10] *See, e.g.*, *NetChoice v. Griffin*, No. 5:25-CV-5140, 2025 WL 3634088 at *27 (W.D. Ark. Dec. 15, 2025); *CCIA v. Paxton*, 747 F. Supp. 3d 1011, 1040-42 (W.D. Tex. 2024); *SEAT v. Paxton*, 765 F. Supp. 3d 575, 601-02 (W.D. Tex. 2025).

outside the bill's requirements. For example, would this apply to customer service chatbots that answer support questions, productivity tools that use conversation interfaces, or even wellness applications that respond to user prompts about goals or progress? Many descriptions of the AI capabilities the bill seeks to regulate are phrased in similarly vague terms. Precise narrowing is required to focus the regulation solely on the intended targets.

Furthermore, several of the bill's requirements apply when an operator "knows or reasonably should have known that a user was a minor". It is difficult, however, to objectively determine when an operator "reasonably should have known" that a user is a minor. Moreover, establishing broadly applicable rules that clarify this standard will be infeasible since every covered business will possess different amounts of information regarding its users. Such framing does not allow covered operators to know what measures will ensure compliance, and risks arbitrary and inconsistent application.

The bill operates as a blunt tool, raising privacy and speech concerns.

The provisions governing "AI companion chatbot", particularly as applied to minors, raise substantial concerns regarding privacy, speech, and proportionality. SB 540 mandates persistent disclosures, parental access to all interactions, and extensive monitoring obligations while pairing those mandates with significant civil penalties. These requirements create strong incentives for covered platforms to prohibit minors from accessing AI-enabled services altogether rather than risk liability.

Such an outcome would have significant unintended consequences. Many minors use AI tools for educational support, creative expression, skill development, and access to information. Requiring constant monitoring and disclosure of all interactions, without narrowly tailored standards or workable safe harbors, risks suppressing lawful and beneficial speech. Teenagers retain constitutional rights to access information, and regulatory frameworks that effectively force websites to over-filter or over-monitor speech raise serious First Amendment concerns.[11] Additionally, such excessive monitoring has been shown to negatively affect minors' mental health and development.[12]

In practice, the bill would push providers toward blunt, exclusionary design choices rather than encouraging thoughtful, risk-based protections tailored to specific harms.

Existing laws already address many aspects of AI, including in high-risk scenarios.

Despite the ongoing trend of AI-specific legislation, existing federal and state frameworks already address many of the risks commonly associated with AI. AI does not operate in a legal vacuum but

[11] *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844, 855-56 (1997).

[12] *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").

rather, it is a tool used within regulated markets that are already governed by long-standing consumer protection, civil rights, privacy, and product liability laws. Before proposing such laws, policymakers must consider what laws already cover AI systems. Policymakers should build upon existing legal protections and focus narrowly on clearly defined gaps where demonstrable harms are not yet addressed. A balanced approach that does not layer expansive new liability regimes on AI developers will better protect consumers and preserve the innovation ecosystem.

SB 540 risks creating a fragmented regulatory environment.

The bill would also contribute to a growing fragmentation 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.

Georgia has long benefited from policies that promote innovation and technological growth. A fragmented regulatory approach threatens that position by making it more difficult for companies to deploy new services and features in the state.

* * * * *

We appreciate your consideration of CCIA's comments and stand ready to provide additional information as you consider proposals related to technology policy.

Sincerely,

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