June 3, 2026

Pennsylvania House Committee on Communications and Technology
Capitol Building
501 North Third Street
Harrisburg, PA, 17120

Re: HB 2006 "An Act providing for safety regarding artificial intelligence in companionship applications; and imposing a penalty" (Oppose)

Dear Chair Ciresi, Vice Chair Nelson, and Members of the House Committee on Communications and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 2006. 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:

HB 2006's vague and subjective definitions would create compliance uncertainty.

Many of the bill's definitions are not clear enough for businesses to ensure they are in compliance. For example, the original version of the bill applies to an "AI companion", but uses a definition with terms such as "humanlike relationship," "engage with the user's preferences," "personalize interaction," "emotion-based questions," and "personal matters" that are inherently subjective and lack objective standards that developers can reasonably apply. The proposed amendment would apply to an AI companion that simulates sustained "human-like relationships by retaining interaction history, asking emotion-based questions and maintaining ongoing dialogues about personal matters designed to mimic interpersonal relationships," again using subjective terms that could lead to regulation beyond the intended scope of the bill.

As drafted, these provisions could create uncertainty about whether products such as educational tutors, productivity assistants, wellness applications, or general-purpose chatbots

[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).

qualify as regulated AI companions if they retain interaction histories or ask anything that could be perceived as an "emotion-based question" on a "personal matter." More precise definitions, including clear technical criteria and limiting principles tied to the intended scope of the legislation, would improve predictability for developers, facilitate consistent enforcement, and ensure that the bill targets the specific category of AI systems it is intended to regulate.

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

The proposed amendment would require age verification to determine if a user is a minor, defined as an individual under 18 years of age. Operators would be required to obtain parental consent for minors to access AI companions and institute reasonable measures to prevent the AI companion from producing or engaging in sexually explicit content. To determine whether a user is a minor, operators would likely need to collect and process additional personal information that many services do not currently gather, creating new privacy risks for both minors and adults.

While well-intentioned, age-verification mandates inherently require the collection of additional sensitive personal information from users, including adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[3] 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.[4] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[5] 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.[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]

---

[3] *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/.

[4] 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/.

[5] *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.

[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*, DTSP (Sept. 2023) at 10, https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

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.

Furthermore, the amendment requires a suitability disclosure and additional notifications for a "known minor," but requires operators to implement safeguards relating to sexually explicit content for minors without clearly specifying what level of knowledge is required to trigger those obligations. This creates uncertainty regarding whether the safeguards apply only when an operator has actual knowledge that a user is under 18, or whether liability could arise whenever a minor accesses the service, regardless of the operator's knowledge. Faced with this uncertainty, operators may feel compelled to collect and retain additional age-related information to reduce legal risk and demonstrate compliance. To better protect user privacy and promote data minimization, the bill should clearly state that obligations relating to minors apply only when an operator has actual knowledge that a user is under 18 years of age.

Excessive civil penalties will deter operators from providing services.

The proposed amendment would grant enforcement authority to the Attorney General, with civil penalties of up to $100,000 per day for each violation. However, the bill does not define what constitutes a single violation, whether it is each individual user, each interaction with an AI companion, or each day a violation persists. As a result, potential liability could escalate rapidly, creating significant uncertainty for operators seeking to comply with the law. Without clear standards governing how violations are calculated, companies may struggle to assess their compliance obligations and legal risk. The bill would benefit from clearer penalty provisions that provide predictable enforcement standards and ensure that penalties are proportionate to the underlying conduct.

While we share concerns about protecting child safety online, we encourage resisting advancing legislation that is not adequately tailored to this objective. We appreciate your consideration of these issues and stand ready to provide additional information.

Sincerely,

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

[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.