February 17, 2026

Maine Joint Committee on Health Coverage, Insurance and Financial Services
Cross Building, Room 220
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

Re: LD 2162 – "An Act to Regulate and Prevent Children's Access to Artificial Intelligence Chatbots with Human-like features and Social Artificial Intelligence Companions" (Oppose)

Dear Chair Bailey, Chair Mathieson, and Members of the Joint Committee on Health Coverage, Insurance and Financial Services:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose LD 2162. 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:

LD 2162'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 bill defines a "human-like feature" as a "behavior that would lead a reasonable person to believe that the artificial intelligence system is conveying that it has humanity, sentience, emotions or desires." 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. Similarly, it is difficult to objectively determine when an AI system is "behaving in a way that a reasonable user would consider excessive praise designed to foster emotional attachment with or otherwise gain the favor of the user." These vague terms do not

[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).

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.

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

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.[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. 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.[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.

---

[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*, 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.

The bill's private right of action would result in the proliferation of frivolous lawsuits and questionable claims.

LD 2162 permits "a minor who uses a chatbot that does not comply with the terms of this chapter, or a parent or guardian acting on the minor's behalf" to "bring a civil action independently, or as part of a class action" for the greater of actual damages, or statutory damages of up to $750 "per violation per user per incident." Additionally, the attorney general may bring a "civil action against a person that violates" the bill, with penalties of up to $2,500 per violation, or up to $7,500 for each "intentional violation."

By creating a new private right of action, and even contemplating class actions, the measure would open the doors of state courthouses to plaintiffs advancing costly, time-intensive claims based on subjective criteria. The vague standards noted above will 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.

This dynamic is particularly troubling in the online safety context, where allegations about foreseeability and reasonableness may rest on broad assertions rather than concrete evidence. By making early dismissal functionally unattainable, overly fact-intensive standards risks transforming the litigation process into a blunt regulatory tool — one that imposes substantial costs and uncertainty even in cases that ultimately fail on the merits. These costs would be passed on to individuals in Maine, 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 appreciate your consideration of these issues 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

---

[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/.