U.S. Senate Committee on Commerce, Science, & Transportation

CCIA Position on Kids Online Safety Act, Youth AI Privacy Act, and CHATBOT Act

August 3, 2026

Chairman Ted Cruz (R-TX)
Committee on Commerce, Science, & Transportation
167 Russell Senate Office Building
Washington, DC 20002

Ranking Member Maria Cantwell (D-WA)
Committee on Commerce, Science, & Transportation
511 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Cruz, Ranking Member Cantwell, and Members of the Senate Committee on Commerce, Science, and Transportation:

The Computer & Communications Industry Association ("CCIA") is an international nonprofit association representing a broad cross section of communications and technology firms. For more than fifty 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. While CCIA shares the goal of increasing online safety for minors, three bills scheduled for consideration during Wednesday's markup—S. 1748, the Kids Online Safety Act (KOSA), S. 4199, the Youth AI Privacy Act (YAPA), and S. 4407, the CHATBOT Act—would threaten privacy, reduce parental choice, and create unworkable and often contradictory compliance obligations for digital services. CCIA offers the following concerns:

- The bills incentivize businesses to collect more sensitive data from minors, undermining their privacy;
- The bills allow the government to determine a family's relationship with technology;
- The bills contain vague, overbroad, and contradictory standards that threaten lawful speech and online access; and
- Congress should promote a consistent, workable regulatory landscape nationwide.

I. The bills incentivize businesses to collect more sensitive data from minors, undermining their privacy.

Several of the bills' requirements increase the amount of sensitive data businesses must collect from minors. At a time when data minimization should be a key priority, each of the bills

would require digital services to collect more highly sensitive information than is needed from the most vulnerable of populations. Rather than forcing digital services to collect information they otherwise would not need, Congress should strengthen nationwide privacy protections for minors while promoting digital literacy initiatives and voluntary parental tools. These efforts protect minors online while minimizing the risk that their most sensitive personal information will be exposed to bad actors. Indeed, several of the most devastating data breaches in recent years have arisen directly from age verification systems.

KOSA covers services based on whether they are "reasonably likely to be used" by a minor. Because no objective standard exists for determining when a service is "reasonably likely" to be used by a minor, covered services will be incentivized to verify the ages of all users, requiring the collection of additional sensitive information from both minors and adults.

Likewise, YAPA and the CHATBOT Act employ ambiguous knowledge standards that force businesses to verify users' ages in order to mitigate litigation risk, despite the bill's stated intent not to require age assurance. In practice, businesses cannot reliably mitigate liability under these standards without verifying users' ages. Age and parental verification systems are expensive to develop and maintain, disproportionately burdening smaller businesses and new market entrants while increasing exposure to cybersecurity threats.

KOSA's third-party audit requirement augments these privacy concerns. Besides duplicating existing compliance frameworks, they may expose sensitive operational details through mandatory disclosures that jeopardize user privacy and covered services' proprietary information. This risk carries little reward, as consumer-facing digital services have already built considerable consensus around mitigating risks, such as ISO/IEC 25389.

II. The bills allow the government to determine a family's relationship with technology.

By imposing overly prescriptive parental control requirements, KOSA and the CHATBOT Act would undermine, rather than promote, parental autonomy. Both bills mandate specific default settings and technical controls rather than setting flexible, outcome-based requirements. These restrictions could interfere with beneficial product features and limit companies' ability to innovate and design effective safety tools.

For instance, the bills could restrict routine personalization on a wide variety of services that provide recommendations, such as music, news, or other content suggestions based on user preferences. Restricting personalization on such services would not carry any meaningful safety benefit for minors and would substantially reduce consumer choice.

Similarly, YAPA's broad restrictions on AI-enabled services could discourage the deployment of

basic natural-language functionality on search tools, and other services that present little or no child-safety risk. Instead, Congress should work with industry leaders to promote parental tools that are tailored to the risks associated with each service. These voluntary tools allow parents to determine their family's relationship with technology rather than imposing a one-size-fits-all federal standard.

III. The bills contain vague, overbroad, and contradictory standards that threaten lawful speech and online access.

Many provisions of KOSA, YAPA, and the CHATBOT Act are vague, inconsistent, or unworkable, leaving covered businesses without a reliable way to know if they are complying with the law. Notably, all three bills institute regulations based on whether a business has "knowledge fairly implied on the basis of objective circumstances" that a user is a minor. This standard creates legal uncertainty and unpredictable liability, especially if interpreted to include aggregate information about a service's user base rather than user-specific facts.

KOSA compounds this uncertainty by assigning covered businesses an undefined "duty of care" that invites courts across the country to create conflicting legal standards, leaving digital services without a clear path to compliance. These standards risk arbitrary and inconsistent application of the laws, ultimately forcing digital services to err on the side of defensively removing lawful speech and limiting access to "sensitive" content. In sum, lawful speech and online access will be restricted.

Ironically, a duty of care creates more legal risks to companies that invest the most in online safety. To develop such features, covered services will likely have to gather data about users' ages, which leads to increased liability. By contrast, those who avoid such investments can escape these obligations, and with it, the broad liability that attaches. Legislation should reward investments in online safety rather than deter them by tying those investments to additional legal and compliance burdens. Accordingly, CCIA recommends replacing the undefined duty of care with clearly defined statutory obligations, and "or knowledge fairly implied on the basis of objective circumstances" from the definition of "know" in both bills.

The CHATBOT Act contains several other requirements that are not well-defined. The bill's definition of "AI chatbot" is overbroad. The current definition could sweep in productivity tools, enterprise software, educational and productivity services incorporating general-purpose conversational AI, customer-service bots, embedded AI assistants, and other tools that do not pose the child-safety risks the bill is intended to address.

YAPA raises similar concerns because its broad scope risks encompassing a wide range of AI-enabled services that present minimal child-safety concerns. For example, educational and productivity services incorporating general-purpose conversational AI, search tools, or

customer-support functions that incorporate basic natural-language capabilities could be swept into the bill despite presenting little or no child-safety risk. To fix this issue, the definition should be limited to AI systems designed and marketed to simulate a sustained human or human-like relationship with a user, rather than capturing any open-ended conversational AI tool.

Similarly, the definition of "covered entity" should be narrowed to exclude developers of general-purpose AI systems that another digital service has incorporated into a user-facing chatbot, while the definition of "targeted advertising" should be narrowed to exclude ads based on first-party data. Likewise, recent revisions removed the bill's "primary function" limitation, significantly expanding the range of covered services. As a result, AI assistants offered as one feature among many within broader platforms may now be swept into the legislation despite presenting little relationship to the harms the bill seeks to address. The legislation should instead focus on AI systems designed and marketed to foster sustained social or emotional relationships with users, rather than task-oriented or ancillary AI features.

The CHATBOT Act also imposes contradictory obligations on covered businesses. The bill simultaneously requires immediate deletion of all personal data upon account termination while also requiring that data to remain available during a 90-day portability window. Fulfilling both of these requirements may prove impossible. Moreover, mandatory data portability requirements may inadvertently increase cybersecurity risks by requiring businesses to create additional public-facing mechanisms for transmitting sensitive user data.

IV. Congress should promote a consistent, workable regulatory landscape nationwide.

The bills now expressly establish federal minimum standards while preserving states' ability to impose additional requirements. This "floor but not ceiling" approach will subject digital services to overlapping and potentially inconsistent legal obligations, frustrating Congress's goal of creating a predictable national framework.

Failure to institute unified federal frameworks has imposed substantial compliance costs in many technological sectors. In practice, every state will contend that its own requirements provide "greater" protections for minors, inviting litigation over the scope of federal preemption and leaving courts, not Congress, to define the governing legal standards. These costs disproportionately burden smaller businesses and new entrants, reducing competition and innovation.

Finally, the bills should ensure consistent, equitable enforcement. To achieve this end, the FTC should have exclusive regulatory authority rather than allowing state attorneys general enforcement powers. Covered businesses should have sufficient opportunity to cure violations before enforcement actions can be brought, and the bill should require the FTC to show actual

harm to a consumer when bringing such actions.

* * * * *

In sum, KOSA, YAPA, and the CHATBOT Act would undermine the very online safety goals they seek to advance. The bills require minors and parents to disclose more sensitive personal information, discourage investments in online safety, reduce parental autonomy, rely on vague legal standards, threaten lawful online speech and access, and create an increasingly fragmented regulatory landscape, while expanding uncertainty regarding which AI systems and digital services are covered. As a result, minors' privacy and safety will be reduced while businesses will be unable to clearly ascertain their legal obligations. These bills must be substantially re-worked if they are to further their own goals.

Sincerely,

Brian McMillan
Vice President, Head of U.S. Policy
Computer & Communications Industry Association