



August 5, 2026

The Honorable Ted Cruz
Chair
U.S. Senate Committee on
Commerce, Science & Transportation
Washington DC, 20510

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on
Commerce, Science & Transportation
Washington DC, 20510

RE: Concerns with the SCREEN Act, KOSA, the Youth AI Privacy Act, and the CHATBOT Act

Dear Chair Cruz and Ranking Member Cantwell,

The Electronic Frontier Foundation (EFF) writes to share our concerns with the current text of several bills being considered before the Committee: the SCREEN Act (S. 737),¹ the Kids Online Safety Act (S. 1748),² the Youth Privacy Act (S. 4199),³ and the CHATBOT Act (S. 4407).⁴

EFF is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 32,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to technology.

We appreciate the Committee's longstanding commitment to protecting the privacy of children and adults, and the goals of many of these bills are laudable. But the current versions of these four bills would jeopardize, not enhance, the privacy and personal safety of all internet users.

¹ Shielding Children's Retinas from Egregious Exposure on the Net Act, S. 737, 119th Congress, first session. Sponsored by Senator Mike Lee. <https://www.congress.gov/bill/119th-congress/senate-bill/737/text>

² Kids Online Safety Act, S. 1748, 119th Congress, first session. Sponsored by Senators Marsha Blackburn and Richard Blumenthal. <https://www.congress.gov/119/bills/s1748/BILLS-119s1748is.pdf>

³ Youth AI Privacy Act, S. 4199, 119th Congress, second session. Sponsored by Senator Ed Markey. <https://www.congress.gov/119/bills/s4199/BILLS-119s4199is.pdf>

⁴ Children's Health, Advancement, Trust, Boundaries, and Oversight in Technology Act, S. 4407, 119th Congress, second session. Sponsored by Senator Ted Cruz. <https://www.congress.gov/bill/119th-congress/senate-bill/4407/text?s=2&r=4&hl=s.4407>

AGE VERIFICATION HARMS PRIVACY FOR ALL USERS

While the bills under consideration are all directed towards minors, the consequences won't be limited to minors. If websites and apps are expected to reliably identify teenagers, adults will be asked to prove they are adults by turning over personally identifying information, either to the platform itself or to third parties.

These bills do not increase user privacy. Rather, they create new privacy problems. Whether companies verify ages by checking government IDs, performing facial analysis, checking users' bank records, or collecting other personal information, these systems require the handing over of more sensitive data to access lawful online speech and services. Once a user turns their personal information over, it's now vulnerable to leaks, data theft, or misuse. This isn't just a hypothetical—we've already seen several breaches of age verification providers.^{5 6}

A better approach would be to offer the same privacy protections to all users and avoid the need for additional data collection to know a users' age.

THE SCREEN ACT

The Shielding Children's Retinas from Egregious Exposure on the Net Act (the SCREEN Act) is a sweeping age-verification bill that would require online services to verify users' ages before they can access any sexually explicit content. If this bill passes, it will force millions of adult internet users to give up their anonymity, privacy, and security before they access lawful speech.

Unlike many state-age verification laws—which have been harmful in their own right—as introduced, the SCREEN Act has no requirement that a significant portion of the website consist of sexually explicit content that is harmful to minors. The bill requires nearly any service hosting even a *single* piece of sexually explicit content to verify the ages of its users. The result is that the bill would apply not only to adult content sites like Pornhub or OnlyFans but streaming services and social media platforms like Reddit, Discord, or Bluesky, if they host any adult content.

Unlike some of the other bills that incentivize or require age verification, the SCREEN Act does not merely require users to attest they are adults. It specifically states that “requiring

⁵ Discord Voluntarily Pushes Mandatory Age Verification Despite Recent Data Breach, by Rindala Alajaji and Samantha Baldwin. February 12, 2026. <https://www.eff.org/deeplinks/2026/02/discord-voluntarily-pushes-mandatory-age-verification-despite-recent-data-breach>

⁶ Hack of Age Verification Company Shows Privacy Danger of Social Media Laws, by Jason Kelley. June 26, 2024. <https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws>

a user to confirm that the user is not a minor shall not be sufficient.” In practice, that means platforms would have to verify users’ ages using methods tied to their real identities. Providing proof of age online is dramatically different, and far more invasive, than showing your ID at the door to a bartender or bouncer.⁷ In the physical world, the bouncer at the door looks at your ID card, confirms you’re old enough, and gives it back to you. Under the SCREEN Act, the “bouncer” will be a digital age-verification service that captures your personal information and saves it to a database for an unspecified amount of time.

The SCREEN Act only includes weak data security protections that impose no meaningful collection, use, or retention limits on services collecting people’s private information.

As written, third party vendors tasked with verifying a user’s age on a platform can collect personal information beyond what is necessary to comply with the law and then use that information for any number of purposes, so long as the vendors deem their actions reasonable. These companies would then be allowed to keep the information users have been compelled to provide for as long as possible, raising security and privacy issues.

The SCREEN Act also targets virtual private network (VPN) users and providers. Unless the service can determine that the user is outside the United States the bill requires covered websites to verify users’ ages based on their IP addresses and specifically requires age verification on traffic coming from known VPN addresses. In practice, this discourages the use of VPNs and proxy servers, which millions of people rely on for vitally important purposes such as protecting personal privacy, securing public Wi-Fi connections, safeguarding journalists and activists, and preventing data tracking.

In short, the SCREEN Act creates onerous age-verification rules that will jeopardize the data security and privacy of all internet users, block adults from accessing lawful speech, and curtail their ability to be anonymous.

THE KIDS ONLINE SAFETY ACT

As introduced, S. 1748 imposes a “duty of care” of reasonableness on online services, including social media, to avoid exposing young people to certain material and features the law deems harmful. But those obligations only work if online services know which users are minors. That means more platforms will be pressured to implement age verification or age estimation systems.

KOSA also empowers attorneys general in states across the country to enforce the bill, meaning those elected officials get to decide what’s appropriate online content for teens

⁷ Why Isn’t Online Age Verification Just Like Showing Your ID In Person? Available at: <https://www.eff.org/pages/online-vs-person-id-checks>

across the country. This will likely lead to limits on what adults are able to see online, as companies shut down potentially controversial forums to avoid legal action.

Whatever disclaimers and exceptions the bill includes, the practical effect is unchanged. When platforms face liability for content that someone later claims contributed to harms like anxiety, eating disorders, or substance use, the safest response is to remove lawful speech or shut down forums discussing those topics altogether. This can include forums where people try to help each other, find community and recovery resources for the exact harms listed in the bill, like gambling and drug addiction. In trying to protect young people, KOSA may actually cut them off from valuable sources of support.

THE YOUTH AI PRIVACY ACT

The Youth AI Privacy Act would require AI companies to create kids-only privacy rules and implement so-called “safe design features,” which would actually require more data collection and make it harder for people to access lawful speech online.

This bill contains a problematic and vague provision that expressly allows AI companies to collect a known minor’s personal data for the purpose of testing, identifying, and addressing “harm to users”—without being clear on what exactly that means. Either way, services will need to collect even more information from young people, who are already targets of data theft and identity fraud.⁸

The bill includes some positive privacy provisions around prohibiting the processing of personal information, like limiting what companies can do with people’s chat logs, including training, profiling, and disclosing them to other companies for training. But a general privacy bill must set these limits for everyone, not just minors.

The bill also requires the use of “safe design features,” which would restrict how online services providers design their systems and would deny teenagers the ability to use features like push alerts and notifications.

⁸ Age Verification Systems Are Surveillance Systems. Available at: <https://www.eff.org/pages/age-verification-systems-are-surveillance-systems#main-content>

We have seen this same type of restriction, sometimes called “age appropriate design code” in several states, including in California,⁹ Texas,¹⁰ and Arkansas.¹¹ Unfortunately, these restrictions run into constitutional problems. In fact, federal courts have largely blocked these laws from going into effect because they likely violate the First Amendment rights of all internet users and the online services they regulate. Specifically, these laws interfere with internet users’ First Amendment rights to either speak or access speech online, and they also violate the rights on online services to decide how they will present information on their sites.

Similarly, the Supreme Court has repeatedly ruled that “minors are entitled to a significant measure of First Amendment protection.”¹² This does not mean that parents or guardians can’t set their own rules for their families—they can and they should, based on the needs and circumstances of the individual teenagers. But it does mean that Congress cannot adopt a “one size fits all” regulation that sets a restrictive government default that affects the First Amendment rights of all internet users, including teenagers.

THE CHATBOT ACT

The CHATBOT Act takes the decision about what role AI should play in schoolwork and everyday life away from families. Instead, Congress would require every covered AI chatbot to build the same federally prescribed “family account” system.

As part of the required parental-consent process for teens, AI companies must offer parents a “family account” that provides access to a “full record of the conversations and activity” of teen users and tools to “monitor, analyze, and understand, at scale” those conversations. They must also send alerts if a teen attempts to bypass or disable parental controls.

This isn’t simply an optional parental-control feature. The bill requires every covered AI provider to build this monitoring infrastructure and present it as part of the parental

⁹ NetChoice, LLC v. Bonta. Order on Motion for Preliminary Injunction, Document 74, by Judge Beth Labson Freeman. September 18, 2023. Available at: <https://www.courtlistener.com/docket/66636540/74/netchoice-llc-v-bonta>

¹⁰ Brief of amici curiae American Civil Liberties Union, Center for Democracy & Technology, Electronic Frontier Foundation, Foundation for Individual Rights and Expression, Media Coalition Foundation, and Tech Freedom, *Free Speech Coalition, Inc v. Angela Colmenero*. September 26, 2023. Available at: <https://cdt.org/wp-content/uploads/2023/09/FSC-v.-Colmenero-amicus-brief-.pdf>

¹¹ Age Verification Mandates Would Undermine Anonymity Online, by Jason Kelley and Adam Schwartz. March 10, 2023. <https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online>

¹² *Erzonznik v. City of Jasonville*, 422 U.S. 205, by Judge Lewis F. Powell, Jr., Supreme Court of the United States. 1974. Available at: <https://www.loc.gov/item/usrep422205>

consent process. Congress is prescribing a single, highly invasive model of how families should supervise teenagers' use of AI.

Parents and families have different ideas about how much independence teenagers should have. Understandably, they also have very different expectations for 8-year-olds, 13-year-olds, and 17-year-olds. The CHATBOT Act effectively requires AI providers to build the same monitoring architecture for users of very different ages.

And this mandated data collection will create new privacy and security risks. Once Congress requires AI companies to create a permanent, centralized record of teen AI conversations for parental review, that will be a valuable vault of extremely personal information. The vast archives of conversations won't be interesting only to parents. They will become valuable targets for hackers, identity thieves, civil litigants, and anyone else seeking access to the deeply personal information of others. The CHATBOT Act requires the records to exist but addresses none of those risks.

The CHATBOT Act takes the basic structure of COPPA,¹³ a nearly 30-year-old law that applies to children aged 12 and under and applies the same “verifiable parental consent” to older teenagers. That’s a dramatic expansion of the law. Congress enacted COPPA to prevent kids from handing over detailed personal information to online services without making sure parents approved. For nearly three decades, Congress has required parental consent before websites collect personal information from any user under 13. Children under 13 are already not allowed to use Microsoft Co-Pilot,¹⁴ Google Gemini,¹⁵ or ChatGPT.¹⁶ Anthropic does not allow users under 18 to use its AI model, Claude.¹⁷

COPPA’s protections against collecting personal information from minors without parental consent already apply to the AI services CHATBOT Act seeks to regulate. Worse, the CHATBOT Act takes COPPA’s privacy protections and inverts them—it will result in AI services likely collecting *more* information about young users.

And the CHATBOT Act also extends that model to high school students using AI assistants that are rapidly becoming tools for learning, research, writing, coding, and creative work. It

¹³ Children’s Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505. Available at:

<https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

¹⁴ Microsoft Copilot for Young People. Available at: <https://support.microsoft.com/en-us/microsoft-copilot/microsoft-copilot-young-people>

¹⁵ Gemini Apps Help: Gemini Apps limits & upgrades for Google AI subscribers. Available at: <https://support.google.com/gemini/answer/16275805?hl=en>

¹⁶ OpenAI: Is ChatGPT safe for all ages? Available at: <https://help.openai.com/en/articles/8313401-is-chatgpt-safe-for-all-ages>

¹⁷ Claude Support: Minimum age requirement access restrictions. March 16, 2026. Available at: <https://support.claude.com/en/articles/13117299-minimum-age-requirement-access-restriction>

then mandates specific, invasive surveillance tools that go well beyond anything COPPA requires.

Supporters may argue that parents of teens don't have to create a family account. But every family with a teenager will still have to go through the bill's parental-consent process before a teenager can use a covered AI system. Providers will need practical ways to verify that an adult is, in fact, the teenager's parent. And parents of kids under 13 have no option to consent to their kids' use of an AI system—the bill's only option is to create a family account.

Congress should not extend the COPPA parental-permission model to millions of older teenagers, and it would be harmful to do so. The government does not require COPPA-style parental permission before a 17-year-old checks out a library book, uses Wikipedia,¹⁸ types search terms into Google, or reads a newspaper online.¹⁹ It shouldn't require parental permission simply because the same question gets asked of an AI assistant. Parents who want family accounts like those described in the bill should be free to choose AI services that offer them. But Congress shouldn't pressure every provider to collect more information about everyone's age simply to comply with the law.

CONCLUSION

Minors deserve meaningful privacy protection online—as do adults. But all of these bills move in the opposite direction by encouraging more data collection, more age verification, as well as more legal pressure for platforms to monitor and restrict lawful speech.

The Senate Commerce Committee should reject these bills. Instead, the Committee should pursue comprehensive privacy legislation that protects everyone—minors and adults—without undermining privacy, security, or free expression.

Thank you for your consideration of our concerns. If you have any questions, please contact India McKinney, EFF's Director of Federal Affairs, at india@eff.org.

¹⁸ Wikipedia: Guidance for younger editors. Available at:

https://en.wikipedia.org/wiki/Wikipedia:Guidance_for_younger_editors

¹⁹ New York Times Help Center. Available at: <https://help.nytimes.com/115014893428-Terms-of-Service>