

## The Senate's GUARD Act would sacrifice privacy and parental rights

*The federal Guidelines for User Age-verification and Responsible Dialogue Act (GUARD Act) would impose mandatory identity verification on every American chatbot user, create criminal liability for covered companies under a vague standard, mandate disclosures that a user is talking to a chatbot every 30 minutes, and bar minors from using artificial intelligence (AI) companion products outright. These choices raise serious privacy and First Amendment concerns that would undermine the bill's child-protection goals.*



### Universal age verification threatens privacy and anonymous speech

- Mandates that every user of every covered chatbot create an account and verify age before access, with no exception for adults. Self-attestation and birth date entry are explicitly insufficient.
- Forces adults to surrender sensitive identifying information, including government IDs or biometric data, to use a chatbot. This sacrifices the First Amendment right to anonymous speech and access to information, which courts have recognized in cases involving online expression.
- The verification mandate builds a national identity database of every chatbot user. Concentrating sensitive personal data at this scale makes users vulnerable to identity theft, breach, and surveillance. The bill's data minimization and retention language does not eliminate the underlying risk.

### Ban on minor access removes parental rights

- Prohibits age-verified minors from accessing any AI companion.
- Substitutes federal judgment for parental judgment. Parents, not Congress, should decide which AI products are appropriate for their own children.
- Reaches every user under 18, with no tier for older teens and no parental consent override, even if a parent has evaluated a product and judged it appropriate.

### Criminal liability rests on a vague standard

- Creates new federal crimes in Title 18 for designing, developing, or making available a chatbot with “knowing or reckless disregard” for risk that it solicits minors into sexually explicit conduct or promotes suicide, self-harm, or violence. Civil and criminal penalties reach \$100,000 per offense, enforced by the U.S. and state attorneys general.

## Backgrounder

- Criminalizes design choices that create the possibility of harm, not the harm itself. AI systems produce outputs that developers cannot fully predict, and a vague, reckless standard paired with criminal fines pushes developers to over-restrict speech or exit the market.
- Provides no safe harbor for developers who implement reasonable safety measures, document testing, and respond to identified risks. Federal law should reward continuous good-faith improvement, not ignore it.

### Federal floor invites fragmented state regulation

- Sets a federal floor rather than a ceiling with Section 7(e), allowing any state to add stricter requirements on top of the federal scheme. Chatbot developers could face numerous, potentially competing compliance obligations across states. A federal chatbot standard should preempt inconsistent state regulation to give parents, children, and operators a single coherent rule.

**Bottom Line:** The GUARD Act would build a surveillance regime without materially improving child safety. A better legislative approach would target harmful conduct, give operators safe harbors for good-faith safety practices, and set a single clear federal standard without compelling disclosure of sensitive personal information.