Backgrounder

The Senate's CHATBOT ACT could undermine privacy and free speech

The Children's Health, Advancement, Trust, Boundaries, and Oversight in Technologies Act (CHATBOT Act), S. 4407, would impose new requirements on chatbot users under 18, require chatbot services to be built around family accounts, and lock default settings into their most restrictive privacy and safety levels. While well-intended, in practice, this approach raises significant First Amendment and privacy concerns.

Age verification would be a precondition for access

- Users under 13 must use a parent-controlled family account, and parents of users 13 and 17 must receive direct notice and give verifiable parental consent before a teen user can create an account.
- Knowledge of a user's age is defined to include information "fairly implied on the basis of objective circumstances," a vague standard that encourages more data collection from all users to avoid legal liability.
- Core requirements depend on reliably determining user ages and verifying parent-child relationships, which pushes companies toward intensive verification systems that use sensitive identifiers such as government IDs or biometric data.
- With penalties exceeding $50,000 per violation, companies would have strong incentives to rely on intensive verification as the safest legal option.

Verification systems would threaten privacy and anonymous speech

- Children would face significant risks because the verification systems meant to protect them require collecting and storing sensitive personal data that makes minors vulnerable to identity theft, surveillance, and data breaches.
- Adults would be required to surrender sensitive identifying information to prove they are not minors, sacrificing anonymous speech protected by the First Amendment.

Product design mandates would replace outcome-based safety standards

- S. 4407 mandates specific design architecture built around family accounts, verifiable parental consent flows, and detailed parental controls, including time limits, notification toggles, transparency labels, parental access to usage time and conversations, and tiered data retention.

Reason Foundation Technology Policy Contact, Richard Sill, Technology Policy Analyst (richard.sill@reason.org)

- The act requires all family account controls to start at maximum protection by default, unless parents actively reduce restrictions, and bans targeted advertising using minors' data.
- Locking in this single model would freeze product design at enactment and assume one architecture fits every chatbot service.
- The bill is vague on how to identify and verify parent-child relationships, yet requires terminating all minor accounts without family accounts or consent and deleting their data, forcing broad account shutdowns under unclear rules.

Bottom Line: Rather than encouraging identity verification mandates and rigid design requirements, Congress should make clear in any chatbot legislation it ultimately passes that it is a national ceiling for chatbot regulation to avoid fragmented compliance obligations across states. Such legislation should incentivize good behavior, for example, by offering and improving parental controls and teen or family accounts, rather than punishing companies based on rigid compliance standards. Together, these changes would produce a law that genuinely puts parents in control without creating surveillance infrastructure, stifling beneficial AI technologies that help children learn and grow, or undermining the First Amendment.

Reason Foundation Technology Policy Contact, Richard Sill, Technology Policy Analyst (richard.sill@reason.org)