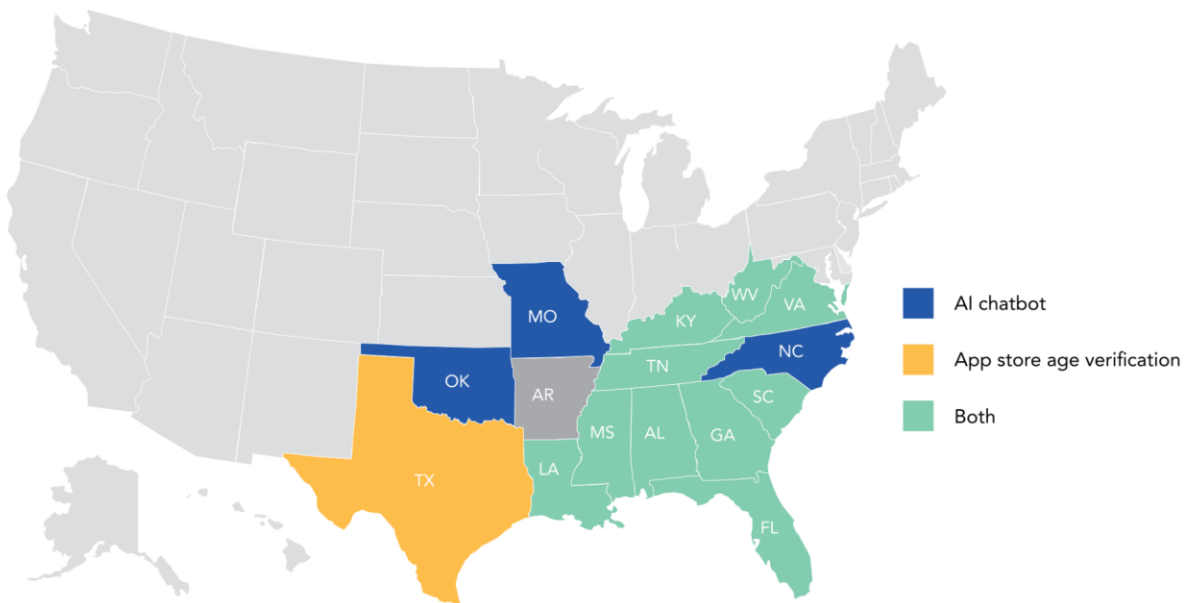


# Artificial Intelligence and Youth Online

As artificial intelligence (AI) use has become widespread, state lawmakers have wrestled with how to implement appropriate guardrails without stifling a nascent industry through overregulation. Online access by minors has drawn particular scrutiny over concerns relating to artificially generated sexual content, potentially harmful mental health content, and unhealthy relationships with AI chatbots. States have also pursued broader child-online-safety litigation against major technology companies, including a multistate [settlement](#) with Meta in 2026 over alleged harms to young social media users.

This year, Southern state lawmakers proposed several measures aimed at limiting minors' exposure to potentially harmful AI interactions and content, including companion chatbot regulation, age verification requirements for app stores, and design code requirements for minors. Underlying these proposals are questions relating to which services should be regulated, how to determine which minors are users, and what protections should be applied.

## Recent AI Chatbot and App Store Age-Verification Legislation in Southern States



Source: MultiState. Data as of September 2026. Reflects examples of legislation addressing companion chatbots or app store age verification requirements during the 2025–26 legislative cycle. Texas's app-store law was enacted in 2025 and took effect in 2026.

## Legislative Response

### *Federal Preemption*

President Trump’s push to limit state regulation of AI loomed over state legislative debates in 2026. In December 2025, Trump signed an [executive order](#) calling for a “minimally burdensome national policy framework” for AI and directing his administration to identify and potentially challenge state laws deemed inconsistent with that approach. The administration has argued that AI regulation could inhibit innovation and ties the issue to federal broadband funds and discretionary grants. The White House’s subsequent national AI legislative [framework](#) calls for federal preemption of state AI laws that impose undue burdens, while preserving states’ authority to enforce generally applicable laws that protect children, prevent fraud, and protect consumers.

While many argue that a patchwork of state requirements could impede innovation and support federal preemption, [Florida Governor Ron DeSantis](#) (R) asserted his state’s role in AI regulation. He proposed an [AI “Bill of Rights”](#) that would have created consumer protections relating to AI use and required large AI models to allow parents to monitor and manage minors’ interactions. However, the measure [failed to advance](#) when House Speaker Daniel Perez (R) opposed state regulation in favor of a federal solution. The White House weighed in on other state legislative debates, [opposing an AI safety and transparency bill](#) in Utah and pressing lawmakers in [Missouri and Tennessee](#) to narrow proposed AI safeguards.

Despite looming federal preemption efforts, many states nationwide enacted new AI-related laws. Legislative activity was more limited in the South, although lawmakers were considerably more active in proposing measures aimed at protecting children online.

### *Companion Chatbots*

Artificial intelligence chatbots are increasingly being used not only to answer questions or complete tasks, but also to provide companionship, emotional support, and conversation. Their growing use among young people has raised concerns. A [2025 Common Sense Media survey](#) found that nearly three-quarters of U.S. teens had used AI companions, with more than half using them regularly and about one-third of users reporting that they had chosen an AI companion instead of a person for an important or serious conversation.

Those concerns have intensified following high-profile lawsuits alleging that chatbot interactions encouraged self-harm, exposed minors to sexual content, or reinforced other dangerous behavior. In June, Florida Attorney General James Uthmeier (R) filed a [first-of-its-kind state lawsuit](#) against OpenAI, alleging the company concealed serious risks to minors associated with ChatGPT and suppressed

internal safety warnings. The lawsuit followed a [criminal investigation](#) launched by Attorney General Uthmeier's office into whether OpenAI bears responsibility for ChatGPT's interactions with the gunman accused of killing two people at Florida State University in 2025. Kentucky Attorney General Russell Coleman also [filed suit](#) against Character.AI in January 2026, alleging that the company's chatbots exposed minors to harmful and sexualized interactions and failed to provide adequate safeguards. Texas Attorney General Ken Paxton has similarly [investigated](#) Meta AI Studio and Character.AI over concerns involving AI companion chatbots and child safety.

In 2026, Georgia ([GA SB 540](#)) enacted legislation to regulate AI companion chatbots, with at least another 11 Southern states considering related measures. The bills generally focused on requiring chatbots to disclose that users are interacting with AI, establishing protocols for responding to suicidal ideation or self-harm, and providing enhanced protections for minors, including restrictions on sexual content and manipulative or addictive engagement techniques.

As chatbots become increasingly capable of simulating friendship, romance, and emotional support, lawmakers have raised concerns that users, particularly minors, may develop a sense that they are interacting with a human rather than software. Disclosure requirements seek to counter that risk by periodically reminding users that they are interacting with an AI system. Companion chatbot laws require some form of disclosure, although the circumstances and frequency vary. A proposed Florida bill ([FL HB 1395](#)) would have required a reminder at the beginning and at least once every hour of an interaction (for minors).

Companion chatbots can engage in personal and emotionally responsive conversations, so users may disclose sensitive issues, much as they might to a family member, therapist, or faith leader. Companion chatbot legislation typically requires operators to establish protocols for responding to expressions of suicidal ideation or self-harm, generally by making reasonable efforts to direct users to crisis services. A proposed bill in South Carolina ([SC SB 1037](#)) would have required covered operators that learn a user faces an imminent risk of death or serious physical injury to make reasonable efforts to notify emergency services or law enforcement within 24 hours. If insufficient information makes notification impracticable, the operator must direct the user to emergency and crisis resources, encourage them to seek immediate help, and document its response. Determining when protocols should be triggered remains a difficult policy question. Users may discuss these matters through jokes, sarcasm, hypothetical scenarios, or fictional role-play, making it difficult for an AI system to distinguish a genuine crisis from nonliteral speech. States have also differed over what an appropriate intervention should entail. Tennessee separately enacted [SB 1580](#), which prohibits AI systems from advertising or representing themselves as qualified mental health professionals.

Minors have emerged as a significant focus of companion chatbot regulation, with states layering additional safeguards reflecting concerns that children may be particularly susceptible. The Georgia law directs chatbot operators to implement measures for minor users that prevent the chatbot from

leading a person to believe the interaction is with a human, engaging in sexual or romantic interactions, encouraging secrets or social isolation, simulating distress when the user disengages, encouraging self-harm, manipulative behavior, or soliciting purchases.

States have taken notably different approaches, however, to determining who receives these protections. Florida lawmakers introduced a bill ([FL SB 1344](#)) that would have required chatbot operators to use standard age verification or anonymous age verification to determine if a user is a minor. A proposed Louisiana bill ([LA HB 295](#)) would have banned any access to companion chatbots for minors, and required operators to use “reasonable age-verification methods.” Other states require age estimation, or only trigger protections when an operator has knowledge that a user is a minor, such as a proposal in Virginia ([VA HB 635](#)).

### *Age Verification and Child Online Safety*

Child online safety was a major theme of southern legislative sessions, as lawmakers responded to growing concerns about the effects of social media and other digital services on young people. Age verification has emerged as an increasingly common policy tool, providing a way for online services to identify minors and apply heightened protections, such as parental consent requirements, limits on certain content or features, and enhanced privacy and safety settings. Age verification requirements may direct a user to provide identification or information that can be checked against existing records or use technologies that confirm a user’s age.

Privacy advocates have challenged these requirements, arguing that they can require the collection of sensitive personal information and may discourage users from accessing online services if they are uncomfortable providing identification or other personal data. To address those concerns, some measures have proposed “age assurance,” requiring platforms to make a reasonable estimate of a user’s age based on information it has already collected about a user, without requiring more invasive measures. Other proposals have even relied on user age attestation, where a user simply enters a birth date or confirms they are over a certain age.

Mississippi enacted [HB 1224](#), the Mississippi Keeping Kids Safe Online Act, which imposes protections governing minors’ use of certain interactive online services and requires new internet- and social-media-safety resources for students and families. North Carolina also proposed a child online safety measure. [HB 301](#) would prohibit children under 14 from maintaining accounts on covered addictive social media platforms, require parental consent for 14- and 15-year-olds, and require age verification for new accounts.

Lawmakers have also debated which entities should be responsible for verifying a user’s age, with proposals placing that responsibility on websites and applications, app stores, operating systems, or

device manufacturers. Alabama ([AL HB 161](#)) and Louisiana ([LA HB 977](#)) each enacted laws requiring app store providers to verify a user's age category, requiring a minor's account to be linked to a parent with parental consent to download certain apps.

### *Age-Appropriate Design Codes*

Age-appropriate design codes take a broader approach to protecting minors online by requiring companies to consider how the design of their services, as well as their data practices, may affect younger users. South Carolina enacted a law ([SC HB 3431](#)) requiring covered online services to exercise reasonable care in their use of minors' personal data and provide safeguards for users they know are minors. The law applies to online services reasonably likely to be accessed by minors, including those powered in whole or in part by artificial intelligence, and requires offering parental controls. Covered services must give minors tools to limit communications with other users, protect their personal information, manage personalized recommendations, and opt out of certain features designed to increase engagement.

These measures typically provide heightened online privacy protections for minors. For example, Arkansas' 2025 "Kids Online Safety Act" ([AR HB 1726](#)) would have put limits on public access to minors' personal data, provided geolocation protections, account and data deletion rights, controls over personalized recommendations, and required transparency for data collection and targeted advertising. Another bill in Georgia ([GA SB 495](#)) would have required covered entities to provide the safest design as the default for minors, and set all privacy settings to the highest level by default, including disabling settings that allow unknown adult users to connect, and disabling search engine indexing.

## **Looking Ahead**

Online child safety will continue to be an issue next session, with recent settlements and other successful lawsuits likely to energize legislative efforts. Many online child safety laws have faced legal challenges over constitutional rights and free speech, so expect lawmakers to tweak laws to address judicial concerns. Courts have shown greater willingness to allow some age-verification requirements to stand, [upholding a Texas online age verification law](#) in 2025 and allowing the [state's app store law](#) to be enforced this year.

States are also likely to continue pursuing AI-specific protections for minors. Although the administration has not independently brought a lawsuit challenging a state AI law, it has intervened in litigation challenging such laws. Companion chatbot regulation is likely to remain a major focus,

particularly as lawmakers consider age verification, restrictions on sexual content, crisis-intervention protocols, and other safeguards for minors.