Articles + Publications | August 4, 2025

Justices' Age Verification Ruling May Lead To More State Laws

WRITTEN BY

Laura Hamady | Jeff P. Johnson | Jessica M. Birdsong | Christopher Carlson

This article was originally published on August 4, 2025 on Law360 and is republished here with permission.

The digital age presents a complex challenge: protecting children online while also allowing free speech to continue to be a thriving marketplace of ideas.

Recent legal battles highlight this tension, particularly the U.S. Supreme Court's June 27 decision in Free Speech Coalition Inc. v. Paxton, which **permits** more content-neutral regulation over internet activities by states.

The Shifting Legal Landscape

Background

Historically, the Supreme Court has navigated the delicate balance between safeguarding minors from harmful content and preserving adults' access to protected speech. Landmark cases like Ginsberg v. New York and Butler v. Michigan illustrate this tension between content that is protected for adults but subject to state regulation for minors.

In its 1968 Ginsberg decision, the court upheld restrictions on minors' access to obscene materials, recognizing the government's interest in protecting youth.[1] Conversely, its 1957 decision in Butler struck down a criminal law that restricted adult access to content deemed inappropriate for minors, emphasizing that adults shouldn't be limited to content suitable only for children.[2]

Congress recognized that the internet complicated this delicate balance when it enacted the Communications Decency Act and the Children's Online Privacy Protection Act, which attempted to balance the interests between free expression for adults, the protection of children, and the safeguarding of innovation in the digital marketplace.[3]

The Supreme Court found the Communications Decency Act unconstitutional in its 1997 decision in Reno v. American Civil Liberties Union due to its excessive burden on adult speech.[4] Similarly, the Children's Online Privacy Protection Act had a dubious future after the Supreme Court's 2004 decision in Ashcroft v. ACLU suggested that a less restrictive alternative existed in the form of parental filtering software.[5]

Free Speech Coalition v. Paxton: What Happened

In 2023, Texas enacted H.B. 1181, which requires commercial websites to verify the age of their customers if more than one-third of their content is sexual material harmful to minors.

The plaintiffs — an adult entertainment industry trade association and related companies — argued that the law unconstitutionally restricted adults' access to protected speech.

The U.S. District Court for the Western District of Texas, guided by Ashcroft, applied strict scrutiny — the most demanding standard of review — and preliminarily **enjoined** H.B. 1181. In 2024, the U.S. Court of Appeals for the Fifth Circuit vacated the preliminary injunction and applied rational basis review, the most lenient standard of constitutional review. The Supreme Court **granted certiorari** to determine which standard of review should apply to H.B. 1181.

Writing for the court, Justice Clarence Thomas found that courts should apply intermediate scrutiny, where a law will pass muster if it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests.

The court's analysis concluded that age verification laws fall within a state's traditional power to prevent minors from viewing obscene material, as evidenced by long-standing in-person verification statutes, and that age verification "is a necessary component of [that] power." It reflected that laws often require age verification to exercise a fundamental right, such as a firearm license.

Further, the court distinguished prior regulations that applied strict scrutiny as cases in which the restriction operated to burden adults from accessing constitutionally protected material.

The court determined that H.B. 1181 only incidentally burdened speech for adults and advanced the important governmental interest in protecting minors from harmful, and importantly, constitutionally unprotected speech.

No party disputed that the government has an important interest in protecting children from obscene material. And the court explained that H.B. 1181 permitted verification via government identification documents to third-party verification services and transactional data, such as credit cards, which have long been used by the adult entertainment industry.

Because the court found that intermediate scrutiny applied, it rejected the petitioners' claim that less restrictive means exist, as the standard only requires that H.B. 1181 is adequately tailored.

Impact on Child Online Privacy and Safety

The Free Speech Coalition decision will significantly expand states' ability to regulate social media access for minors. By applying intermediate scrutiny to regulations that incidentally burden adults' free speech while targeting minors' access to adult content, the court has signaled a favorable view of such measures.

Practically speaking, this means that government regulation over the means of compliance — such as requiring commercially reasonable or recognized age verification practices — is also likely to pass judicial review.

This decision will incentivize more states to adopt similar social media, privacy and age-appropriate design regulations, potentially resulting in the adoption of robust age verification systems across many types of online properties.

It's critical to emphasize what the Free Speech Coalition decision does not change. States still may not create new categories of unprotected speech, as established in the Supreme Court's 2009 decision in U.S. v. Stevens.[6] Outside of existing categories — like obscenity, defamation, fraud, incitement or speech integral to criminal conduct — strict scrutiny, which is almost always fatal to regulation, will apply.[7]

Indeed, in its 2011 decision in Brown v. Entertainment Merchants Association, the court rejected California's attempt "to create a wholly new category of content-based regulation that is permissible only for speech directed at children."[8] While these permissible categories are narrowly limited, they encompass consumer protection and fraud statutes, which courts have declined to limit.

Although the Free Speech Coalition decision applies specifically to regulations governing "sexual material harmful to minors," privacy advocates express concern that this ruling will serve as a precedent for extending age verification requirements to a much broader range of online content and platforms. Such additional regulation will likely affect access to general audience websites and social media, which may overly chill speech for adults.

The case marks a significant change in the Supreme Court's view on government regulation of internet-based commerce. In the early days of the internet, the court expressed reservations about legislation for fear of hampering innovation, considering the rapid changes in technology. In the wake of Free Speech Coalition, the court has now greenlit increased regulation, even as technological capabilities increase at an unprecedented pace.

The Regulatory Patchwork: State Laws Protecting Minors Online

Although age verification tools may help keep minors safe online, they introduce significant privacy risks due to their reliance on sensitive data. These tools often require collecting highly sensitive personal data, such as government-issued identification documents or even biometric data, which is becoming more common to access devices and personal passkeys.

As a result, laws and regulations designed to promote the privacy and safety of minors online will continue to include data handling, retention and other governance requirements. In addition to creating significant data handling and retention burdens for online operators, these burdens also elevate the risk of large-scale data breaches, and the potential for the unauthorized use or sale of improperly exposed data.

Critics point out that the court largely dismissed these privacy concerns in its decision, drawing an analogy to in-person visual identification checks that do not account for the persistent digital footprint created by online age verification. These complex data governance issues will increase the operational costs and complexity for large and small online businesses alike.

Children and Teen Social Media and Online Safety Laws

State legislatures are, and have been, enacting laws that attempt to enhance minors' safety and privacy online — resulting in a challenging regulatory patchwork.

Many require social media companies to conduct age verification checks, often through third-party vendors.[9] Some states — like Florida and Georgia — mandate express parental consent for minors to have social media accounts.[10] Other states have enacted restrictions on features deemed addictive by the legislature.

California, for example, limits minors' access to "addictive" feeds and prohibits notifications during specific hours unless parental consent is obtained.[11] Similarly, Utah bans features like autoplay and infinite scrolling to reduce minors' excessive engagement.[12]

Implementing age verification tools presents significant technological hurdles. The constant evolution of online behavior and technologies, such as the use of artificial intelligence, means that even robust systems may be vulnerable to sophisticated work-arounds by minors, creating an ongoing challenge for platforms and regulators alike to maintain effective controls.

Interplay With Existing Privacy Laws

New state-level online safety laws mandating age verification, parental consent and restrictions on certain platform features interact with existing federal privacy laws and emerging comprehensive state privacy laws.

These overlaps lead to significant challenges. Child safety laws complement comprehensive privacy laws by addressing specific risks faced by minors, such as exposure to harmful content or exploitation through targeted advertising. But businesses must also navigate the complexities of complying with multiple layers of regulation and being able to prove they have complied in the past, ensuring that their practices align with both general privacy standards and specific protections for children.

Defending against state inquiries into their past compliance with age verification laws will be difficult if privacy laws also prevent businesses from collecting or storing information about minors. That is especially salient when businesses must determine what rules apply to which users based on their geolocation data.

Must they determine only that the device accesses the website from a particular jurisdiction, or does the location of their primary residence control? Does a business have to keep such data to show regulators they have complied, and can they share information from one jurisdiction with the regulator in another?

The patchwork definition of "child" also presents complications because at the federal level, the Children's Online Privacy Protection Act only covers children under the age of 13, but states have enacted their own data privacy laws, which can vary significantly in terms of age coverage, parental consent requirements and data protection measures.

This will lead to inconsistencies in how businesses determine what data protection requirements apply, and those practices may conflict between jurisdictions, especially as each state determines when its youth become responsible for their actions.

The Age Verification Conundrum: Legal and Practical Challenges

Implementing age verification technologies presents practical and legal hurdles. Self-attestation is largely understood to be unreliable, and regulators reject it as insufficient. Government-issued ID verification offers accuracy but raises privacy concerns.

Biometric analysis presents different challenges, such as accuracy, bias and equity. Ensuring facial identification technologies are trained on diverse datasets is essential for their effective operation. Although advancements have improved accuracy in leading solutions, there remains a risk of misidentification when systems are trained on data lacking demographic diversity. This highlights the importance of inclusive training to prevent errors, particularly in identifying people of color.

Third-party age-estimation services depend on provider reliability, and device-based solutions require ongoing maintenance.

And all of these methods present the continued challenge of protecting against a data breach that may expose personal information, and risk legal and reputational damage.

Even if these concerns were not significant, the solutions present additional financial and practical costs. New technologies may affect user experience by introducing friction to the accessibility of information or commerce, which can potentially increase user drop-off and lower engagement.

These technologies also cause increased financial and operational costs to provide robust age verification systems, which will affect all businesses, but especially smaller organizations and startups.

Moreover, the accuracy and equity of these technologies are under scrutiny, as biases can lead to disparate impacts on different user populations.

How Businesses Should Respond

With the court signaling that age verification requirements may pass constitutional muster under intermediate scrutiny, the legal fight over online speech is likely to shift from if the state can regulate, to how far such authority can take them. Further, trial and intermediate appellate courts are likely to be mindful of this precedent when evaluating age verification requirements outside the context of websites that include adult content.

Given that state legislatures will pass additional age verification statutes outside the context of adult content, companies must choose whether to comply with such laws — particularly mindful of the implementation burdens, data privacy and whether other approaches could achieve compliance, instead of pursuing legal action to enjoin future laws.

Companies should be mindful that state attorneys general are willing to assert violations of state consumer protection laws if the regulators deem a company's age verification mechanism to be ineffective. In such cases, the states may argue that, by allowing minors to access a platform at all, or without parental consent, companies are misrepresenting the controls they deploy to ensure minors join and navigate their platforms safely. It remains

to be seen whether such lawsuits will pass muster.

---

[1] *Ginsberg v. New York*, 390 U. S. 629 (1968).

[2] *Butler v. Michigan*, 352 U. S. 380 (1957).

[3] Communications Decency Act of 1996, Pub. L. No. 104-104, §§ 501-561, 110 Stat. 56, 133-43 (1996).; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).

[4] *Reno v. American Civil Liberties Union*, 521 U. S. 844, 885 (1997).

[5] *Ashcroft v. American Civil Liberties Union*, 542 U. S. 656, 670 (2004).

[6] 559 U.S. 460 (2010).

[7] Id.

[8] *Brown v. Ent. Merchants Ass'n*, 564 U.S. 786, 794 (2011).

[9] For example, Arkansas mandates the use of third-party vendors to verify users' ages through government-issued identification, ensuring that minors cannot create accounts without proper age confirmation. Ark. Code Ann. § 4-88-1401–1404 (West 2025).

[10] Fla. Stat. Ann. § 501.1736 (West 2025); Ga. Code Ann. § 39-6-2 (West 2025) (effective July 1, 2025).

[11] Cal. Civil Code §§ 1798.99.28–1798.99.40 (West 2025).

[12] Utah Code Ann. § 13-71 (West 2025).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- Regulatory Investigations, Strategy + Enforcement