USA: Legal, regulatory, and enforcement developments regarding children's data

Alaap Shah
Member of the Firm
abshah@ebglaw.com
Epstein Becker & Green, P.C., Washington, DC

Lisa Pierce Reisz
Attorney
LPierceReisz@ebglaw.com
Epstein Becker & Green, P.C., Washington, DC

Introduction

Protecting the digital lives of children in the United States remains a bipartisan concern and continues to be prioritized at the state and federal levels as regulators seek ways to modernize privacy rules in response to new technologies, data-driven business models, and rising social concerns. As minors increasingly interact with digital ecosystems - including social media platforms, artificial intelligence (AI) chatbots, educational apps, and content recommendation engines - the vulnerabilities of children to data exploitation and manipulation have become a central issue for lawmakers.

In recent years, federal and state legislatures, regulators, and enforcement authorities have taken numerous steps to enhance oversight of how children's data is collected, processed, and shared. These legal shifts reflect a growing consensus that the Children's Online Privacy Protection Act (COPPA), first enacted in 1998, is insufficient in isolation to protect minors in today's complex digital environments. In response, both Congress and the Federal Trade Commission (FTC) have sought to modernize COPPA's reach, while a growing number of states remain active by enacting parallel or supplementary privacy laws focused on the protection of minors.

This article surveys the latest developments in US children's privacy law, focusing specifically on enforcement trends and the implications of recent federal and state regulatory updates. It examines the rise of age-appropriate design mandates, heightened data handling obligations, biometric protections, and the expanding role of state attorneys general (AGs).

State enforcement developments: From legislation to litigation

Age verification and platform accountability

One of the most prominent themes in recent children's privacy legislation is the imposition of age verification and parental consent mandates for social media and other digital platforms. State statutes enacted in Florida, Georgia, Tennessee, and Utah in 2024 and 2025 are prime examples of this movement. Florida's Social Media Safety Act, for example, prohibits children under 14 from creating accounts and mandates parental consent for users aged 14 or 15. Enforcement mechanisms include monetary penalties and injunctive relief, with state AGs empowered to bring civil actions.

Similarly, Tennessee's Protecting Children from Social Media Act authorizes parental monitoring and consent dashboards, signaling a shift toward operational transparency and family-level oversight. States such as Georgia and Utah have added requirements for age verification on both personal and school-issued devices, further broadening the scope of compliance responsibilities for platforms.

While these laws aim to mitigate online harms such as addiction, exposure to adult content, and data misuse, their enforcement

has been uneven due to ongoing litigation challenging the constitutionality of such laws. By way of illustration, in *NetChoice v. Bonta*, the Ninth Circuit blocked provisions of California's design code law, finding potential First Amendment violations. Meanwhile, Utah's age verification laws are currently stayed pending similar litigation in *NetChoice, LLC v. Reyes*, which is currently under appeal before the U.S. Court of Appeals for the Tenth Circuit. Nonetheless, the existence of legal challenges has not deterred states from adopting increasingly aggressive regulatory postures.

Age-appropriate design codes and risk mitigation

States are also embracing design-centric regulatory frameworks modeled on the UK's Age Appropriate Design Code. California's Age-Appropriate Design Code Act requires platforms likely to be accessed by children to assess and mitigate risks to minors, conduct Data Protection Impact Assessments (DPIAs), and minimize personal data collection. Although parts of the law have been enjoined, its enactment has influenced all DPIAs, consent management protocols, and Privacy by Design mechanisms.

Enforcement under these design codes will largely depend on investigatory powers and prosecutorial discretion. Maryland's Age-Appropriate Design Code Act (the Kids Code), for instance, bans the use of geolocation data and manipulative features (e.g., autoplay, endless scroll) for children, and empowers the State's consumer protection division to initiate investigations. However, enforcement of the Maryland Kids Code remains stalled due to ongoing litigation in *NetChoice vs. Gruhn*, which alleges the law's requirements, including conducting DPIAs, violate the First Amendment.

Further, even if enforcement were to proceed at the State level, the absence of a federal law preempting State law indicates enforcement across states will vary in frequency and approach. Yet, the common trend is unmistakable: State regulators are taking a front-line role in defining and policing child-centric privacy standards.

Restrictions on harmful content and liability exposure

A parallel trend is the enactment of laws requiring platforms to verify users' ages before granting access to adult or harmful content. As of 2025, 19 states have adopted such statutes. These laws impose civil liability on platforms that fail to implement 'commercially reasonable' verification procedures.

Texas' HB 1181 - currently under review by the U.S. Supreme Court in *Free Speech Coalition, Inc. v. Paxton* - may become a landmark case for determining the constitutional limits of content-based regulation involving minors. If upheld, the decision could open the door for more aggressive state enforcement strategies targeting not just adult content but a broader range of online harms.

Federal enforcement: Modernizing COPPA

Revisions to the Children's Online Privacy Protection Rule

Recognizing the evolving threat landscape, the FTC finalized significant amendments to the Children's Online Privacy Protection Rule in January 2025. These updates modernize COPPA's core definitions and compliance obligations to address biometric data, AI-powered systems, and platforms serving both child and adult audiences.

Key changes include:

- expanded definition of personal information: COPPA now includes biometric identifiers such as facial recognition, voiceprints, and genetic data, reflecting a broader understanding of how children's identities can be exploited by emerging technologies;
- mixed audience requirements: Platforms must implement neutral age screens and are prohibited from encouraging falsification of age, closing a major loophole that previously allowed platforms to avoid COPPA by claiming not to be 'directed to children;'
- parental consent mechanisms: The rule introduces stricter standards for verifying parental consent, including multi-step authentication, mail-in forms, and voice verification methods; and
- Safe Harbor reforms: The FTC tightened requirements for COPPA Safe Harbor programs, emphasizing transparency, independence, and reduced conflicts of interest, and these reforms aim to restore public confidence in self-regulatory compliance programs.

These changes expand the FTC's enforcement toolkit and bring COPPA closer to parity with international frameworks like the EU General Data Protection Regulation (GDPR), while retaining its core US principles of notice, consent, and limited data collection.

Enforcement actions and penalties

Over the last several years, the FTC has also demonstrated renewed commitment to enforcing children's privacy rules through high-profile settlements under COPPA.

- In January 2025, the FTC settled with a video game developer for alleged violations of COPPA. The FTC alleged that the company deceived children and other users about the real costs of in-game transactions and the odds of obtaining rare prizes. Under the terms of the settlement, the company agreed to pay $20 million and to block children under 16 from making in-game purchases without parental consent.
- In July 2024, the FTC and the State of California alleged that a technology company participated in deceptive and unfair practices in violation of federal and state law (including COPPA) in

the development, design, marketing, distribution, sale, and operation of their anonymous messaging app. The complaint alleges that the company not only actively marketed its service to children and teens, but that it also falsely claimed that its AI content moderation program filtered out cyberbullying and other harmful messages. It also alleges that the defendants sent fake messages that appeared to come from real people and tricked users into signing up for their paid subscription by falsely promising that doing so would reveal the identity of the senders of messages. To settle, the company agreed to pay $5 million and is banned from offering its app to anyone under the age of 18.

- In January 2024, the FTC secured a $275 million penalty for COPPA violations by a major online gaming company, including unauthorized data collection and inadequate parental consent mechanisms. The settlement also imposed comprehensive data governance reforms.
- In June 2023, a technology company from Washington agreed to pay $20 million to settle FTC charges that it violated COPPA by collecting personal information from children who signed up for one of its gaming systems without notifying their parents or obtaining their parents' consent, and then by illegally retaining children's personal information. As part of the settlement, the company was required to strengthen its privacy protections for child users of its gaming system.
- Less than a week earlier, in a separate 2023 action, the FTC fined an e-commerce company $20 million for allowing unauthorized in-app purchases by children, reinforcing the agency's position that user interface design choices can amount to deceptive practices when they exploit minors' lack of understanding.

These enforcement actions signal that monetary fines will be paired with mandated operational reforms, including independent audits, data deletion requirements, and the implementation of child-specific controls. The FTC's strategy reflects an effort to shift from reactive enforcement to proactive structural change.

The rise of state AGs in enforcement

Perhaps the most consequential enforcement trend in children's privacy law is the emergence of state AGs as pivotal enforcers.[1] No longer content to rely solely on federal regulators, states are pursuing independent investigations and lawsuits grounded in both newly enacted statutes and general consumer protection laws.

State-level enforcement examples

- On April 29, 2025, the Michigan AG filed a lawsuit against a technology company from California, alleging that it collects and processes, and allows third parties to collect and process, children's personal information, including voice recordings, location data, IP addresses, and browsing histories, in violation of COPPA. It also alleges that the company monetizes children's personal information to increase its advertising revenue and to make its platform more attractive to content providers and advertisers. Finally, the complaint asserts that the company misleads parents about its collection of their children's personal information and creates confusion about parents' rights to protect such information.
- On March 7, 2025, New York AG Letitia James reached a settlement with a software company from New York for $650,000 to resolve alleged privacy violations involving their social networking app geared towards high school students. The complaint alleged that the company represented that it would verify users' school email credentials to ensure that the app did not allow non-students to join, and only users from the same school could interact with each other on the app. However, the NY AG determined that the company stopped authenticating email credentials, allowing users from different high schools to message each other and non-students to access almost all app features. The AG alleged that the company's practices amounted to fraudulent and deceptive trade practices in violation of New York Executive Law §63(12), the New York General Business Law, and Section 5 of the FTC Act.
- In December 2024, Texas AG Ken Paxton launched investigations under the Securing Children Online through Parental Empowerment (SCOPE) Act into into companies deploying AI chatbots that interact with minors, citing risks of emotional manipulation and data misuse.
- California AG Rob Bonta reached a $500,000 settlement with a games publisher company from New York for COPPA and CCPA violations related to their collection and sharing of children's personal information without parental consent in one of their mobile app games. The California AG's office determined that the company's age verification methods failed to encourage users to enter their age accurately and simply defaulted to older ages, that it misconfigured third-party software development that did not limit the collection, disclosure, and use of personal data based on age or consent, and that its advertising was deceptive and unlawfully targeted minors. In addition to the monetary fine, the company was subject to injunctive terms to ensure legal data collection and disclosure and diligence in configuring third-party software in their mobile games.
- In New Mexico, AG Raul Torrez filed a lawsuit against a social media company from California on September 5, 2024, to protect children from sextortion, sexual exploitation, and harm. In the lawsuit, the New Mexico Department of Justice (DOJ) alleged that the company's policies, seemingly ephemeral content, and recommendation algorithm foster the sharing of child sexual abuse material and facilitate child sexual exploitation. The New Mexico DOJ also alleged that the company's executives have misled the public about the platform's safety with ads declaring that the platform is 'more private' and 'less permanent' than other social media platforms.

While enforcement challenges persist, these enforcement powers are not merely symbolic. In the aggregate, they introduce a decentralized, multi-jurisdictional compliance risk for companies operating nationally. Businesses that once relied on harmonized federal standards must now navigate a fragmented enforcement landscape where failure to comply with one state's rule may trigger broader scrutiny.

Conclusion

Children's privacy law in the United States is undergoing continuous evolution driven by new state statutes, federal rulemaking, and unprecedented enforcement momentum. The convergence of legislative focus on protecting children, regulatory updates, and heightened litigation risk requires digital platforms to reassess how they engage with young users.

While federal amendments to COPPA provide a renewed baseline for compliance, the true frontier of enforcement lies in state-level action and the application of privacy principles to emerging technologies like AI and biometrics. Companies operating in the youth digital market must now contend with a patchwork of substantive obligations, increasing enforcement risks, and a rising expectation for transparency, consent, and Privacy by Design.

Above all, the evolving regulatory landscape signals a clear policy direction: Safeguarding children's digital lives is no longer optional; it is a legal imperative.

[1] It should be noted that on March 7, 2024, a bipartisan coalition of 43 state AGs sent a 19-page letter to the FTC with detailed comments on the FTC's January 2024 Notice of Proposed Rulemaking. Although the FTC published the Final Rule updating COPPA on April 22, 2025, making the updates effective on June 23, 2025 (with a compliance date of April 22, 2026), the detail in this letter certainly highlights the thinking of 43 state AGs who have taken an active role in the enforcement of COPPA and may be helpful to entities trying to navigate state-level enforcement efforts.