Children’s Online Privacy and Safety: State Laws, Age-Appropriate Design, and Emerging Compliance Trends Beyond COPPA

Laura Riposo VanDruff, Alysa Z. Hutnik

November 4, 2025

Regulators are intensifying efforts to address the complex challenges of protecting children’s privacy and safety in an increasingly digital world. As experts warn of the psychological and developmental risks of growing up “terminally online,” policymakers are grappling with an online ecosystem where companion chatbots, social media, and gaming platforms are part of children’s daily lives. At the same time, emerging technologies that can estimate a user’s age are reshaping expectations of what responsible design looks like. As a result, the policy debate is expanding beyond the decades-old COPPA framework, signaling a broader rethinking of how the law should protect children in an increasingly interconnected world.

How States are Extending Protections Beyond Age 13

Since 2000, the federal Children’s Online Privacy Protection Act ("COPPA") has restricted the collection and use of certain personal information collected from children under the age of 13. Impatient with Congress’s failure to update the law, a bipartisan mix of states has taken steps to add protections for teens, principally by requiring a teen to opt-in to the sale of their information or receive targeted advertising, or to ban use of teen information for profiling. Comprehensive state laws vary, requiring companies to navigate a patchwork of compliance obligations and make strategic decisions about implementation, including whether a state-by-state approach online is even viable.

Age-Appropriate Design Codes

California reshaped the conversation in 2022 with its Age-Appropriate Design Code (“CA AADC”), modeled after the UK’s approach. Although federal courts have twice enjoined enforcement of the CA AADC, other states—including Maryland, Connecticut, Nebraska, and Vermont—are pressing forward. These laws share a common goal: requiring businesses with digital offerings to prioritize children’s interests and reduce online harms through thoughtful design.

New Social Media Requirements

States next targeted social media platforms directly. New laws in Florida, Georgia, Louisiana, Mississippi, Nebraska, Tennessee, and Utah would restrict minors’ access to social media accounts,

including by mandating the collection of age information and requiring parental consent for minors to open or maintain a social media account. While these laws face a wave of litigation that will take years to fully resolve, other states, including California, Colorado, and Minnesota are tackling concerns regarding social media with prominent warnings.

California's Digital Age Assurance Act

California's new Digital Age Assurance Act ("DAAA"), signed on October 13th, marks a significant shift. As we describe here, it puts responsibility on operating system developers to collect age information and generate an "age signal" that app developers must then honor. Unlike earlier efforts, including in Utah and Texas where the states' laws include a private right of action, the DAAA garnered support from major tech players like Google and Meta. Instead of other laws' more rigid age verification and parental consent frameworks, the California model requires operating systems to provide developers with a device user's age range based solely on information provided by the account holder. Developers, in turn, must treat the age signal as the "primary indicator" of a user's age unless there is "clear and convincing" information that the user's age is different. Critically, the DAAA shifts primary compliance obligations from operating systems to app developers, giving developers actual knowledge of the user's age and thereby triggering state-law privacy and COPPA obligations.

Congress

In Congress, the House Energy and Commerce Committee is reportedly finalizing a package of bills that would address children's privacy and safety. The Committee may hold a hearing in the weeks ahead, with negotiations in the Senate to follow. Whether Congress, which is mired in the politics of the government shutdown, delivers a unified framework or adds complexity to an already fragmented landscape remains to be seen. Resolution during this legislative session seems increasingly unlikely.

Litigation

Children's safety is also the focus of court challenges. Roblox is facing a wave of lawsuits from families and state attorneys general—including in Kentucky and Louisiana—alleging that although the company led parents to believe the platform was safe, its design allegedly made children vulnerable to abuse. Roku is similarly being sued by attorneys general in Florida and Michigan for improperly collecting and sharing children's personal information and facilitating access to inappropriate content.

Privacy Regulators

Global regulators recently announced that they are joining forces, including with the California Privacy Protection Agency, to scrutinize how companies protect children online, underscoring just how urgent this issue has become. The Attorney General Alliance also recently launched its "Partnership for Youth Online Safety," an initiative of state attorneys general, industry participants, civil society, families, and academic stakeholders. The Partnership's aim is to identify practical, design based safeguards for children's online safety, establish rapid information sharing frameworks between platforms and law enforcement, and promote greater parental awareness through education and tools. Together, these efforts signal a redoubling of regulators' commitment to protecting children's privacy and safety online.

Compliance Takeaways

- Stay current – State and federal rules for children’s privacy and safety are evolving quickly. To stay ahead of the curve, companies should track both new legislation and ongoing litigation, regularly reassessing existing practices to determine whether current policies, procedures, and assumptions align with emerging obligations and risk.
- Leverage technology – Age signals, parental controls, and safety-by-design features are increasingly expected, and new legal requirements will phase in over the near- and long-term.
- Coordinate across platforms – Compliance requires alignment among operating systems, platforms, and apps to ensure consistent protection for minors.