Cooley

Comprehensive Online Safety Legislation Comes to the US: How KOSA is Copying UK, EU and Australian Laws

March 5, 2026

The proposed Kids Online Safety Act (KOSA) is the most significant attempt to overhaul federal online child safety laws since the passage of the Children's Online Privacy Protection Act in 1998. If passed in any of the forms currently contemplated, KOSA would impose new requirements on tech companies and amplify an already significant global regulatory risk landscape.

KOSA is still being debated, with the Senate and House disagreeing on important aspects. Both the Senate (S.1748) and House (H.R. 6484) bills aim to protect online users under 17 from harmful design features. The Senate bill imposes a "duty of care" on platforms to prevent harms, including "compulsive usage," eating disorders and other mental health harms, whereas the House bill requires "reasonable policies, practices, and procedures" to address more limited harms. On February 10, 2026, a coalition of 40 state and territorial attorneys general sent a letter urging passage of the Senate bill over the House version.

The analysis below focuses on the Senate bill, which would present a greater sea change in how online safety is regulated in the United States.

Cross-border convergence: Where S.1748 borrows from the European Union, UK and Australia

Over the last few years, many tech companies have invested significant resources building toward compliance with the EU's Digital Services Act (EU DSA), the UK's Online Safety Act (UK OSA) and Australia's Online Safety Act (AU OSA). Companies that have invested in such compliance programs will take some relief in key similarities:

User reporting

S.1748 requires covered platforms to provide a "readily accessible and easy-to-use means" for users and visitors to report harms to a minor. Platforms must confirm receipt of the report and provide a response within specific time frames. This closely tracks the UK OSA notice and takedown requirements, which require swift processing.

Safety and privacy by default

S.1748 would require platforms to provide "readily accessible and easy-to-use safeguards" that are turned on by default for minors, including preventing communication from strangers, limiting "compulsive usage" features (e.g., auto play and infinite scroll) and restricting geolocation data. Article 28 of the EU DSA requires "a high level of privacy, safety, and security of minors" and prohibits platforms from targeting advertisements to minors using profiling. The more granular prescriptions in S.1748 track many of the European Commission's Guidelines on Article 28. Child Safety Codes issued under the UK OSA and Industry Codes issued under the AU OSA likewise impose similar default setting requirements.

Parental tools

S.1748 mandates that platforms provide "readily accessible and easy-to-use parental tools" that allow parents to manage a minor's privacy and account settings. These tools must also include the ability to restrict purchases and financial transactions, as well as view and restrict the total time the minor spends on the platform. For users

the platform knows or should know are minors, these tools must be enabled by default. These requirements are broadly similar to the EU DSA Article 28 Guidelines, which recommend similar measures, recognizing KOSA would make them mandatory.

Algorithmic opt out

S.1748 requires platforms to provide a "prominently displayed" option for minors to opt out of personalized recommendation systems. Article 38 of the EU DSA contains the closest parallel, but the European requirement is less prescriptive – it requires very large services to provide an option for their recommender systems that is not based on profiling, which often results in a chronological or popular community feed.

Mandatory reporting and transparency audits

Across these jurisdictions, transparency is a core pillar. S.1748 would require platforms to publish, at least annually, transparency reports based on independent, third-party audits. Similarly, the EU DSA requires independent audits, systemic risk assessments and publication of transparency reports. The UK OSA requires platforms to send annual transparency reports to the UK regulator. Both the UK and Australia authorize their regulators to demand information from platforms regarding their safety systems. The independent audit requirement under the DSA has been criticized for its cost and burden, and it remains subject to focused pushback in S.1748.

US exceptions: What stands out in S.1748

There are several important ways S.1748 differs from its international counterparts – reflecting both the US legal environment and a focus on regulating platform design over restrictions on content.

Constitutional limits

S.1748 focuses on platform design – likely to avoid content-based restrictions that may violate the First Amendment. It clarifies that KOSA would not require platforms to restrict a minor from "deliberately and independently searching for … content." Additionally, the bill explicitly prohibits regulators from enforcing KOSA based on users' viewpoints. In contrast, the UK OSA and EU DSA more directly regulate harmful content, including "content that is harmful to children" (UK) and content that poses "systemic risks" (EU).

Duty of care

S.1748 would impose a duty on platforms to exercise "reasonable care" in the design of features to prevent foreseeable harms. At a high level, this parallels duties of care under the UK OSA to, among other things, take "proportionate measures" to mitigate and manage harm to children online and the DSA Article 35 obligation to "put in place reasonable, proportionate and effective mitigation measures" to mitigate systemic risks from their services. However, the KOSA duty is more focused on the design process, rather than directly regulating the speech outcome, likely reflecting at least in part First Amendment concerns with the latter approach. Specifically, the UK OSA mentions duties related to "illegal content" and "content that is harmful to children," and the EU DSA identifies "illegal content" as a systemic risk, while the KOSA duty makes no mention of content and instead focuses on preventing and mitigating specific harms caused by "any design feature."

Age verification

While Australia recently introduced laws to ban social media for those under 16 and require age verification, and the EU, UK and other countries are considering similar moves, S.1748 explicitly rejects mandatory collection of age data. Instead, S.1748 relies on a "knowledge" standard, imposing requirements if a platform knows or should know a user is a minor. This knowledge standard will raise a particular challenge for platforms that have deployed age assurance systems, but it will not necessarily require those who have not deployed age assurance systems to do so.

FTC enforcement risk

Enforcement risk under KOSA also stands out. S.1748 would authorize the Federal Trade Commission (FTC)

and state attorneys general to enforce the law. The FTC is empowered to impose civil penalties of more than $50,000 per violation of KOSA. Simultaneously, state attorneys general may initiate civil actions regarding violations of KOSA's safeguards, disclosure and transparency provisions. This creates a fragmented enforcement landscape that platforms must navigate alongside more centralized regulatory models in the UK, EU and Australia.

Takeaways

If passed, KOSA will increase the complexity of the online safety regulatory landscape and give new tools to a set of motivated regulators. In assessing positions to take on KOSA, tech companies should consider what work they have already done to meet UK OSA, AU OSA and the EU DSA – and consider where existing approaches should be revised to account for US-specific requirements and enforcement risks.

Our cross-functional team of tech regulatory and enforcement practitioners leverages deep, hands-on experience guiding tech companies through complex global frameworks – like the EU DSA, UK OSA and AU OSA – as well as navigating online safety inquiries from the FTC and state attorneys general. We are uniquely positioned to help platforms design trust and safety strategies to meet KOSA's specific requirements, holistically assess risks and mitigations, and proactively prepare for emerging US enforcement interest.

Read our latest FTC update: Learn more about the FTC's recent policy statement announcing that it will exercise enforcement discretion under the Children's Online Privacy Protection Act to facilitate broader adoption of age verification technologies.

Key Contacts

Janet H. Kim Washington, DC	janetkim@cooley.com +1 202 728 7060
Sean Quinn New York	squinn@cooley.com +1 202 728 7075
Tristan Lockwood London	tlockwood@cooley.com +44 20 7556 4115

Adam Silow New York	asilow@cooley.com +1 212 479 6163