

# Congress and State Legislatures Proposing Youth-Focused Privacy Laws

February 2022

*Privacy In Focus®*

Legislators in Washington, DC, and in multiple states have rolled out proposals focused on children's and teens' privacy that would significantly affect companies that provide online applications and services. At the federal level, on February 16, 2022, Sens. Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN), respectively the Chair and Ranking Member of the Senate Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Data Security, introduced the Kids Online Safety Act, which would impose significant new requirements on companies that provide internet services used by children. At the state level, legislators in California and Washington have introduced bills that would require companies to treat minor users differently than adults for privacy compliance purposes.

If enacted, these bills would have a significant impact on companies. For example, the proposed federal law would require significant engineering and policy changes for applications and online services. Both the federal and California proposals would establish a duty for companies to act "in the best interest" of children using their products—a standard with uncertain application to the digital economy.

Below, we summarize the key elements of these proposals, which companies should continue to monitor.

## The Kids Online Safety Act

## Authors

Duane C. Pozza  
Partner  
202.719.4533  
dpozza@wiley.law

Kathleen E. Scott  
Partner  
202.719.7577  
kscott@wiley.law

Joshua K. Waldman  
Associate  
202.719.3223  
jwaldman@wiley.law

## Practice Areas

Cyber and Privacy Investigations, Incidents  
& Enforcement  
Privacy, Cyber & Data Governance

The bill recently introduced by Senators Blumenthal and Blackburn—S. 3663, the Kids Online Safety Act—is notably presented as a child safety measure, not a privacy bill, apparently to set the bill apart from the myriad of other privacy and social media-focused legislation under consideration. The senators introduced the bill after months of public discussion, including holding five subcommittee hearings with major social media companies between September and December 2021. Other Senate Commerce subcommittees have also recently addressed these issues, most recently in a December 9, 2021 hearing of the Communications, Media, and Broadband subcommittee focusing on algorithms.

The proposal is broad in scope and could encompass a wide range of internet services that could be used by children. It defines a “covered platform” as any commercial software application or electronic service that connects to the internet and is used, or reasonably likely to be used, by anyone 16 years old or younger.

The bill proposes several requirements on covered platforms. For example, it would create a “duty of care” for covered platforms to act “in the best interests of a minor” consumer and prevent or mitigate specific potential harms, including the physical or mental health of minors (such as self-harm, suicide, eating disorders, and substance abuse), online bullying or harassment, sexual exploitation, selling or promoting substances or activities that are illegal for children, predatory, unfair, or deceptive advertising or marketing practices, and patterns that indicate or encourage addiction-like behavior.

Beyond the duty of care, the bill would require covered platforms to implement privacy and data controls that allow parents and minor users to manage how information about minor users is collected and shared, limit certain features that increase user engagement (such as autoplay or notifications), and let users opt out of algorithmic recommendations. These requirements include mandatory parental controls that would let a parent track the child’s time spent on the platform, restrict purchases, and make complaints to the platform.

Covered platforms would also be subject to additional disclosure and transparency requirements, including an annual public report that would summarize company user data along with results from an independent third-party audit addressing the potential harms specified in the bill, and the company’s prevention and mitigation efforts.

Finally, under the proposal, the U.S. Department of Commerce would manage a new program to enable researchers to obtain data from covered platforms to conduct public-interest research. The Federal Trade Commission and state attorneys general would have enforcement authority for the proposed law.

### **State Legislative Proposals**

States are also keying in on children’s and teen’s privacy issues. In particular, the California Age-Appropriate Design Code Act (Assembly Bill 2273), introduced February 16, 2022, addresses digital products and services used by children under the age of 18, but takes a somewhat different approach than the federal bill. Like the federal proposal, the California bill would apply to all businesses that provide a good, service, or product feature likely to be accessed by children. But rather than designating a list of mandatory privacy or data controls for such services, A.B. 2273 would set the “best interests of children” as the standard for designing, developing, and providing the service, and require companies to prioritize the privacy, safety, and well-being

of children over “commercial interests.”

However, some features of A.B. 2273 are similar to elements of the Blumenthal-Blackburn bill, including requiring strict privacy settings by default for children users, and mandating that terms-of-service and privacy policies use age-appropriate language, although neither the federal nor the California bill provide detailed guidance regarding how to determine the respective age-appropriate standards. Products must display an “obvious signal” to minor users when enabling a parent, guardian, or any other consumer to monitor their online activity or track their location. The California proposal also would require companies to develop a data protection impact assessment, conduct an assessment of the age of the company’s consumers, and only disclose user or location data for children when there is a “compelling reason” that the disclosure is in the best interests of the child.

The legislation would also forbid companies from using a child’s personal information (adopting the definition used in the California Consumer Privacy Act) in a way that is “demonstrably harmful” to physical or mental health or well-being. The bill assigns the California Privacy Protection Agency to establish a task force to evaluate best practices and help small- and medium-sized businesses comply with the law.

In Washington State, Senator Reuven Carlyle and four co-sponsors introduced a bill that addresses several privacy and data protection matters, which includes provisions specifying collection and security practices for data from children and adolescent users. The bill identifies adolescents (ages 13 through 17) as a class separate from other children under 18, and has three main provisions: establishing consumer rights regarding data about children and adolescents, requiring consent for use of that data, and mandating a set of duties for businesses that collect and process that data.

Of note, the bill would establish a right for an adolescent or the parent of an adolescent or child to access, correct, or delete personal data that a business holds. It would also extend this protection to current adults for data collected about them when they were minors. The proposal also would require consent from parents of children, or the adolescents themselves, to collect and process personal data, and further would require a separate and express consent from an adolescent to sell their personal data or conduct targeting advertising. Finally, the bill would require businesses to conduct a data protection assessment, be transparent about collection and processing practices, secure personal data, and minimize data collection and retention.

\*\*\*

Wiley’s Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws, and advocate before government agencies. Please reach out to any of the authors with questions.

© 2022 Wiley Rein LLP