Bloomberg Law

Photographer: Matt Cardy/Getty Images

November 18, 2024

Laws to Keep Kids Safe Online Are Causing Legal Entanglements

Lindsey Tonsager
Covington

Priya Leeds
Covington

- *Covington attorneys describe states' online privacy law issues*
- *Companies should update privacy notices, monitor court rulings*

A flurry of state laws related to children's online privacy largely breaks down into two categories: age-appropriate design codes with requirements for online services targeting minors, and laws that govern the nature and terms of minor access to social media.

The focus and nature of these laws have shifted in the two years since California became the first state to adopt age-appropriate design codes. Some trends have emerged in states, including:

- Statutes requiring parental consent for minor access to social media and age assurance requirements have been found unconstitutional
- Recent laws have imposed duties of care on regulated companies
- Certain laws have imposed additional requirements on social media companies

Companies seeking to comply with these laws should understand the instances where they collect personal information from children and how such information is used. They should update their privacy notices to be readable by minors, reconfigure privacy defaults to provide high levels of privacy for younger users, collect information only as disclosed to provide their services, and delete that information once it's no longer needed.

For certain other requirements, such as parental consent for social media use and age assurance, companies should monitor whether the courts continue to find such requirements unconstitutional.

Several states have passed laws requiring parental consent for teens to use social media. Florida requires 14- and 15-year-olds to obtain parental consent and prohibits children younger than 14 from creating accounts.

Many states take the requirement even further. Ohio, Georgia, and Louisiana require parental consent for older teens, while Tennessee, Arkansas, and Mississippi mandate parental consent for all minors. New York has a similar provision, requiring parental consent for an "addictive feed" to minors.

However, Ohio's law requiring parental consent for minors' social media use was found to violate the First Amendment. The US District Court for the Southern District of Ohio said in February that it targeted speech on social media platforms based on content, speaker, and viewpoint and burdened both adults' and minors' access to speech.

A court enjoined a similar law in Mississippi on First Amendment grounds, finding that the law regulated content and was likely to fail strict scrutiny because it wasn't "remotely tailored" to the goal of protecting children from online harms.

The proliferation of these laws is also in tension with other state laws that recognized circumstances where the privacy of teens should outweigh parental oversight. While Maryland's law permits companies to allow parents to track their minor child's location without providing an obvious signal to the minor, California law requires services to notify minors when a parent is doing so.

Courts also have struck down numerous laws containing age assurance requirements. An Arkansas law requiring social media companies to conduct age verification was preliminarily enjoined on First Amendment grounds when a

court found it "likely that many adults who otherwise would be interested in becoming account holders on regulated social media platforms will be deterred—and their speech chilled—as a result of the age-verification requirements."

The court cited the submission of official government documentation and biometric scans as methods to verify age that would unconstitutionally burden speech. Similarly, Utah had required social media companies to implement "an age assurance system" with an accuracy rate of at least 95% to determine whether a user was a minor. The law was enjoined before it could take effect.

Some state laws impose a duty of care on companies that handle personal information. California requires bars minors' personal information from being used in a way that a company knows, or has reason to know, would be materially detrimental to minors' physical or mental health or well-being.

By contrast, Maryland requires that regulated companies ensure the best interests of children when designing their products, and that they process data consistently with those interests. Maryland's law specifies that products designed in the best interests of children must not benefit the company to the detriment of minors and can't cause material or severe physical, financial, psychological, or emotional harm.

A bill in Vermont, which was vetoed in June, had stated that regulated companies have a minimum duty of care to minors, meaning they shouldn't use personal data in a way that benefits the company to the detriment of minors or in a way that would cause reasonably foreseeable emotional distress or excessive use of the service.

Both the Maryland and Vermont measures eliminated the knowledge requirements and materiality threshold present in California law. It is unclear how these ambiguous standards will be interpreted and applied in Maryland.

Certain laws contain additional obligations on social media companies. Georgia requires companies provide parents with a list of the service's content moderation features. Utah mandates companies to disable autoplay and infinite scroll for minors.

California directs companies to limit minors' ability to access an "addictive" feed to one hour per day by default. The state also requires companies to allow parents to set their child's default feed to a non-personalized feed and limit their

child's ability to view the number of likes or other forms of feedback to their content.

If this trend continues, we may observe a rise in state-by-state compliance approaches as companies grapple with increasingly burdensome state-specific requirements.

(Updates Nov. 18 article to correct status of Vermont measure in 17th paragraph.)

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Lindsey Tonsager is partner at Covington and co-chairs the global data privacy and cybersecurity practice.

Priya Leeds is an associate at Covington and a member of the privacy and cybersecurity practice group.