Hashed & Salted | A Privacy and Data Security Update
August 2023

A Roundup of State Laws Related to Children's Privacy

Key Takeaways

- States are not just concerned about the collection of information. They also are focused on the emotional and mental harm the collection or use of the information may cause.
- The regulation of personal information such as precise geolocation information and biometric information will be more closely watched and regulated.
- States are expanding the definition of "child" to include children under the age of 16 or 18.
- States are not only focused on websites that are directed to children. They now are broadening their scope to general audience sites that are collecting information from a "known child" (under general privacy laws), social media sites (even if they are not directed toward children) and sites that are likely to be accessed by children. Under these definitions, even sites that are directed toward adults will have to be concerned with children's privacy.

For a wide variety of entities — from the Biden administration and the Federal Trade Commission (FTC) to state attorneys general and advocates — protecting children's privacy has been a top priority in the past two years. While the issues that arise from children's online activities aren't limited to privacy, the potential misuse of children's personal information has put children's digital rights in the spotlight. As we look at the legislative landscape, it is evident that the forefront of action lies not at the federal level, but within individual states. While Congress has not yet passed an update to the Children's Online Privacy Protection Act (COPPA) or any other federal privacy law, a patchwork of state-level initiatives has emerged, each attempting to fill the regulatory void and provide safeguards for children.

We are seeing states pass either laws specifically focused on children's privacy or comprehensive privacy laws that incorporate special protections for children. Both types of laws will have a significant impact on how businesses collect and use information not only from children under the age of 13 (who are already protected by COPPA) but also from minors under the age of 18. Below is a summary of these laws.

California Privacy Rights Act. One of the first state laws to address children's privacy was the California Consumer Privacy Act (CCPA), which has been updated by the California Privacy Rights Act (CPRA). Both laws are general privacy laws that include special protections for children in California. Under the CPRA, a business cannot sell or share the personal information of a child aged 13 to 15 without the affirmative consent of the child, and for a child under the age of 13, without the affirmative consent of the child's parent or guardian.

Does your business have to comply with the CPRA?

Only businesses that meet one of the following thresholds must comply with the CPRA: (1) make annual revenues of more than $25 million, (2) collect personal information

Attorney Advertising

from more than 100,000 consumers or households, or (3) generate at least half of its revenues from selling or sharing California personal information.

California Age-Appropriate Design Code. California was not only the first state to pass general privacy legislation, but it was also the first state to pass legislation specifically focused on children's privacy. The California Age-Appropriate Design Code (CAADC) becomes effective on July 1, 2024. For a full discussion of the CAADC, read our client alert. Some highlights of the CAADC include:

- The act expands the definition of "children." Unlike COPPA, which applies to children under the age of 13, the CAADC applies to minors under the age of 18.
- The scope of the CAADC is broader than COPPA. COPPA only applies to online services that are directed to children or when the service providers have actual knowledge that children are using the online service. The CAADC applies to a business (as defined by the CPRA) that is "likely to be accessed" by minors. This includes online services that are routinely accessed by a significant number of children or are similar to online services that are routinely accessed by a significant number of children.
- Data Protection Impact Assessments. The act requires businesses to conduct Data Protection Impact Assessments (DPIA) to analyze whether the service will harm children, including by exposing children to harmful or potentially harmful content or contacts. "Harmful" and "potentially harmful" are not defined by the CAADC, and we are still awaiting guidance from the California Attorney General on their definitions.
- The act requires businesses to have an age estimation requirement. For online products and services likely to be accessed by children, a business must be able to estimate the age of child users with a reasonable level of certainty appropriate to, and a level of assurance proportionate to, the risks that arise from the data management practices of the business. If the business is unable to reasonably estimate the age of child users, the business must apply the privacy and data protections afforded to children to all users. Because treating all users as children may significantly hamper the ability of users to access the online product or services and the ability of the online product or service to collect information, this requirement essentially may mean businesses must implement some form of age verification or age gate for all end users.
- The act strictly regulates the collection and use of geolocation information. The collection, sharing or selling of precise geolocation information by default is prohibited unless it is "strictly necessary" and only for a limited time. In addition, the CAADC requires businesses to provide an "obvious signal" to the child when the child's activity or location is being tracked by a third party (i.e., parent or guardian).
- The act prohibits the use of dark patterns. Under the CAADC, businesses cannot use dark patterns or other techniques to (1) encourage children to provide additional personal information beyond what is reasonably expected for the online product or service; (2) forgo privacy protection measures; or (3) take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health or well-being.

Does your business have to comply with the CAADC? If you answer yes to any of the questions below, then your business may be covered by the CAADC.

1. Is your company considered a business under the CPRA's threshold requirements?
2. Is the online service one that minors would like to participate in or would be attractive to minors? To determine whether an online service is attractive to minors, review the content of the online service, third-party information such as news articles or market research, and advertisements for the online service. Remember that "minors" is now anyone under age 18, which may mean that general news and entertainment sites may fall within scope.
3. Is your activity or program accessed by a significant number of minors (i.e., more than a small or insignificant number of minors use the service)? To determine whether an online service is accessed by a significant number of minors, review internal analytics or the analytics of similar online services.

State laws limiting minors' access to social media. Several states have passed laws limiting the access of minors under the age of 18 to social media. The most aggressive of these laws is Florida's. The Florida law,

which goes into effect on July 1, 2024, applies not only to social media companies but also to "online platforms," which are defined to include online games and online gaming platforms. Similar to the other laws limiting children's access to social media, Florida's law applies to all minors under the age of 18, not just children under the age of 13, and all online platforms that are "predominantly" accessed by minors. While the law does not prohibit the use of social media by minors, it prohibits online platforms from processing (which includes collecting) a minor's personal information if it may result in substantial harm or privacy risk to a minor; profiling minors (except under limited circumstances); and collecting, selling or sharing any precise geolocation data of a child unless it is strictly necessary for the online platform to provide the service. In addition, the Florida law borrows two concepts from the CAADC – it prohibits (1) the use of dark patterns to encourage minors to provide personal information and (2) the collection of precise geolocation information of a minor without an obvious sign to the child for the duration of the collection that collection is taking place. Most important, as compared to the other laws limiting minors' access to social media, the Florida law does not have an exception to the prohibition if a parent or guardian consents; the Florida law is a blanket prohibition on this type of collection and use of minors' information.

Arkansas, Utah and Louisiana also have adopted laws limiting minors' access to social media, effective Sept. 1, 2023, March 1, 2024, and July 1, 2024 respectively. Under these laws, minors cannot have a social media account without the express consent of their parent or guardian. The Utah law also prohibits minors from accessing social media between the hours of 10:30 p.m. and 6:30 a.m., unless a parent allows the child to access it during these times, and limits the collection and use of minors' information. Unlike many other privacy laws, the Arkansas and Utah laws also include a private right of action if children are harmed due to violation of these laws. The Louisiana law gives the Louisiana Department of Justice exclusive authority to administer and enforce the law.

Finally, Texas recently passed a children's privacy law directed at social media (effective July 1, 2024). Unlike the Louisiana, Utah, and Arkansas laws, the Texas law does not require verifiable parental consent for a child to have a social media account. Instead, the Texas law requires parental consent for specific collections and uses of a minor's information. The Texas law also requires digital service providers to develop a strategy to prevent a minor's exposure to harmful material and create tools to allow parents to control a minor's privacy and account settings and to monitor and limit a child's use of social media, and it limits targeted advertising through the social media platform.

Does your business have to comply with the state laws limiting minors' access to social media?

1. Is your business a "social media service" according to the relevant state law's definition? Some of the laws, such as those in Louisiana, Utah and Arkansas, define "social media service" in terms not only of its functionality but also with respect to any membership or revenue thresholds. However, the Texas law does not have any such thresholds, and the Florida law is much broader, applying not only to social media platforms but also to online games and online gaming platforms.
2. All of these laws apply to children under the age of 18 and 16, which is a much broader standard than COPPA. The age verification requirements are also much stricter under these laws than under COPPA. For instance, Arkansas requires the social media company to use a third-party vendor to perform age verification, and Louisiana and Utah is still determining which age verification requirements will be acceptable.

General Privacy Laws. Multiple states have passed general privacy laws in the past year, all of which appear to have a standard method for addressing children's privacy. The following aspects are similar in all these laws:

- Definition of "personal information." The definition of "personal information" under these general privacy laws is broader than COPPA's definition. Under these laws, "personal information" is defined as information that is linked or reasonably linkable to an identified or identifiable person. Notably, under COPPA, personal information does not include information that is collected offline or from parents. The new state laws do not have this exception. Even if personal information is collected offline or from parents, it is covered under these state laws as long as it is linkable to an identifiable person.
- Definition of "sensitive information." The definition of "sensitive information" includes personal information from a known child. Therefore, any personal data collected from a known child would be considered sensitive.

- Treatment of "Sensitive Information" All of these states require companies to obtain consent from a parent or guardian before they can collect sensitive information from a known child.

Below is a chart of the states that have adopted general privacy laws, the effective date of these laws and any notable deviation of these laws as they relate to children's privacy.

State	Effective Date	Notable Deviations
Colorado	July 1, 2023	This law does not apply to personal information already covered by COPPA.
Connecticut	July 1, 2023	None
Florida	July 1, 2024	This law also applies to minors ages 13-18. Therefore, online service providers must obtain affirmative authorization from 13-18-year-olds or consent from their parents/guardians to process or sell their sensitive data.
Indiana	Jan. 1, 2026	Verifiable parental consent under COPPA complies with the law.
Iowa	Jan. 1, 2025	None
Montana	Oct. 1, 2024	Verifiable parental consent under COPPA complies with the law.
Tennessee	July 1, 2025	Verifiable parental consent under COPPA complies with the law.
Texas	July 1, 2024	Verifiable parental consent under COPPA complies with the law.
Utah	Dec. 31, 2023	Verifiable parental consent under COPPA complies with the law.
Virginia	Jan. 1, 2023	Verifiable parental consent under COPPA complies with the law.

Does your business have to comply with the general state privacy law requirements?

1. All the states have different thresholds for the businesses that must comply with their privacy laws. Many of these revolve around the number of users that reside in the state and the percentage of revenue that is derived from the processing of user data.
2. All these state general privacy acts have exclusions. Be sure to review the exclusions to see whether your business falls under one of them.

Related Professionals

Nerissa Coyle McGinn . . . . . nmcginn@loeb.com
Chanda Marlowe . . . . . cmarlowe@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

© 2023 Loeb & Loeb LLP. All rights reserved.

7380 REV1 08-23-2023