Privacy Alert

September 2022

California Children's Privacy and Online Safety Bill Becomes Law: What Does It Mean for Businesses?

General Summary

AB 2273, also known as the California Age-Appropriate Design Code Act (ADCA), was signed into law on September 15 and will become effective on July 1, 2024. The ADCA will impose new requirements and prohibitions on a broad range of businesses beyond those that are included in the Children's Online Privacy and Protection Act (COPPA), with the aim of better protecting children's privacy and online safety.

In brief, the ADCA, which is modeled after the U.K.'s Age Appropriate Design Code that came into force in September 2020, will require businesses to:

- Consider the "best interests" of children when designing, developing and providing an online product or service (note that the privacy, safety and well-being of children must be prioritized over commercial interests)
- Conduct detailed Data Protection Impact Assessments (DPIAs) for new or existing online products and services
- Configure default settings provided to a child to a "high level of privacy"
- Provide an obvious signal to the child when the child's activity or location is being monitored
- Provide privacy information, terms of service, policies and community standards in a concise, prominent and clear manner (using language suited to the age of children likely to access their services), along with prominent, accessible and responsive tools to help children, parents and guardians exercise their privacy rights and report concerns

The ADCA will prohibit businesses from:

- Using a child's personal information in a way that is materially detrimental to the health or well-being of a child
- Profiling a child by default (subject to limited exceptions)
- Collecting, selling, sharing or retaining any personal information that is not necessary to provide the online product or service with which a child is engaged
- Using personal information for any reason other than a reason for which that personal information was collected
- Collecting, selling or sharing precise geolocation information by default unless the collection of such information is strictly necessary for the business to provide the online product or service

The California Attorney General will have the authority to adopt regulations, which will likely be based on recommendations from child privacy experts who are members of the ADCA's newly established Children's Data Protection Working Group, and enforce the violations of the ADCA through civil penalties.

Attorney Advertising

Who Does the ADCA Apply To?

As written, the ADCA is very broad and could impact many general audience websites that would not otherwise be covered by COPPA. This is not only because the ADCA will raise the age for which children's privacy protections exist from under the age of 13 to under the age of 18 but also because the law is triggered when a "business" (as defined by the California Consumer Privacy Act (CCPA)) provides an online service that is "likely to be accessed" by minors. This can be distinguished from the current standard in the United States under COPPA, which is triggered by an online platform's collection of personal information from children. Under the ADCA, an online product or service will be considered "likely to be accessed" by children when it meets any of the following criteria:

- It is directed to children as defined by COPPA.
- It is routinely accessed by a significant number of children (based on reliable audience composition evidence).
- It is similar to or the same as an online product or service already determined to be routinely accessed by a significant number of children.
- It has advertisements marketed to children.
- It has design elements that are known to be of interest to children, including but not limited to games, cartoons, music and celebrities who appeal to children.
- It has an audience base made up of a significant number of children (based on internal company research).

There is some ambiguity surrounding what is meant by some of the indicators of whether an online service is "likely to be accessed" by children (listed above). For example, it is unclear how many children must access a site in order for the site to be considered "routinely accessed by a significant number of children," as the term "significant" is not defined under the ADCA. Depending on how the ADCA is interpreted, it would potentially apply to a wide range of online products, like video conferencing services, online games and social media sites that were previously thought to be geared toward a general audience if those products and services have an audience that includes a notable number of kids (and there's nothing that explicitly states that a significant number of children is greater than 50%). Hopefully, the definition of "significant" will be clarified in future regulations promulgated by the California Attorney General.

DPIA Requirement

The ADCA would require companies to complete a DPIA for new and existing online products and services and biennially review all DPIAs as long as these online products and services are likely to be accessed by children.

The ADCA DPIA requirement is prescriptive. Specifically, the DPIA must identify the purpose of the online product or service, how it uses children's personal information, and the risks of material detriment to children that arise from the business's data management practices, by analyzing whether the online product or service could do any of the following:

- Harm children, including by exposing children to harmful or potentially harmful content
- Lead to children experiencing or being targeted by harmful or potentially harmful contacts
- Permit children to witness, participate in, or be subject to harmful or potentially harmful conduct
- Allow children to be party to or exploited by harmful or potentially harmful contacts
- Harm children by its use of algorithms
- Harm children by its use of targeted advertising

The DPIA must consider whether and how system design features are used to increase, sustain or extend children's use of the online product or service, as well as whether, how and for what purpose the online product or service collects or processes children's sensitive personal information. "Harmful" and "potentially harmful" are not defined by the ADCA, which also makes those terms ripe for definition by the California Attorney General through regulation.

If the DPIA identifies any risks to children as defined by the ADCA, businesses must create a plan for modifying the online product or service to mitigate or eliminate the risk. While the identified harms do not need to be immediately mitigated or eliminated, businesses must create the plan prior to the online service or product going live.

It is worth noting that the DPIA requirement here is much broader than the requirement under the California Privacy Rights Act (CPRA), which only requires businesses to conduct DPIAs in limited circumstances, such as where processing activities present a "significant risk" to privacy and security (rather than requiring a DPIA for all online services and products that are likely to be accessed by children). Under the CPRA, there are no products, features or activities that are automatically in scope for a DPIA. Furthermore, the CPRA's DPIA evaluation requirements are not as prescriptive (although this topic may be further addressed by forthcoming regulations from the California attorney general). The CPRA currently requires DPIAs to:

- Indicate whether the processing involves sensitive personal information
- Identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, with the goal of restricting or prohibiting such processing if the risks to the privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders and the public

With respect to reporting, under the CPRA, businesses will be required to submit DPIAs to the California Privacy Protection Agency on a regular basis, whereas ADCA DPIAs must be made available to the attorney general within five business days of receipt of a written request.

Finally, businesses should consider engaging a third party to conduct their DPIAs under the ADCA so that the DPIAs could be considered privileged work product. Because the ADCA DPIAs focus on identifying potential harms to children, those DPIAs may contain sensitive business information that would potentially be used against a company in litigation. Therefore, businesses may want to take proactive steps to protect their DPIAs from disclosure during litigation. Note, however, that the ADCA does provide businesses with some protection in matters involving the Attorney General. The ADCA expressly states that disclosure of information in DPIAs to the California Attorney General does not constitute waiver of privilege or work product protection.

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 and a level of assurances 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 service and the ability of the online product or service to collect information from users, this essentially may require businesses to implement some form of age verification or age gate for all end users.

Prohibition on Automated Profiling

Automated profiling is prohibited unless "appropriate safeguards" have been implemented and the profiling is either necessary to provide the service or "in the best interest of children." "Profiling" is defined broadly as "any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." While other privacy laws—in particular, state student privacy laws—may prohibit the creation of profiles for use in connection with behavioral advertising, the ADCA's definition of "profiling" is much broader than behavioral advertising profiles and can include profiles that are created for any purpose.

Geolocation Requirements

The ADCA also strictly regulates the collection and use of geolocation information. Under the ADCA, 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 ADCA requires businesses to provide an "obvious signal" to the child when the child's activity or location is being tracked by a third party (e.g., parent or guardian). The fact that the child or the child's parent has previously agreed to the collection of this information does not relieve the business of the obligation to comply with this requirement.

Businesses that are only collecting geolocation information or tracking activity in the background will need to consider how they will communicate this signal to end users. Note that the U.K.'s Age Appropriate Design Code contains a similar requirement to provide an obvious sign to the child when they are being monitored and recommends a "lit-up icon."

Dark Patterns

Under the ADCA, businesses cannot use dark patterns or other techniques to (i) encourage children to provide additional personal information beyond what is reasonably expected for the online product or service; (ii) forgo privacy protection measures; or (iii) 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. This can be distinguished from the CCPA/CPRA's prohibition of dark patterns, which focuses on making sure consumers can make their own informed choices without having to navigate misleading interfaces and design features. The ADCA's prohibition of dark patterns is much broader because it is tied to a child's best interest and well-being.

Penalties

Penalties under the ADCA can be severe. Any violation of the ADCA is subject to an injunction and liable for a civil penalty of up to $2,500 per affected child for each negligent violation or up to $7,500 per affected child for each intentional violation, if the violation is not cured within a 90-day period. While the penalties are limited to each child, it is possible that there may be multiple violations per child, which could greatly increase the number of penalties imposed on businesses. The ADCA does not include a private right of action. The California Attorney General has exclusive jurisdiction to enforce the law.

What Does the ADCA Mean for Businesses?

The breadth of the ADCA may sweep in many online services and products that are now considered outside the scope of children's privacy laws. These may include children's websites that do not collect personal information; websites directed toward teens; and general audience sites that are routinely accessed by a significant number of children. In addition, the ADCA's requirements for compliance are much broader than those of any children's privacy laws or other California privacy laws because the ADCA focuses not only on the use and collection of personal information but also on how the design of the online product or service may harm a child. Because of the breadth of the ADCA, even though businesses have almost two years until the law is effective, they should consider determining how this law may affect their business as soon as possible.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Nerissa Coyle McGinn . . . . . nmcginn@loeb.com
Robyn Mohr . . . . . rmohr@loeb.com
Allison Cohen . . . . . ahcohen@loeb.com
Shely Berry . . . . . sberry@loeb.com
Chanda Marlowe . . . . . cmarlowe@loeb.com

7087 REV1 09-27-2022