BCLP. Client Intelligent

Insights

CALIFORNIA'S AGE-APPROPRIATE DESIGN CODE ACT HEADS TO NEWSOM'S DESK – WHAT DOES THIS MEAN FOR BUSINESSES?

Sep 07, 2022

SUMMARY

The protection of children's online data has come to the forefront as one of the most important data privacy issues both in the United States and EMEA, and California is now expected to join the list of jurisdictions to enact regulations in the space. On August 30, 2022, the California legislature unanimously passed AB 2273, the Age-Appropriate Design Code Act (AADC). The AADC is intended to further the purposes and intent of the California Privacy Rights Act of 2020 (CPRA) by "promot[ing] privacy protections for children." The AADC is modeled after the U.K. Age-Appropriate Design Code, thus businesses that have already come into compliance with the U.K. counterpart to the AADC will not have a significant compliance burden. For all others, the AADC (if signed by Governor Newsom and enacted) will go into force on July 1, 2024, providing companies with lead time to prepare, but as organizations have learned over the course of the last few years with the passage or amendments of complicated privacy laws in the United States and abroad, it is critical to start early in efforts to adapt and expand existing privacy programs to meet new requirements. To help with these efforts, we've set out below a brief set of FAQs to break down the draft law.

Who does the AADC aim to protect?

"Children" or "child," as defined by the statute, includes a California resident who is under the age of 18 years.[1]

Who must comply?

"Businesses" - as defined by the CPRA[2] - that develop and provide "online services, products, or features likely to be accessed by a child" are required to comply with the specified standards.[3] This includes online products and services specifically directed at children, as well as all other online products and services they are likely to access.

"Likely to be accessed by a child" means that it is reasonable to expect, based on the nature of the content, the associated marketing, the online context, or academic or internal research, that the service, product, or feature would be accessed by children.[4] The AADC is far-reaching in its application, particularly when viewed against the more narrow standard of the federal Children's Online Privacy Protection Act (COPPA), which applies when a business operates a website or online service directed to children, or such a business has actual knowledge that it is collecting or maintaining personal information from a child and only covers children under the age of 13 rather than 18.

What is required?

The AADC imposes 7 requirements on qualifying online businesses and prohibits such businesses from engaging in 8 different actions.

In-scope organizations must:

1. Perform a Data Protection Impact Assessment (DPIA) for any features likely to be accessed by children, review any DPIAs every 24 months or before any new features are offered to the public, and make any such DPIAs available to the Attorney General within 5 business days of receipt of a written request.

2. Estimate the age of "child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business, or apply the privacy and data protections afforded to children to all consumers."[5]

3. Configure all default privacy settings provided to children to the settings that offer the highest level of privacy protection offered by the business.

4. Provide privacy information, terms of service, policies, and standards in concise language that can reasonably be understood by the children likely to access the business' online service, product, or feature.

5. Where the business enables a child's online activity or location to be tracked by a third party (e.g., parent or guardian), provide an "obvious signal" to the child when the child is being monitored or tracked.

6. Enforce the published terms, policies, and community standards established by the business.

7. Provide prominent, accessible, and responsive tools to help children, or where applicable their parent or guardian, exercise their privacy rights and report concerns. This requirement appears to be duplicative of the CPRA's detailed disclosure requirements regarding how consumers can exercise privacy rights.

In-scope organizations may not:

1. Use the personal information of any child in a way the business knows or has reason to know is materially detrimental to the physical health, mental health, or well-being of a child.

2. "Profile" a child by default. "Profiling" is defined 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."[6] The AADC does provide limited exceptions to the prohibition on default profiling.

3. Collect, sell, share, or retain any personal information that is not necessary to provide the online service, product, or feature with which a child is actively and knowingly engaged.

4. Use a child's personal information for any reason other than the reasons it was collected.

5. Collect, sell, or share any precise geolocations information unless it is necessary to provide the service, product, or feature. In such instances, collection of precise geolocation information must be limited only to the time necessary.

6. Collect, sell, or share any precise geolocation information without providing an obvious sign to the child for the duration of that collection.

7. Use dark patterns or other techniques to encourage children into providing additional personal information or foregoing privacy protection measures.

8. Use or retain any personal information collected or processed to estimate age or age range for any other purpose, other than to estimate age. Age assurance shall be proportionate to the risks and data practice of a service, product, or feature.

Who/how will the AADC be enforced?

The AADC creates the California Children's Data Protection Working Group, a 10-member group appointed from various branches of government and the California Privacy Protection Agency. The Working Group is tasked with evaluating best practices for the implementation of the AADC.

- The Working Group will consist of Californians with expertise in children's data privacy, physical and mental health and well-being, technology, and children's rights.
- The Working Group will make recommendations for best practices in implementing the AADC. For example, helping identify which online services are likely to be accessed by children.

The Attorney General may also adopt regulations as necessary to clarify the requirements of the AADC and will assume enforcement powers – there is no private right of action. The AADC includes a 90-day cure provision for companies to rectify violations.

If enacted, as is likely to be the case, the AADC will be one of the most consequential laws impacting the online ecosystem. Stay tuned, as we dig deeper into the AADC's operational impacts and discuss how businesses can begin to comply.

---

[1] AADC, Section 1798.99.30(b)(1).

[2] A "business" as defined by the California Consumer Privacy Act – a for-profit organization that does business in California and meets any of three criteria:

1. Has an annual gross revenue of more than $25 million in the prior calendar year, or
2. Alone or in combination, buys or, sells, or shares the personal information of more than 100,000 consumers or households; or
3. Derives 50% or more of its annual revenues from the selling or sharing of consumers' personal information.

[3] Id. at Section 1798.99.30(b)(4).

[4] Id. at Section 1798.99.30(b)(4)(A)-(F).

[5] Id. at Section 1798.99.31(5).

[6] Id. at Section 1798.99.30(b)(6).

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448
