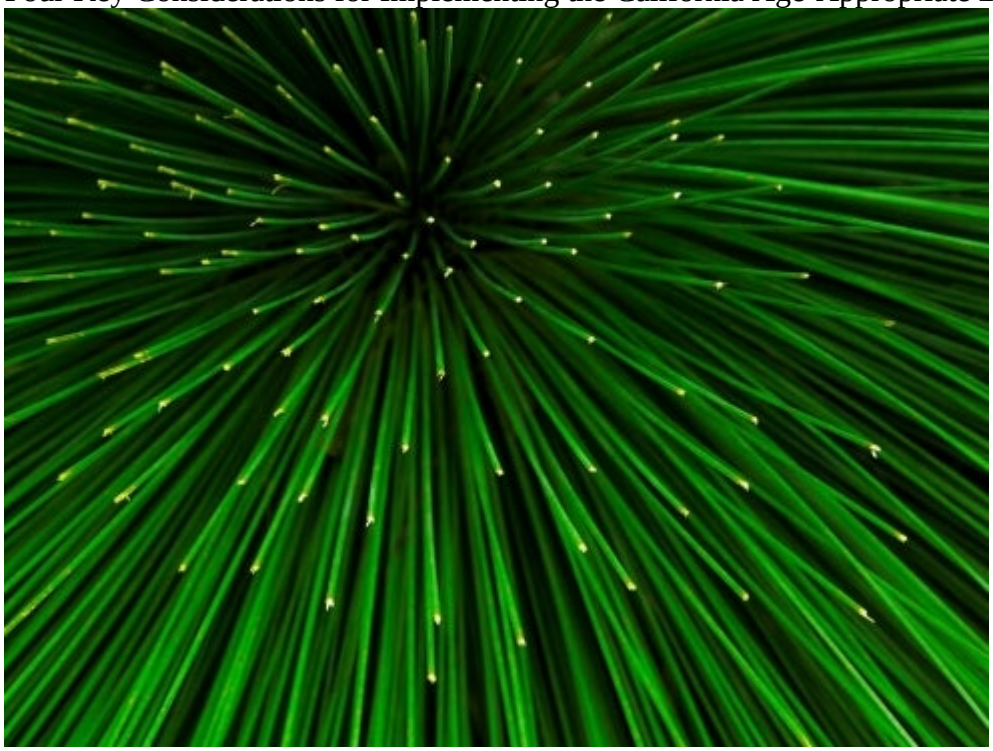
Updates
March 30, 2023
Four Key Considerations for Implementing the California Age-Appropriate Design Code



Since 1998, the Children's Online Protection Act (COPPA) has governed how websites directed to children in the United States must approach data privacy for individuals under age 13. COPPA focuses mostly on the collection, use, and disclosure of personal information and the concept of parental notice and control. But there have been efforts in recent years, both in the United States and abroad, to more extensively regulate content directed to minors. These efforts aim to address the privacy of personal information, the protection of teens in addition to children under age 13, as well as general online safety, beginning with the United Kingdom's Age-Appropriate Design Code (UK AADC).

The UK AADC requires online providers to comply with a series of privacy and product design obligations and extends to websites that are likely to be accessed by children. In September 2022, California became the first state to adopt similar protections for children's online privacy with the adoption of the California Age-Appropriate Design Code Act (CA AADC). The CA AADC largely mirrors the UK AADC's privacy requirements and builds on its product design and online safety requirements for kids under age 18. The CA AADC's notable obligations include requiring providers to configure default privacy settings to a "high level" of privacy; assess whether algorithms, data collection, or targeted advertising systems could harm children; and use clear, age-appropriate language for user-facing information and documents. More generally, the CA AADC states in its legislative findings that businesses should consider the "best interests of children" when designing, developing, and providing online services, products, or features likely to be accessed by children.

A lawsuit to invalidate the CA AADC on constitutional grounds was recently filed in federal court, and more challenges may follow. In the meantime, businesses that may be subject to the law when it goes into effect on July 1, 2024, may want to consider if they are in scope and, if so, how this may affect how they design, develop, and provide their online offerings.

Here are four key considerations:

1. Is Your Company in Scope?

The CA AADC applies to companies that (1) meet the definition of a "business" under the California Consumer Privacy Act (CCPA) and (2) provide online services, products, or features that are "likely to be accessed by children." Companies may be subject to the CA AADC even if their website or online service is not "directed to children" as defined under COPPA, as the CA AADC focuses on what children are "likely to access," rather than whether the website or online service is *specifically directed* at children. However, apart from the CA AADC's focus on all minors under age 18 and COPPA's focus only on those under 13, it is not yet clear how different the "likely to access" standard will be.

(a) Definition of a Business Under CCPA

Under the CCPA, a "business" is any for-profit California entity that collects and processes the personal information of California residents and satisfies one of the following thresholds: (1) had annual gross revenues in excess of $25 million in the preceding calendar year; (2) alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more California residents or households; or (3) derives 50% or more of its annual revenues from selling or sharing the personal information of California residents.

(b) "Likely To Be Accessed by Children"

Businesses meeting the above thresholds will need to assess whether their online service, products, or features are "likely to be accessed by children," meaning "reasonable to expect" that the service, product, or feature would be accessed by children, based on a list of indicators listed in the statute. Companies are directed to look at whether an online service, product, or feature:

• Is directed to children (as defined by COPPA).

• Is routinely accessed by a significant number of children (as determined by competent and reliable evidence regarding audience composition).

• Contains advertisements marketed to children.

• Is substantially similar or the same as another online service product or feature that is determined to be routinely accessed by a significant number of children.

• Has design elements that are known to be of interest to children (e.g., games, cartoons, music, and celebrities who appeal to children).

• Has children constituting a significant amount of its audience (as determined by internal company research).

Since the definition of "likely to be accessed by children" encompasses the definition of "directed to children" under COPPA, it is important to look at that definition as well, which considers things such as the subject matter and language of the site or online service, the visual or audio content, the age of models, the use of animated characters or other child-oriented activities and incentives, the nature of advertising on or promoting the site or online service, the presence of child celebrities or celebrities who appeal to children, and empirical evidence regarding audience composition and intended audience. Companies should carefully evaluate all of the relevant factors cited in both statutes when making the determination if their online service, product, or feature is "likely to be accessed by children."

2. What Are the Ages of Any Children Likely To Access Your Products?

The CA AADC requires that companies subject to the law estimate the age of child users with a reasonable level of certainty (appropriate to the applicable level of risk) or apply the required protections to all consumers. It does not, however, provide guidance as to how this is to be done or how to do it in a manner that addresses principles such as data minimization.

The legislative declarations underlying the CA AADC note that businesses should take into account the unique needs of the different age ranges of children and separate these age ranges into five developmental categories: 0 to 5 years of age or "preliterate and early literacy," 6 to 9 years of age or "core primary school years," 10 to 12 years of age or "transition years," 13 to 15 years of age or "early teens," and 16 to 17 years of age or "approaching adulthood."

Although it is not yet clear exactly how these categories will come into play, companies should consider these developmental categories as they start to evaluate the safety of their data practices and, in particular, where there are specific requirements to take the age of the user into account.

Companies should also be mindful about how the CA AADC interacts with COPPA and other children's privacy laws. For example, general-audience sites generally don't need to worry about COPPA unless they have actual knowledge that they are collecting information from a child under 13. Obtaining data about the age of specific users could provide that knowledge.

3. How Does Your Company Address Privacy by Design and Default?

Two key principles under the CA AADC are: (1) privacy by design and (2) privacy by default. Privacy by design requires a company to consider data protection and privacy throughout the entire data life cycle, starting from the design phase at inception. Although privacy by design has been a part of the U.S. privacy framework since 2012, the CA AADC provides a new level of specificity around this requirement and requires businesses to address a variety of specific harms that could arise based on their design.

The statute requires that businesses configure all default privacy settings provided to children with a "high level of privacy," although it is not yet clear what this undefined phrase means.

Companies may want to consider implementing a privacy by design and default approach even before the CA AADC goes into effect, as enforcement actions in this area are on the rise from the Federal Trade Commission (FTC), the UK Information Commissioner's Office, the Irish Data Protection Commission, and other enforcement organizations based on more general requirements under existing children's privacy law. Companies that fail to implement appropriate privacy and design product changes will continue to risk sizable fines, particularly in the EU and United States.

4. How Can Your Company Start To Identify and Address Potential Risks?

The CA AADC requires companies to use Data Protection Impact Assessments (DPIAs) to evaluate their compliance with its principles. Before offering any new online services, products, or features likely to be accessed by children, businesses will need to (1) complete a DPIA that identifies the risks of material detriment to children that arise from the business' data management and product design practices, and (2) create a timed plan to mitigate or eliminate those risks. Companies will be required to provide these DPIAs to the attorney general upon request.

While many companies are familiar with DPIAs as a result of the EU's General Data Protection Regulation (GDPR), the CA AADC's DPIA requirements extend well beyond the GDPR's focus on data processing and collection. The CA AADC requires that DPIAs identify the purpose of the online product, service, or feature,

how it uses children's personal information, and whether the design of the online service, product, service, or feature could:

- Harm children (e.g., exposing children to harmful or potentially harmful content).
- Lead children to either experience or be targeted by harmful, or potentially harmful, contacts on the company's platform.
- Permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the platform.
- Allow children to be a party to or be exploited by a harmful, or potentially harmful, contact on the company's platform.
- Harm children via algorithms used by the online product, service, or feature.
- Harm children via targeted advertising systems used by the online product, service, or feature.
- Extend, increase, or sustain the use of the online product, service, or feature by children (e.g., rewards, notifications, and autoplay of media).
- Include the collection or processing of sensitive personal information of children (and if so, how and for what purpose).

Notably, the CA and UK AADCs reflect an emerging trend in online safety regulation, with an increasing focus on due diligence obligations and risk assessments. The EU's Digital Services Act (DSA), Australia's Online Safety Act (OSA), India's Intermediary Guidelines, and Singapore's Online Safety Bill, for example, also require certain providers to be proactive in addressing online safety risks, with an emphasis on the protection of minors. Several pending bills, including the U.S. Kids Online Safety Act, the U.K. Online Safety Bill, and state bills in Maryland, New Jersey, New Mexico, and Utah also seek to make service providers responsible for keeping minors safe online.

Takeaway

While the CA AADC will not go into effect until next year, companies within its scope may want to get an early start in identifying potential risks in a DPIA and take measures to address them, as appropriate. Considering these privacy and safety issues early in the product development cycle could help reduce risk and facilitate compliance.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Digital Media & Entertainment, Gaming & Sports

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors