Articles + Publications | October 4, 2022

California Age-Appropriate Design Code Is Not Child's Play – Five Practical Tips to Comply and Protect Kids' Privacy

WRITTEN BY

Ronald Raether, Jr. | Tambry Lynette Bradford | James Koenig | Robyn W. Lin

This article appeared in the January 2023 edition of Pratt's Privacy & Cybersecurity Law Report.

On September 15, 2022, California Governor Gavin Newsom signed Assembly Bill 2273 — the California Age-Appropriate Design Code Act (ADCA) — into law. Inspired by the United Kingdom's (U.K.) Age-Appropriate Design Code, the ADCA will impose data privacy requirements on businesses that provide "an online service, product or feature likely to be accessed by a child." Unlike the Children's Online Privacy Protection Act (COPPA), which governs the use and sharing of children's data once it has been collected, ADCA goes further by requiring businesses to consider children during the development of a product or service. This includes considering the different needs of a child based on their age.

Applicable Businesses. ADCA only applies to businesses subject to the California Consumer Privacy Act, *i.e.,* including its qualification thresholds (as of January 1 of the preceding calendar year, had annual gross revenues in excess of $25 million; or buys, sells, or shares the personal information of 100,000 more consumers or households; or derives 50% or more of its annual revenues from selling or sharing consumers' personal information).[1] More specifically, ADCA only applies to businesses that "develop and provide online services, products, or features that children are likely to access." While COPPA applies to targeting children, and businesses are free to make that choice, and the U.K.'s ICO sets a high bar in requiring focus groups, California now sets potentially the highest bar by requiring "likely access" by children. It's hard to believe an argument can't be made that children would likely access any content on the internet. As this may be the potentially most impactful provision of the law, the law sets forth a working group to create a report on best practices for ADCA implementation.

Comparison to the U.K. and COPPA

Provision		
Applicable Entities		

Definition of Child

Limits on Data Collection

Precise Geolocation

Default Privacy Settings

Determining Age

Prohibitions. ADCA imposes a number of restrictions on businesses.

- ***Profiling a Child by Default.*** The ADCA defines "profiling" as any "form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person … ." While this will hopefully be subject to additional guidance, automated processing will likely apply to all adtech, casual and hyper-casual gaming, and other sites that provide customization and automated decision-making.

- ***Collect Precise Geolocation.*** The ADCA prohibits collecting precise geolocation, unless there is an obvious signal to the child that this information is being collected.

- ***Dark Patterns.*** The ADCA prohibits the use of dark patterns to encourage children to provide additional personal information that is unnecessary, as well as to forego privacy protection measures. Dark patterns is defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice" and is subject to further rulemaking.

Requirements. ADCA imposes a number of requirements (and prohibitions) on businesses. A few of these requirements build on those already in place under other regulatory regimes, such as data privacy impact assessments (DPIA) similar to those under the European Union (EU) General Data Protection Regulation (GDPR) and conspicuously posted privacy notices.

- ***Data Protection Impact Assessment (DPIA).*** ADCA requires businesses to undertake a DPIA before any product or service that a child is likely to access is offered to the public. This assessment must be made available to the California attorney general pursuant to a written request within five days.
  - **Implementation Tip:** Businesses already subjected to the U.K.'s Age-Appropriate Design Code can likely leverage past DPIAs. Additionally, this is an area of rulemaking for all businesses subject to the CCPA. The notice and cure for regulatory actions expires on January 1, 2023. Five days is a much shorter deadline than what is available when the attorney general serves a subpoena — all creating a need to be proactive.
  - **Implementation Tip:** DPIAs are required in an increasing number of countries, including the EU and China. The trend for many companies is to develop a global DPIA and to incorporate standard dropdown boxes based on regulatory guidance for these forms to be quickly and easily completed by engineers and attorneys alike.

- ***Apply Protections Appropriate to a Child's Age or Treat All Users the Same.*** ADCA requires a business to reasonably estimate the age of a child-user. Further, ADCA requires businesses to consider the unique needs of different age ranges (*e.g.,* the needs of a preliterate child to an early teenager).
  - **Implementation Tip:** Segmenting child-users will be tricky. Functionality of the product or service will be important. Some products will obviously be impacted — others not (think attractive nuisance). Ensuring privacy considerations are incorporated early on within the product or software development lifecycle and are captured in the DPIA will ensure efficient compliance, which requires the entire team (*e.g.,* business, marketing, IT, compliance) to interact from concept design to release. Normally, companies targeting children use an age gate to determine the age of a child and whether verifiable parental consent or other controls are required (*see*, for example, superawesome.com).

- ***Prominently Feature Privacy Notices and Enforcement.*** ADCA requires a business to prominently feature any privacy information, terms of service, and policies and to enforce of these policies. For example, the California AG recently published several enforcement examples, including businesses that failed to include methods for exercising consumer rights in their privacy policies. Enforcement of a business's privacy policy would include ensuring the consumer request process is being carried out as described in the policy.

- ***Configure All Privacy Settings to the Highest Level by Default.*** ADCA requires all default privacy settings provided to children to offer the highest level of privacy (*e.g.,* automatically setting any social media profiles to private by default as opposed to public), unless the business can demonstrate a compelling reason that a different setting is in the best interest of the child.
  - **Implementation Tip:** The California legislature does not specify what is considered a "compelling reason." This may be an area that the attorney general solicits comments for rulemaking. That said, customization that doesn't impact personal information (*e.g.,* gaming high score, favorite color, and other information-capture product features) may be ripe for review under this area.

Implementation Tips: ADCA goes further than COPPA since it requires a business to consider the interests of a child during the development of a product or service, as opposed to obligations that are triggered when children's information is knowingly collected. That said, California doesn't impose an obligation to investigate and/or audit whether there are children among their users.

1. **Implement Age Gates for Content Accessible to Children 13-17 Years Old.** Companies have historically determined the age of children by using age gating (*see* superawesome.com, or alternatively, companies may rely on the Google app store as Google has begun rolling out targeted ads for children under 18). Up until now, U.S. companies have always had the flexibility to only use age gates if they believe that their content was directed to children under 13 in the U.S. and in the EU, unless a higher age was set by local law. Since California copied the ICO in making the requirement apply to children under 18 who might have access to the content, many companies who didn't target young children, but focused on gaming and social media and other content for teenagers and older users, will now have to start implementing age gates where previously they had not.

2. **Develop an Integrated DPIA Form Addressing Global and Children's Nuances**. While the GDPR launched the development of DPIAs, other countries have followed suit. For example, China largely enhanced the European DPIA as the basis for its security assessment relating to or transferring data.[2] Similarly, the same DPIA template could also have age considerations, as well as privacy by default standards, for targeted advertising, location data, customization, and other potentially high-risk data collection or technologies.

a. Companies should note that New York has introduced a similar bill. Just as the CCPA inspired different states to enact their own privacy legislation, other states may also begin to focus on children's privacy.

3. **Test.** Test the value of targeted advertising versus contextual advertising before the effective date.

4. **Update Your Privacy Policy and Develop New Notices.** Update privacy policy, but more importantly, develop new just-in-time notices and consent mechanisms to provide more detail around information collected from children for products and services with features that rely on location, profiling, targeted advertising, and or other technologies to result in the highest engagement. For example, many companies went through a similar struggle when Apple implemented its IDF application-specific consent requirements, and many companies had to think of the best way to obtain consent for permission for customized experiences and advertising.

a. Companies creating websites to comply with CCPA's nondiscrimination provision can likely use these same websites for children as well.

5. **Data Mapping.** Conduct a data inventory and mapping of your product. Identify all the location of your services (especially as different countries have different age limits), what you collect from children, and how that data is used in any downstream process (*e.g.,* profiling, customization, data lake for analytics, downstream advertisement).

---

[1] For additional information about the CPRA, see Troutman Pepper's five-part series, consisting of: (1) introduction and overview; (2) consumer rights; (3) notice and disclosure obligations; (4) data processing obligations; and (5) litigation and enforcement.

[2] For further information, check out Troutman Pepper's publication on transferring under PIPL: https://www.troutman.com/insights/simplifying-a-complicated-process-four-steps-to-comply-with-chinas-pipl-new-security-assessment-requirements-for-cross-border-data-transfers-sept-1-2022.html.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management