KPMG

Are the kids alright?

The California Age-Appropriate Design Code Act: A new era for children's online privacy in the U.S.?

2023

kpmg.com

Contents

Kids privacy: a new wave? Is the COPPA clock up?

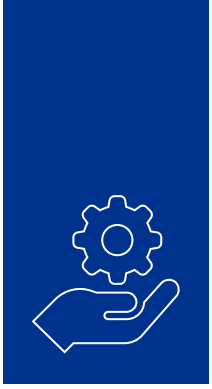
Since 1998, children's privacy in the U.S. has largely been protected by the Children's Online Privacy Protection Act (COPPA). When COPPA was introduced, there was a markedly different digital landscape than the one we are now living in, with only 9 percent of households having access to the internet and 41 percent of adults being "online"[1] (and likely not from the comfort of their own homes let alone via smartphones). This provides a sharp contrast to internet access today, where an estimated 95 percent of children between the ages of 3 and 18 are online and just over half of U.S. children now own a smartphone by age 11.

The UK has led the way with the introduction of the Age-Appropriate Design Code (AADC), which sets out 15 standards designed as "a set of technology-neutral design principles and practical privacy features." Social media, gaming, and streaming providers have since come under scrutiny from the Information Commissioner's Office (ICO), the governing body responsible for reviewing compliance with the AADC. TikTok, for example, was recently fined 12.7m GBP by the Information Commissioner's Office (ICO) for failure to adequately check who was using their platform and using personal data belonging to children without parental consent.

Borrowing significantly from the UK AADC, the California Age-Appropriate Design Code Act (ADCA) was signed into law on September 15, 2022 and is set to take effect July 1, 2024. The ADCA should not necessarily come as a surprise to businesses given the extent of digital creep into even the most mundane corners of analog life, resulting in a burgeoning need to protect children's privacy online. This, together with steps taken by other jurisdictions in this area (namely the UK with the AADC and Ireland with the Data Protection Commissioner's Fundamentals), has inspired legislative action in California. Nevertheless, some aspects of the ADCA may still come as a shock to businesses with some provisions going beyond that of the AADC.

The following provides a summary of the key focus areas for impacted companies and a comparative analysis on the impact of COPPA, the AADC, and the ADCA.

[1] Source: Pew Research Center web site, Susannah Fox (June 21 2007)



Taking the first steps to ADCA compliance

The ADCA applies to "businesses," as defined under the California Consumer Privacy Act (CCPA), operating in California and providing online services, products, and features "likely to be accessed by children" ("children" being defined as minors under the age of 18). This scope is not insignificant given the vast number of California-based businesses providing these types of products and services to minors—or to general audiences that may include children under 18. The breadth of the ADCA, together with the developing patchwork of privacy laws proliferating across the U.S., demands businesses take a proactive approach towards compliance with the ADCA—and, indeed, towards privacy regulations more generally. The following sets out five key focus areas for businesses falling in scope of the ADCA.

1

Age estimation and verification

- Implementation of risk-based approach to estimate a child's age
- Integration of age verification mechanisms where necessary

2

Age-appropriate by design and default

- Consideration of "best interests of children" when designing online services, features, and products
- High-level privacy settings by default for children users

3

General business practices

Review of products, services, and features for prohibited activities, including nudge techniques, dark patterns, unnecessary data collection, and prohbited third-party data sharing

4

Data protection impact assessments (DPIAs)

Establish or update of DPIA process to fulfill ADCA-specific DPIA requirements

5

Children's privacy rights

Provision of prominent, accessible, and responsive tools to help children and/or parents on behalf of children, to exercise their privacy rights and report concerns

A comparative analysis: COPPA/UK AADC/ADCA

Provision	COPPA	UK AADC	ADCA	Analysis
Scope of application	Defines children as minors under 13 and applies to businesses that have products and services *directly* aimed toward children	Defines children as all minors under 18 and applies to information society services (ISS) providing online products/services that process personal data and are likely to be accessed by children in the UK	Defines children as all minors under 18, and applies to businesses providing services "likely to be accessed by children"	The scope of application under the AADC and ADCA is clearly much broader than the federal framework with the "likely to be accessed" standard encompassing a much broader range of online products and services than COPPA's "directed to children" standard.
Age estimation and age-appropriate design	No age-estimation exercise requirement	The age of the child should be estimated to a degree of certainty appropriate to the risks arising from the data processing, or the highest protections should be afforded to all consumers. Upon estimation/verification of age, protections, safeguards, and policies should be designed appropriate to that age. Note: age ranges can be used when designing privacy protections/safeguards/policies, e.g., for ages 5–10, ages 11–15, etc.	The age of the child should be estimated to a degree of certainty appropriate to the risks arising from the data processing, or the highest protections should be afforded to all consumers. Age-appropriate language must be used for privacy disclosures for children age 10 and over. Privacy safeguards and protections must be appropriate to the age of the child, or, as stated above, the highest protections should be afforded to all consumers. Note: there is no mention of using age ranges as per the AADC.	Liability is created under the UK AADC and the ADCA if a service knew or should have known that children are *likely* to access its products/services, even if those products/services are not directed to children, creating a broader scope of application than COPPA's "actual knowledge" standard. With regards to age-appropriate design, unlike the AADC, the ADCA does not utilize age ranges, potentially raising implementation issues with businesses being forced to curate age-appropriate language and safeguards/protections for a very broad range of development needs for children between ages 10 and 18.

Provision	COPPA	UK AADC	ADCA	Analysis
DPIAs	No DPIA requirement	AADC DPIAs are the same as General Data Protection Regulation (GDPR) DPIAs, so they must be carried out to assess and mitigate risks to the rights and freedoms of children likely to access the service/ product.	Prior to creating a new product/service/feature likely to be accessed by a child, businesses must conduct a DPIA identifying the purpose of the product/service, how children's personal information will be used, and the risks arising from the data processing. Note: there is an obligation to analyze risks to the general well-being of the children as opposed to specific privacy risks. Upon request from the California Attorney General (CA AG), a list of all DPIAs must be produced within three business days and copies of requested DPIAs must be submitted within five days of a request.	Businesses in the UK/ European Union will most likely already have a DPIA process in place (or should) under the GDPR/ UK GDPR. However, the ADCA is more prescriptive than the AADC/UK GDPR DPIA obligation. As such, impacted businesses must review and update their DPIA process accordingly. Particular regard should be given to the tight turnaround times for responding to requests from the CA AG and the requirement to consider the general well-being of the child.
Privacy-by-default	No privacy-by-default obligation	Settings must be "high privacy" by default unless a "compelling reason" exists for a different default setting that takes into consideration the best interests of the child.	Settings must be "high privacy" by default unless a "compelling reason" exists for a different default setting that takes into consideration the best interests of the child. Note: This includes a restriction on the profiling of children by default and default sharing of "precise geolocation information."	The AADC and ADCA both require businesses to enforce a high-privacy approach to default settings. As such, businesses should determine settings controlling the processing of data are sufficiently granular, transparent, and set to "Off" by default. There may be more scope for default profiling of children under the ADCA if a "compelling reason" exists. Similarly, with regards to default sharing of "precise geolocation information," the specification of "precise" in the ADCA indicates that default sharing of *nonprecise* geolocation information may be permitted.

Provision	COPPA	UK AADC	ADCA	Analysis
Dark patterns and nudge techniques/ data minimization	Prohibits conditioning a "child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity"	Prohibits the use of manipulative techniques that lead or encourage children to turn off privacy protections or to disclose personal data that is unnecessary for providing the service to which a child is "actively and knowingly engaged"	Prohibits the use of "dark patterns" or nudge techniques that lead or encourage children to provide more personal data than is necessary for the provision of a service to which the child is "actively and knowingly engaged"; give up privacy protections; or take action that is "materially detrimental" to the "health, physical or mental, or well-being of a child"	While the AADC and ADCA are consistent with COPPA's prohibition on conditioning the participation of the child, they are broader in scope, with the ADCA going even further than the AADC with the prohibition of nudges that could be "materially detrimental" to the well-being of the child. As a result, businesses will need to be more vigilant when it comes to identifying dark patterns that could negatively impact a child's well-being as opposed to just their privacy. Note: "Materially detrimental" has not yet been defined, so the impact of this term remains unknown.
Enforcement	COPPA is enforced by the Federal Trade Commission, by certain federal agencies, and at the state level. Penalties can be issued of up to $46,517 per violation.	The ICO is responsible for the enforcement of the UK GDPR and Privacy and Electronic Communications Regulations (PECR). The UK AADC will inform the ICO's enforcement of the UK GDPR/ PECR, breaches of which can result in regulatory fines of up to 17.5 million GBP or 4 percent of gross annual worldwide turnover (whichever is higher). However, the AADC is not law, so it cannot be legally enforced.	The ADCA is enforced by the CA AG, who can issue a 90-day cure period and fines of up to $7,500 per violation, per child. Penalties recovered from businesses are put to a Consumer Privacy Fund. The ADCA also creates the California Children's Data Protection Taskforce, a rulemaking entity responsible for adopting regulations by April 1, 2024 and providing compliance guidance.	Given the significant fines that can arise under these laws/codes, businesses should carefully review all relevant practices and processes. Businesses should be especially careful under the ADCA given the creation of a specific task force and evident attention the state is giving to children's privacy.

Looking ahead

The ADCA signals a shift in privacy lawmaking towards an approach more responsive to the needs of children living an increasingly digital life. While emanating in California, this is a shift that ought to be expected nationally. California has set a precedent of not only leading new waves of privacy law in the U.S. but also determining the amplitude of those waves, as demonstrated by the CCPA and the California Privacy Rights Act which amends and extends the CCPA. It is likely only a matter of time, therefore, before other states start following suit with their own iterations of the ADCA. In fact, New York has already introduced a children's privacy bill (Senate bill 9563, The New York Child Data Privacy and Protection Act) in the New York Senate mirroring the provisions of the ADCA. It is on this basis that a proactive grappling with the terms of the ADCA should be encouraged beyond the businesses currently impacted, for it is only a matter of time before the California law takes effect and more states start taking similar legislative steps to protect the mental, physical, and general well-being of the child online. In fact, the ADCA may signal the dawn of a new era of privacy lawmaking for at-risk groups in general—as opposed to just children—in which case, its impact will be even greater than initially thought.

How KPMG can help

At KPMG, our privacy team is ready to assist your organization in driving change for clients preparing for the ADCA. KPMG has significant experience in this space, having helped clients prepare for a host of privacy laws over recent years, including GDPR, CCPA, CPRA, and, most recently, the ADCA. Below is a three-stage process for companies to follow, with the help of KPMG privacy specialists, to successfully adapt their privacy programs to comply with the ADCA.

Learn more about the KPMG approach to privacy methodology and how it has helped clients respond to regulatory change in California by reviewing The California Consumer Privacy Act (CCPA).

Stage 1: Review and Assess	Stage 2: Create and Update	Stage 3: Finalize and Supplement
• **Perform review of products/ services/features** to determine (1) current processing of children's data and (2) likelihood of being accessed by children • **Analyze your business model** as it relates to the use of children's personal data (i.e., use of nudge techniques/dark patterns, default profiling techniques, sharing of precise geolocation data) • **Conduct age estimation balancing exercise** for applicable products/activities/ services • **Review age-appropriateness of privacy protections, safeguards, and policies**	• **Implement age verification mechanisms** at necessary points identified from age estimation exercise(s) • **Update privacy protections, safeguards, and policies** to be age-appropriate (including updating tools to be "prominent, accessible, and responsive" for children/ parents exercising privacy rights or concerns) • **Configure default privacy settings** to a high level of privacy for all child users or, alternatively, all users • **Implement/update tools** handling DSR to enhance suitability for child/parent use • **Create or update DPIA process** to account for ADCA-specific DPIA provisions • **Review and renegotiate vendor agreements** with third parties with whom children's personal data is shared in a "materially detrimental" manner	• **Finalize age verification mechanisms** and integrate where necessary • **Finalize updates to privacy protections, safeguards, and policies** to be age-appropriate • **Finalize DPIA process** with necessary updates to fulfil ADCA obligations • **Publish supplementary material** as needed providing guidance to children and parents in an age-appropriate manner • **Provide training and guidance** to employees on new and/or updated processes

Contact us

Clowance Wheeler-Ozanne
Sr. Associate Cyber Security Services
T: 214-840-2000
E: cwheelerozanne@kpmg.com

Rachael Reinis
Manager, Cyber Security Services
T: 202-533-5046
E: rreinis@kpmg.com

Michael Rossi
Director, Cyber Security Services
T: 212-954-4103
E: mnrossi@kpmg.com

Orson Lucas
Principal, Cyber Security Services
T: 813-301-2025
E: olucas@kpmg.com

Steven Stein
Principal, Cyber Security Services
T: 312-665-3181
E: ssstein@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia