wiley

NEWSLETTER

# California Age-Appropriate Design Code Act to Impose Significant New Requirements on Businesses Providing Online Services, Products, or Features

September 2022

*Privacy In Focus®*

On September 15, 2022, California Governor Newsom announced his signing of A.B. 2273, the California Age-Appropriate Design Code Act, which the legislature passed on August 30. The law – modeled after the United Kingdom Information Commissioner's Office code of practice for age-appropriate design – will impose broad new requirements on businesses that provide an online service, product, or feature that is "likely to be accessed by children," which the law defines as any individual under 18. The Act is scheduled to go into effect July 1, 2024.

Below, we provide a high-level summary of the sweeping new obligations businesses will need to navigate under this law, which is likely to have significant impacts on a wide range of companies.

**Whom Does the Law Apply to?**

The law applies to "businesses" 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, or
2. Alone or in combination, buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of more than 50,000 consumers, households, or devices; or

## Authors


Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law


## Practice Areas

Privacy, Cyber & Data Governance

3. Derives 50% or more of its annual revenues from selling consumers' personal information.

**What Products and Services Are Covered?**

The California Age-Appropriate Design Code Act (Act or bill) imposes requirements and restrictions on any "business that provides an online service, product, or feature likely to be accessed by children," and children are defined as "a consumer or consumers who are under 18 years of age." The law defines indicators of whether an online service, product, or feature is "likely to be accessed by" children:

- It is directed to children as defined by the Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 *et seq*. (COPPA), which means:
  - A commercial website or online service targeted to children; or
  - That portion of a commercial website or online service that is targeted to children.
- It is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children, or an online service, product, or feature that is substantially similar or the same as one routinely accessed by a significant number of children;
- It has advertisements marketed to children; or
- Internal company research determines that a significant amount of the audience of the online service, product, or feature consists of children.

This standard departs significantly from COPPA – the federal children's privacy framework. That law applies to children under the age of 13 and is triggered 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. Here, the age of protected individuals is expanded to include teenagers up through age 17, in addition to children under 13, and the standard for when the law is triggered is broader.

Further, while the law is modeled after the UK's age-appropriate design code, the California law notably exempts the delivery or use of physical products, while the UK code incorporates "connected" toys or devices. The California bill also includes other exemptions – namely, it exempts broadband internet access services and telecommunications services, as well as health care providers and medical information covered by what are commonly known as HIPAA rules, and clinical trial information.

**What Does the Law Require?**

The law imposes several new types of requirements on covered businesses, many of which are focused on default settings and transparency. For example:

- Services will need to estimate the age of child users with a "reasonable level of certainty" appropriate to the potential risks, unless they provide the same privacy and data protections appropriate to children to all their users. However, the information collected to estimate users' age cannot be used for any other purpose or retained longer than necessary to conduct that estimate.

- All products and services subject to the Act need to be subject to a Data Protection Impact Assessment before launch. The bill sets a July 1, 2024 deadline for any existing products or services, or those that will be rolled out before the deadline, to the extent they continue to be offered after July 1, 2024. The Data Protection Impact Assessment must consider:
  - The risk of harm from content, contacts, conduct, algorithms, and targeted advertising used;
  - Features that increase use, such as rewards, autoplay media, and notifications; and
  - The collection and processing of sensitive personal data.
- Any "risk of material detriment to children" identified in the Data Protection Impact Assessment requires a plan with deadlines to mitigate or eliminate risk before children access the product or service.
  - The contents of the assessment must be provided to the California Attorney General within five business days of a written request, but would be exempt from public disclosure, and companies would not waive any privileges associated with the reports by providing them in response to the Attorney General's request.
- Covered businesses must configure all default privacy settings provided to children by the online service to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.
- Covered businesses must offer any privacy information, terms of service, policies, and community standards "concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature." Importantly, the new law requires providers to enforce the published terms of service, policies, and community standards.
- Covered businesses also need to create "prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns."
- If the service, product, or feature allows parental tracking or any other user to monitor the child's online activity or location, the child must receive an "obvious signal" that they are being monitored.

**What Does the Law Prohibit?**

The law also includes strict prohibitions on many forms of collection, use, and sale of children's personal information.

- The law prohibits online products and services from using a child's personal information in any way the company knows or has reason to know is "materially detrimental" to the physical or mental health and well-being of the child.
- It also bans use of a child's personal information for any reason other than for which it was collected, unless there is a "compelling reason" that the use is in the best interests of the child.
- Covered businesses are not be allowed to collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless they can show a compelling reason why doing so is in the best interests of

the child.

- An online product, service, or feature is prohibited from default collection, sharing, or selling of "precise geolocation information" unless "strictly necessary" to provide the service or feature, and only during the limited time period that the collection is necessary to offer it. Further, any collection of precise geolocation information must include an "obvious sign" to the child user that the collection is taking place.
- The bill also bans profiling 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.
  - Providers can only conduct profiling by default if they have instituted "appropriate safeguards" and the profiling is necessary to provide the service and profiling is limited to what the child is actively using.
- Finally, the bill will prevent products, services, or features from using "dark patterns" to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forgo privacy protections, or to 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.

**How Will the New Law Be Implemented and Enforced?**

***Enforcement.*** The law does not provide a private right of action – instead, the California Attorney General has exclusive jurisdiction to redress violations through civil action. Fines for violations could be momentous, ranging from $2,500 per affected child for negligent violations, up to $7,500 per affected child for intentional violations. The enforcement provisions offer a strong incentive for companies to develop and implement a robust Data Protection Impact Assessment and mitigation plan process, because companies that have achieved "substantial compliance" with those assessment and mitigation plan requirements would have a 90-day grace period to cure, without penalty, any violations identified by the California Attorney General.

***Rulemaking.*** The California Attorney General will also have the authority to adopt regulations to clarify the law's requirements. As with the California Consumer Privacy Act, businesses should be prepared for future rounds of rulemaking. The Attorney General's office may look to the recommendations and best practices from the Children's Data Protection Working Group (described below) for issues to address with rulemaking.

***Children's Data Protection Working Group.***

The law would establish the California Children's Data Protection Working Group, which will be charged with developing recommendations and best practices to help address some of the key uncertainties in the language. Among other questions, the Working Group will be charged with addressing how to further define

and evaluate which online services or features are likely to be accessed by children, determining which "age assurance methods" are proportionate to online risks to children, what language in privacy and other policies is suited to children, and how to assess and mitigate risks to children online. The Working Group would include representatives with expertise in children's health, privacy, and computer science, and must take input from "a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses."

**The Act Will Have Significant Implementation Costs for the Tech Industry**

The California Age-Appropriate Design Code Act represents a massive shift in technology regulation with respect to minors in the U.S. Companies subject to the new California law will need to devote engineering, legal, privacy, and policy resources to implementing the new requirements and prohibitions for California users. At the same time, critical questions that would help drive implementation remain unanswered: What constitutes a "material detriment" to children? What is a "reasonable level of certainty" for age verification? How can privacy and other policies be written clearly for an audience of children?

As we have learned from the California Consumer Privacy Act, and given the breadth of this new law, it is important to begin planning for compliance now.

***

Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws, and advocate before government agencies. Please contact any of the authors with questions.