California's Age-Appropriate Design Code Act Summary

On September 15, 2022, Governor Gavin Newsom (D) signed AB 2273, the California Age-Appropriate Design Code Act into law, which is scheduled to go into effect July 1, 2024. A non-comprehensive summary of significant elements of the Act, including the *NetChoice v. Bonta* lawsuit challenging it, follows:

Covered Entities: Who does this law apply to?

- "Child" or "Children": a consumer or consumers who are under 18 years of age.
- "Online Service, Product, or Feature": businesses that develop and provide online services, products, or features that children are likely to access. Businesses not included under this definition are broadband internet access services and telecommunications services.

Key Definitions: How does the bill define terms key to successful compliance?

- "Likely to be accessed by children": means it is *reasonable* for a business to expect that the online service, product, or feature would be accessed by children based on several factors: if (A) it is directed to children as defined by the Children's Online Privacy Protection Act; (B) it is determined to be routinely accessed by a significant number of children; (C) its advertisements are marketed to children; (D) it is substantially similar or the same as another product or service "routinely accessed" by a large number of children; (E) it has design elements that are known to be of interest to children, such as cartoons, music, and celebrities who appeal to children; or (F) a significant amount of its audience is determined, based on internal company research, to be children.
- "Data Protection Impact Assessment": a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online service, product, or feature at issue that arises from the provision of that online service, product, or feature.

Data Protection Impact Assessments: What is required?

- Before any new "online services, products, or features" are offered to the public, the business must complete a "Data Protection Impact Assessment" for any online service, product, or feature "likely to be accessed by children" and maintain documentation of this assessment.
- The assessment must identify the purpose of the online service, product, or feature, how it uses children's personal information, and the risks of material detriment to children that arise from the data management practices of the business.
- The assessment must address eight different requirements, including whether the design of such services could lead to children experiencing or being targeted by harmful contacts, whether algorithms used by the service could harm children, and whether the service uses system design features to increase, sustain, or extend the use of the online product by children such as rewards for time spent and notifications.

Business Obligations: What do digital services have to do in order to comply?

- They must configure all default privacy settings offered to the 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.
- They must provide privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access the online service.
- They must complete a Data Protection Impact Assessment before implementing any new online services, products, or features, and must maintain documentation of this assessment.
- They must not use personal information, if the end user is a child, for any reason other than for which the personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

Implementation: How is this being enforced and by whom?

This law authorizes the state Attorney General to seek an injunction or civil penalty against any business that violates its provisions. The law would hold violators liable for a civil penalty of not more than $2,500 per affected child for each negligent violation, or not more than $7,500 per affected child for each intentional violation. There is no general cap on how much a business could be liable for. A district court granted a preliminary injunction that enjoined the enforcement of the Act in September 2023, and the state Attorney General appealed in October 2023.

Impact: What will the internet look like after this law goes into effect and is implemented by digital services?

This prescriptive approach significantly alters the current harmonious nature of the web, limiting the ease with which one can navigate between websites. It mandates covered entities to require users to reveal highly sensitive information before they can access a service, including requiring the presentation of an ID card or license, potentially containing their address, height, weight, and other personally identifiable information. In addition to discouraging users from visiting any site or online service, the mandate imposes heavy costs for businesses that must either create a new compliance program or feed users' data into costly and untested third-party products to conduct any online business.

This approach also normalizes for users (specifically minors new to the internet) that revealing sensitive personal information is a normal and appropriate thing to do before being allowed to read content, and this type of socialization and technological infrastructure would likely force companies to collect, manage, and verify more sensitive personal information than businesses want to collect, and more information than users want to give. Access to protected speech should not be conditioned upon disclosing personally identifiable information as a matter of course.

Policymakers stated that the goal of implementing age verification requirements is to give minors "extra protection" from a website's practices. However, the law paradoxically could introduce more risks by requiring covered entities to collect and store additional data in the name of compliance. This creates an incentive to simply prohibit minors from using digital services rather than face potential legal action for non-compliance. Consequently, this law could produce barriers for young adults using the internet for education or expression purposes, and inhibit their ability to learn how to navigate the internet while maturing their digital skills. Such skills are key to the personal and professional success for many adults in a society that increasingly relies on and uses digitally connected services.

Conversely, a business could also be forced to treat every user as if they were a minor, drastically limiting the user experience, including not allowing any users to comment on posts or speak on sensitive topics. This, in turn, creates a chilling effect on speech as there is an inability to anonymously or pseudonymously post online criticisms, critiques, or comments, including whistleblowing. Thus, while trying to address one issue, such an approach could produce a host of other problems.

Additional Resources:

- CCIA blog post on First Amendment Challenges to Age-Gating Mandates
- CCIA amicus brief in *NetChoice v. Bonta*