Articles + Publications | May 13, 2024

Maryland Enacts Age Appropriate Design Code

WRITTEN BY

Kim Phan | Laura Hamady | Marnishia Jernigan

On May 9, Maryland became the second state to enact an (AADC), the Maryland Kids Code, alongside the Maryland Online Data Privacy Act (MODPA) — Maryland's first comprehensive data privacy bill. Maryland's AADC follows California's Age-Appropriate Design Code Act (CAADCA), which similarly seeks to protect children's online privacy by imposing certain requirements, including a general duty to act in a manner consistent with the best interests of children, on online platforms reasonably likely to be accessed by individuals under the age of 18.

Maryland's AADC will take effect on October 1, 2024, and will require entities offering online products likely to be accessed by children to complete data protection impact assessments (DPIA) by April 1, 2026.

Applicability

The AADC applies to for-profit legal entities that collect consumers' personal data and meet certain financial or data handling thresholds, including (1) annual gross revenues in excess of $25 million; (2) buying, receiving, selling, or sharing the personal data of 50,000 or more consumers, households, or devices annually; or (3) deriving at least 50% of its annual revenues from the sale of consumers' personal data. Because the definition of "covered entities" expressly includes businesses organized for the "financial benefit of its shareholders or other owners," certain not-for-profit organizations — such as trade associations — may also fall within the scope of the AADC. The AADC specifically applies to online products and services reasonably likely to be accessed by individuals under 18.

Obligations Under Maryland's AADC

Under the AADC, covered entities must adhere to various obligations, including configuring default privacy settings to the highest level, designing age-appropriate experiences for children based on set age ranges, providing easily accessible tools to allow children to report privacy concerns, and providing privacy notices in language clear enough for children to understand. Covered entities are also required to prepare a data protection impact assessment (DPIA) for any online product subject to the law. The DPIA must identify the product, its use of children's data, and whether the product design is in the best interests of children. Additionally, covered entities are prohibited from selling the personal information of children. Covered entities are also prohibited from each of the following unless strictly necessary to provide the product or service (1) collecting sensitive personal information from children — such as data on ethnicity, religion, health, sexual orientation, precise location, biometrics, or immigration status; (2) tracking the location of children; or (3) using children's personal data to estimate the age of a child.

These requirements overlap significantly with MODPA, which also (1) requires companies to conduct and

document “on a regular basis,” a data protection assessment for each data processing activity and algorithm which might present a heightened risk of harm to a consumer; (2) imposes significant data minimization requirements; (3) prohibits companies from processing the personal data of a consumer for purposes of targeted advertising or selling the personal data of a consumer where the company “knew or should have known that the consumer is under the age of 18 years”; and (4) imposes stricter regulations on “sensitive data,” including data related to ethnicity, religion, health, sexual orientation, precise location, biometrics, or immigration status.

Enforcement Rights

The state attorney general (AG) is granted exclusive authority to enforce violations under the AADC. Failure to comply with the AADC could result in fines or penalties up to $2,500 per affected child for negligent violations, and $7,500 for intentional violations.

Like MODPA, the AADC expressly incorporates Maryland’s Unfair, Deceptive, or Abusive Acts or Practices (UDAP) law. Each UDAP violation may incur a civil penalty of up to $10,000 for each violation, and up to $25,000 for each repeated violation. In addition to civil penalties, a person who commits a UDAP violation is guilty of a misdemeanor and is subject to a fine of up to $1,000 or imprisonment of up to one year, or both.

Exemptions

Certain online products are expressly exempted from the AADC’s requirements, including telecommunications services, physical products sold and delivered by online retailers, and broadband internet access services. There are also exemptions for certain types of data, including de-identified data and publicly available information.

Constitutional Challenges

Maryland’s AADC has faced opposition from groups, such as NetChoice, a tech industry trade association representing Amazon, Google, Meta, and TikTok, which has successfully sued to halt children’s online privacy or social media restrictions in several states, including the CAADCA, arguing that the laws violated its members’ constitutional rights to freely distribute information.

In *NetChoice v. Bonta*, NetChoice sued the California AG seeking to halt enforcement of the CAADCA on several grounds, including allegations that the law violates the First Amendment. The U.S. District Court for the Northern District of California preliminarily enjoined the enforcement of the CAADCA in September 2023, holding that it “likely violates the First Amendment.” The court found that the state had not met its burden of demonstrating that the DPIA requirement, age estimation restriction, high default privacy settings, and age-appropriate policy language requirements actually addressed the harm they sought to cure: protecting children’s online safety.

NetChoice’s objections to Maryland’s AADC are based on similar grounds. NetChoice argues that the AADC impinges on companies’ rights to freely distribute information as well as the rights of minors and adults to freely obtain information. Maryland legislators have responded to these objections with assurances that they have worked with constitutional experts to amend the AADC to address free speech concerns, resulting in a bill that they allege is “better adapted to the first amendment jurisprudence and the American legal ecosystem.” Key changes include a clear definition of the “best interests of the child” standard, the inclusion of a reasonableness

standard to the term “likely to access,” and realigning the DPIA requirement to focus on the product’s compliance with the duty to act in the best interests of children.

Despite these differences, some provisions of Maryland’s AADC remain similar to challenged portions of the CAADCA, such as requiring high default privacy settings for children and requiring covered entities to provide their privacy policies in language that is concise and capable of being understood by children. These provisions may be subject to additional constitutional challenges in the future.

Key Takeaways

Companies that meet the AADC’s data handling and revenue thresholds and offer online products to consumers in Maryland should determine whether their products are reasonably likely to be accessed by children. For each product reasonably likely to be accessed by children, companies should be prepared to provide a DPIA by the deadline and further assess their compliance with the statute. This will likely require an assessment of product design and implementation of additional features aimed at children who may be using the products.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber