



December 4, 2024

Maryland Is The New State To Watch When It Comes To Data Privacy

by Gary Kibel

There are now 19 states that have enacted comprehensive consumer data privacy laws, eight of which are currently in effect.

When talk turns to the most impactful of these state privacy laws, the conversation usually starts and stops with California. However, recent developments should alter that conclusion.

The Maryland Online Data Privacy Act (MODPA) takes effect on October 1, 2025. And the Maryland Age-Appropriate Design Code (AADC) is already in effect as of October 1, 2024.

Taken together, the MODPA and AADC may make Maryland the most challenging state for compliance by the digital media industry.

Maryland Online Data Privacy Act

MODPA has a number of provisions that go far beyond the comprehensive consumer privacy laws currently enacted in other states, including the California Consumer Privacy Act (CCPA).

Data minimization – Under MODPA, a business is required by law to limit its collection of personal data to that which is “reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains.”

While such data minimization is a concept promoted by the Federal Trade Commission and other regulators, MODPA strictly codifies this concept.

These restrictions will have a major impact on the ad tech industry’s data-gathering practices. Retargeting pixels operating in the background of a website to collect data for behavioral advertising, profiling or even measurement and analytics are all things that may not be considered “requested” by the consumer.

Prohibition on selling sensitive data – Many new state privacy laws require a business to secure the consent of a consumer in order to collect sensitive data, and the business must provide the consumer with the right to opt out of the sale of such data.

MODPA states that, except as strictly necessary to provide or maintain a specific product or service requested by the consumer, the business may not sell sensitive data – full stop!

Even if the consumer consents and swears on a stack of Bibles that you may sell their sensitive data, a business may not do so under MODPA. Sensitive data is defined to include data revealing racial/ethnic origin, religious beliefs, health data, sexual orientation, children's data and precise geolocation.

Rarely have we ever seen a privacy law that so discounts a consumer's consent. This outright prohibition is very unique among the new state laws.

Maryland Age-Appropriate Design Code

Similarly, many companies are overlooking the AADC, which is currently in effect. This law impacts several marketing business practices and how platforms treat children and adults.

Who is a child – Under AADC, a child is defined as anyone under the age of 18. Few privacy laws have set the age bar so high. Age 13 or 16 are more common.

Best interests of the child – If an online service is reasonably likely to be accessed by a child, the provider may only process personal data if doing so is in the best interests of the child.

The commonplace phrase “best interests” has a specific definition under the AADC, which prohibits actions, such as causing psychological or emotional harm to a child, intrusions upon privacy and discrimination based on a child's demographics.

Basically, a business needs to consider what is best for the child before considering what is best for the business.

Default privacy settings – Any online service that is reasonably likely to be accessed by a child must configure all default privacy settings to the highest level of privacy. This could prove to be the most impactful provision of the AADC.

Consider a website's consent management platform. By default, all options for data collection will likely need to be turned off for anyone under the age of 18.

As with any law, there are exceptions to these provisions and areas that require closer scrutiny. However, at this time, it may be challenging to engage in any behavioral advertising with users under the age of 18 in Maryland.

Fortunately, there are 49 other states out there. Here's hoping they don't follow Maryland's lead.



Gary Kibel is a partner in the Privacy, Technology + Data Security Practice Group of Davis+Gilbert LLP. He may be reached at gakibel@dglaw.com or 212 468 4918.

