State of Maryland
OFFICE OF THE ATTORNEY GENERAL

OAG Privacy Legislation Enforcement Status Report - Maryland Online Data Privacy Act

Requested in the Joint Chairmen's Report on the Fiscal 2026
State Operating Budget and the State Capital Budget
and Related Recommendations

Prepared by:

CONSUMER PROTECTION DIVISION
OFFICE OF THE ATTORNEY GENERAL

Submitted to the Senate Budget and Taxation Committee and
House Appropriations Committee

September 1, 2025

This report was produced in response to the request of the Senate Budget and Taxation Committee and House Appropriations Committee that the Office of the Attorney General (OAG) "submit a report on the status of implementation and enforcement of Chapters 454 and 455" from the 2024 Session,[1] which codify the Maryland Online Data Privacy Act (MODPA).[2] Since MODPA, which empowers consumers with greater control over their personal data, does not go into effect until October 1, 2025, this report provides a blueprint for implementation and outlines potential enforcement plans.

Background

The Consumer Protection Division

The Consumer Protection Division (the "Division") is responsible for a wide range of activities, including the protection of the privacy of Maryland consumers. The Division receives notice of and investigates data breaches pursuant to the Personal Information Protection Act (PIPA).[3] PIPA requires companies that collect personal information to protect it with reasonable security measures and obligates them to notify the OAG and consumers in the event of a breach. The number of breach notices received by the Division has increased dramatically over the years – in 2019, we received fewer than 1,000 breach notices but in 2023, we received over 1,500 breach notices affecting more than 3 million Marylanders.

In addition to receiving notices and tracking data breaches that impact Maryland consumers, the Division responds to consumer inquiries about data breach notices, advises consumers about mitigating the risks of identity theft, and conducts public education workshops.

On the enforcement side, primarily working with multistate partners, the Division has investigated breaches and negotiated settlements that set robust data security standards. These settlements include high-impact breaches such as Equifax, Uber, Target, Experian/TMobile, and Marriott, the investigations of which the Division helped to lead. The Division continues to investigate breaches that have a high impact on Marylanders based on numerous factors including scope, severity, and sensitivity of the personal information that was breached.

Until now, the Division has relied upon the Consumer Protection Act (CPA) to address consumer privacy violations. For example, in 2013, Maryland was part of a settlement with Google Streetview for gathering emails, passwords, and other private information from wifi networks that were not password protected. That same year, we also concluded another multistate investigation of Google that was led by the Division regarding misleading statements the company made regarding its placement of cookies when consumers used its Safari browser. In 2014, OAG conducted an investigation of Snapchat for misleading consumers about the ability to capture, save, and disseminate messages sent using the Snapchat app and entered into a Maryland-only settlement to address the issue. More recently, Maryland joined a multistate

[1] Joint Chairmen's Report, 2025 Session at 14.
[2] Md. Com Law §§ 14-4701, *et seq*. (eff. Oct. 1, 2025).
[3] *See* Md. Com Law §§ 14-3501, *et seq*.

settlement with Google over its location tracking practices and filed a multistate lawsuit against Meta for violations of the Children's Online Privacy Protection Act.

These CPA-focused privacy investigations have been handled by attorneys in the Division's General Enforcement unit. To date, in most cases, we have capitalized on the multistate investigation format; by partnering with other states we have been able to conduct investigations with limited resources. As other states expand their privacy and data security staffing and are increasingly able to conduct independent investigations, however, there may be fewer opportunities for coordination in the future.

The Maryland Online Data Privacy Act

In 2024, Maryland became the 19^{th} state to pass a comprehensive consumer privacy law. The Maryland Online Data Privacy Act goes into effect on October 1, 2025. MODPA provides Maryland residents with more control over their personal data and imposes restrictions on the ways that companies can collect, process, or sell that data.

MODPA applies to any individual or entity that conducts business in Maryland or that provides products or services to Maryland residents if, during a calendar year, that individual or entity controls or processes the personal data of (1) at least 35,000 Maryland residents; or (2) at least 10,000 Maryland residents *and* derives 20% of annual gross revenue from the sale of personal data. The individuals or entities that fit that description are called "controllers."

MODPA empowers Maryland residents with rights over their personal data and establishes privacy protection requirements for businesses that process personal data. Specifically, Maryland residents have the right to: access data that companies hold on them, correct personal data that is inaccurate, request that companies delete their personal data, and opt-out of processing of personal data for targeted advertising, the sale of personal data, and profiling in furtherance of automated decisions that produce legal effects.

Like other state comprehensive privacy statutes, under MODPA, controllers are obligated to notify consumers when they collect personal data, minimize the data they collect, and provide easy opt-outs for consumers who request it. They are also prohibited from selling sensitive personal data. Controllers will be required to conduct data protection assessments that analyze how they use certain types of personal data.

A violation of MODPA is considered a violation of the Consumer Protection Act.[4] As such, entities may face civil penalties up to $10,000 per violation for a first offense or $25,000 per violation for repeated violations of the law. The Consumer Protection Division may also impose other remedies pursuant to the Consumer Protection Act including restitution, disgorgement, and injunctive relief. MODPA lacks a private right of action and enforcement solely falls to the Attorney General.

During the legislative hearings on MODPA, the Attorney General emphasized the need for enforcement resources, especially given the lack of a private right of action. MODPA is a

---

[4] Md. Com. Law § 14-4713 (eff. Oct. 1, 2025).

complex statute that requires staff with specialized expertise, technical capabilities, and the ability to investigate large, well-funded companies. Unfortunately, no additional staffing or budget allocations were included when MODPA was enacted.

Other states of smaller size that passed comprehensive data privacy laws established or expanded units dedicated to investigating and prosecuting data breach and consumer privacy violations. For example, following the passage of the Oregon Consumer Privacy Act, the Oregon OAG created a privacy unit consisting of three attorneys, one policy analyst, and a technology-oriented research analyst who works full-time on privacy and data security.[5] With the passage of the Connecticut Data Privacy Act, the Connecticut OAG expanded its privacy unit to consist of six attorneys and an in-house technical expert.[6] Similarly, Delaware added two attorneys and two full-time staff to enforce the Delaware Personal Data Privacy Act.[7] Presently, the Division must enforce MODPA using existing staff within its General Enforcement Unit. Even if the Division devoted its entire General Enforcement Unit to data privacy matters—such that, outside of several dedicated units[8] the Division would handle only Consumer Protection Act cases involving privacy and ignore the rest of the marketplace—it would still have fewer resources dedicated to privacy and data security than Connecticut.

Legal Authority

MODPA augments the Division's authority to protect the privacy of Maryland consumers pursuant to a number of existing statutes including:

- *The Consumer Protection Act*, Md. Code Ann. Com. Law § 13-101, *et seq*., prohibits unfair, abusive, or deceptive trade practices.
- *The Personal Information Protection Act*, Md. Code Ann. Com. Law § 14-3501, *et seq*., requires businesses to protect the personal information they collect using reasonable data security measures and to notify the OAG and consumers if they suffer a breach.
- *The Online Child Safety Act*, Md. Code Ann. Com. Law § 14-3701, *et seq*. requires internet access providers to offer parental controls that allow parents to restrict access to certain websites.
- *The Genetic Information Privacy Act*, Md. Code Ann. Com. Law § 14-4401, *et seq*., requires companies that offer direct-to-consumer genetic testing to obtain consent before collecting, using, or disclosing genetic data and maintaining genetic data securely.
- *The Age-Appropriate Design Code Act*,[9] Md. Code Ann. Com. Law § 14-4801, *et seq*., was passed in 2024 and requires companies whose online products or services target

[5] Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months (March 2025) available at https://www.doj.state.or.us/wp-content/uploads/2025/03/OCPA-Six-Month-Enforcement-Report.pdf.
[6] Report to the [Connecticut] General Assembly's General Law Committee (2024), available at https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.
[7] Fiscal Note (Revised), House Bill No. 154, Delaware, 152nd General Assembly, May 22, 2023.
[8] The Division also has units with dedicated funding that handle cases related to housing, finance, and health.
[9] Section 14-4806 went into effect on October 1, 2024. The remainder of the Age-Appropriate Design Code Act will go into effect on April 1, 2026. The statute is currently the subject of litigation filed by NetChoice that the OAG is defending.

children under the age of 18 to assess the risks to children, and to implement measures to mitigate those risks.

Privacy Enforcement

While it is challenging to anticipate the specific types of violations that may occur, privacy violations are distinct from other consumer protection issues in that they often do not manifest in consumer-facing conduct. Instead, they occur within data collected by large enterprises across complex networks, making their presence difficult to detect. Consequently, they are less likely to be recognized by consumers, often do not give rise to formal complaints, and typically require sophisticated investigative efforts to uncover. Enforcement of a statute such as MODPA would typically involve proactive sweeps of policies and data processing activities along with monitoring of emerging technologies and new business practices for potential risks and violations. Ultimately, it would involve the examination of complex data sets to determine whether data is being collected or used in a manner that violates MODPA. These investigations are highly technical and must be conducted by attorneys, investigators, and technologists with the requisite expertise.

Because MODPA provides consumers with new rights, public education is also critical to helping consumers understand and implement those rights and for businesses to understand their obligations. Public awareness could be aided with statewide privacy campaigns and privacy-literacy workshops, as well as online resources including FAQs and online toolkits for both business and consumers.

The OAG's fiscal request attached to MODPA provided for a bare-bones privacy unit consisting of 4 additional staff, including attorneys, technologists/investigators, and support staff, as well as technical resources. In the absence of budgetary constraints, this was the minimum number of staff anticipated for meaningful enforcement of MODPA by itself. This estimate was developed after reviewing the resources that other state OAGs dedicated to privacy and data security enforcement and evaluating existing staffing and resource allocation. In addition to personnel, enforcement of MODPA requires IT infrastructure, funding for public education campaigns, and compliance and audit tools.

Rollout Plans

Given that the passage of MODPA did not come with corresponding resources, the Division intends to use existing staff, where available, from the General Enforcement Unit of the Division to conduct investigations into violations of MODPA. Currently, the Division has a single attorney who has the necessary expertise and certifications to conduct privacy investigations and has no technologists. Using existing staffing, the Division will be limited to a portion of this attorney's time with some support from investigators who lack specialized knowledge.

With limited resources, the Division will have to select the cases it pursues judiciously. Any contemplated privacy case will be weighed against other potential matters using a lens of scope and severity of the harm, the vulnerability of the population impacted, and the ability to effectuate broad-based impact. Difficult decisions may have to be made. The Division will focus on high-impact cases and, where possible, will seek to coordinate with other state attorney general offices in order to further leverage its resources. Public education and outreach will be limited to select materials for website publication such as FAQs and factsheets that will be updated less frequently. The Division will modify its existing complaint portal to identify privacy-related complaints and direct them appropriately. Although the Division will seek to be vigilant for privacy violations, there will be limited to no proactive sweeps or investigations.

Preparing for Implementation

Using the roadmap outlined above for enforcement with limited resources, the Division is preparing for MODPA to go into effect by:

- Updating the consumer complaint portal to ensure that Maryland residents can flag complaints they believe relate to MODPA so that the appropriate staff can review and respond to these complaints as well as track the number of complaints received for potential enforcement actions;
- Creating MODPA-related materials for consumers and businesses that will be posted on the OAG's Consumer Protection website. These materials will highlight key components of MODPA for consumers and businesses as well as provide resources. The information may be supplemented as the Division becomes aware of common issues or questions as the law goes into effect. The OAG may also issue relevant consumer alerts from time to time;
- Developing internal training to aid consumer hotline staff and mediators in responding to MODPA-related concerns; and
- Speaking on panels at local conferences to explain MODPA to businesses, lawyers, and technology professionals in the region.

In the absence of additional resources, the Division will make every effort to educate the business community and consumers about MODPA's requirements and will use MODPA as one of the tools to address privacy-related consumer issues. With dedicated enforcement resources, however, the Division could take a more proactive approach to ensuring that MODPA achieves its intended legislative objectives.