STATE PRIVACY & SECURITY COALITION

February 24, 2026

The Honorable Pamela Beidle, Chair
The Honorable Antonio Hayes, Vice Chair
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

RE: SB504 - Data Privacy

Chair Beidle, Vice Chair Hayes, and Members of the Committee:

The State Privacy & Security Coalition (SPSC), representing over 30 companies and seven trade associations across the retail, telecommunications, technology, automotive, healthcare, and payment card sectors, appreciates the opportunity to provide testimony on Senate Bill 504.

SPSC understands the Legislature's concern regarding the use of personal data in ways that may expose individuals, including immigrant communities, to unintended consequences. We share the view that certain categories of personal data warrant heightened protections, particularly where misuse could undermine consumer privacy or result in uses that extend beyond consumers' reasonable expectations. Maryland has already enacted the Maryland Online Data Privacy Act, which includes restrictions on the sale of all sensitive data, including data such as precise geolocation information and data revealing citizenship or immigration status. We respectfully approach SB 504 with recommendations intended to help ensure the legislation achieves its objectives in a clear, targeted, and workable manner.

I. THE LEGAL PROCESS EXCLUSION AMENDMENT WOULD BENEFIT FROM A KNOWLEDGE STANDARD

Section 14-4712(a)(2) of the Maryland Online Data Privacy Act establishes a legal process exclusion that permits controllers and processors to disclose personal data when necessary to comply with civil, criminal, or regulatory inquiries, investigations, subpoenas, or summonses issued by governmental authorities. Legal process exclusions serve an important function in modern privacy law by ensuring that companies can comply with valid legal obligations while maintaining appropriate safeguards for personal data. SB 504 amends that exclusion to prohibit compliance with legal process that pertains solely to immigration enforcement.

We understand the importance of the issue the Legislature seeks to address through this provision and are working with our members to identify a constructive path forward. At the same time, the proposed language puts businesses in the legally precarious position of navigating conflicting federal and state laws. At a minimum, we are concerned that the amendment does not account for whether the responding entity has knowledge of the request's underlying purpose, which unnecessarily exacerbates the risks associated with the provision.

Companies routinely receive legal process from federal, state, and local authorities that identifies the information sought but does not disclose investigative purpose or enforcement classification. Organizations are expected to assess the validity of legal process based on legal sufficiency rather than independently determining the government's intent. As a result, controllers and processors may not have visibility into whether a request relates solely to immigration enforcement or to other lawful investigative activities.

Absent a knowledge qualifier, entities acting in good faith to comply with facially valid legal process may face uncertainty regarding how to interpret and apply the provision. Legal exposure could arise even where the responding entity had no way of knowing the request pertained solely to immigration enforcement. Providing clarity regarding when the restriction applies would help ensure consistent application.

To address that concern, SPSC respectfully recommends revising the provision as follows:

> **Section 14–4712.**
>
> **(a) Nothing in this subtitle may be construed to restrict a controller's or processor's ability to:**
>
> **(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, State, local, or other governmental authority, EXCEPT TO THE EXTENT THAT *A CONTROLLER OR PROCESSOR KNOWS* AN INQUIRY, AN INVESTIGATION, A SUBPOENA, OR A SUMMONS PERTAINS SOLELY TO IMMIGRATION ENFORCEMENT."**

Incorporating a knowledge standard would not alter the core prohibition or narrow the Legislature's intention to prevent the disclosure of personal data in response to requests made solely for immigration enforcement purposes. Rather, such clarification would ensure the restriction applies in circumstances where a controller or processor has clear awareness of the request's purpose. Controllers and processors would remain prohibited under Maryland law from knowingly responding to requests made solely for immigration enforcement, preserving the Legislature's intent.

Finally, implementation of the provision will require controllers and processors to update procedures for reviewing and responding to legal process. Because legal process often does not specify investigative purpose, organizations will need time to integrate the new standard into existing review workflows and ensure requests are handled consistently. Providing additional time will support effective and orderly implementation of the amended law. SPSC therefore recommends extending the effective date by six months, from July 1, 2026, to January 1, 2027.

II. THE BILL'S RESTRUCTURING OF THE "SENSITIVE DATA" DEFINITION WARRANTS ADDITIONAL CLARIFICATION

SB 504 alters the statutory definition of "sensitive data" by redesignating the existing definition as "sensitive attribute" and introducing a new definition at subsection (hh). Under SB 504, "sensitive data" would include personal data that contains a sensitive attribute, as well as personal data processed "for the purpose of identifying a sensitive attribute." That revision expands the statutory scope beyond personal data that directly reveals a sensitive characteristic to also include personal data based on how it may be processed.

By defining sensitive data based on processing purpose, subsection (hh) shifts the statutory trigger from the nature of the data to the characterization of processing activities. Because heightened statutory obligations attach to sensitive data under Maryland law, SB 504's proposed language makes it less clear when those obligations apply. As a result, identical personal data could be subject to different statutory treatment depending on how processing activities are characterized, rather than based on whether the data reveals or indicates a sensitive characteristic.

Maryland's existing privacy law relies on objective criteria to determine when heightened protections apply. Other comprehensive privacy laws similarly address inferred sensitive characteristics while preserving objective statutory triggers tied to whether data reveals or indicates a sensitive characteristic. The Colorado Privacy Act Regulations, for example, provide that sensitive data includes "inferences made by a controller based on personal data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status."[1] Incorporating inference language in that manner ensures protections apply when sensitive characteristics are actually identified or indicated, without altering the underlying statutory trigger.

Accordingly, SPSC respectfully recommends removing subsection (hh) and incorporating Colorado's targeted inference language directly into subsection (gg). Specifically, subsection (gg) should include an additional provision stating as follows:

> **(gg)(5) "Sensitive data" includes inferences made by a controller based on personal data, alone or in combination with other data, which are used to indicate any of the sensitive data categories identified in subsections (gg)(1) through (gg)(4).**

[1] *See* Colo. Att'y Gen., Colorado Privacy Act Rules, 4 Colo. Code Regs. § 904-3, Rule 2.02 (effective Dec. 1, 2025), https://www.sos.state.co.us/CCR/DisplayRule.do?action=ruleinfo&ruleId=3396&deptID=11&agencyID=11&deptName=Department%20of%20Law&agencyName=Attorney%20General-Consumer%20Protection%20Section&seriesNum=4%20CCR%20904-3.

The inclusion of outcome-based inference language within subsection (gg) would ensure that derived sensitive characteristics receive the same protections as directly collected sensitive data. Sensitive characteristics, whether directly collected or inferred, would remain fully protected under Maryland law. Preserving Maryland's existing definition while incorporating targeted inference language would also maintain clear statutory triggers and support consistent and predictable compliance and enforcement.

III. THE DEFINITION OF "PRECISE GEOLOCATION DATA" SHOULD NOT BE MODIFIED

Across the 20 states that have passed comprehensive privacy legislation, the definition of "precise geolocation data" is one that is virtually identical across all statutes. The key to this definition is that it is tied ***to the consumer***, so that the consumer's personal data receives heightened protections. Extending this to mobile devices and vehicles, neither of which are necessarily tied to a consumer, could significantly expand the scope of how businesses must understand the requirements of this law.

The definition of "personal data" is critical here because it is data that is "linked or can reasonably linked to an identified or identifiable consumer." That is the core definition upon which the entire law is based. Implicit in this definition is that it covers ***all*** personal data – whether that is data attached to a mobile device, an automobile, a smart device, etc. Moving beyond this definition for one data element, for particular devices like mobile devices or vehicles, creates unnecessary confusion if the goal is to ensure those data types are already covered by this statute.

IV. THE BILL'S REVISED DEFINITION OF PUBLICLY AVAILABLE INFORMATION RAISES IMPORTANT CONSTITUTIONAL AND IMPLEMENTATION CONSIDERATIONS

SB 504 revises the definition of publicly available information by providing that information obtained from government records qualifies as publicly available only when processed in accordance with any restriction or term of use imposed by the governmental entity. The amendment appears to reflect the Legislature's effort to address how personal information contained in government records may be used after disclosure, particularly where public records include sensitive personal details.

Importantly, the First Amendment protects the right to collect, use, and disseminate truthful information lawfully obtained from public records. The U.S. Supreme Court has recognized that the government may not restrict the publication of lawfully obtained truthful information absent a state interest of the highest order. *See, e.g.*, *Florida Star v. B.J.F.*, 491 U.S. 524, 532-33 (1989) (holding that the First Amendment protects publication of truthful information obtained from publicly released government records); *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 102 (1979) (reasoning that governmental attempts to restrict the publication of truthful information "seldom can satisfy constitutional standards."). Restrictions on the use or dissemination of lawfully obtained information also implicate core constitutional protections because the creation and dissemination of information constitute protected speech. *See Sorrell v. IMS Health*

Inc., 564 U.S. 552, 570–71 (2011) (holding that restrictions on the use, disclosure, and dissemination of lawfully obtained information constitute content- and speaker-based regulations subject to heightened First Amendment scrutiny).

Lower courts applying those principles have likewise recognized that statutory restrictions affecting publicly available information must be carefully drawn to satisfy constitutional requirements. A federal district court, for example, recently held that restricting the dissemination of publicly available personal information constituted a content-based regulation of speech that could not survive constitutional scrutiny where the law burdened the use of truthful information obtained from public records. *See Jackson v. Whitepages, Inc.*, No. 1:24-cv-00080, at *24-33 (N.D.W. Va. Aug. 18, 2025) (holding that statutory restrictions on the dissemination of publicly available personal information violated the First Amendment because they were not narrowly tailored).

Publicly available government records play an important role in supporting transparency and the lawful exchange of information. Conditioning publicly available status on downstream processing restrictions may make it difficult to determine when information retains its public character, even where the information was lawfully obtained from government sources. Clarifying that lawfully obtained government records remain publicly available would ensure consistency with established constitutional principles while preserving Maryland's privacy framework and providing clear and workable statutory standards.

* * *

SPSC appreciates the Committee's consideration of SB 504 and its focus on ensuring strong and appropriate protections for Maryland residents' personal data. The issues addressed in the bill, including government requests for personal data, inferred sensitive characteristics, and the treatment of publicly available government records, raise important questions regarding how privacy protections are implemented in practice.

The recommendations outlined above are intended to ensure the statute can be applied as intended and, in a manner, consistent with Maryland's broader privacy framework. These revisions do not alter the bill's core protections. Instead, they provide clarity regarding how those protections apply, supporting consistent implementation while preserving the Legislature's policy objectives.

SPSC respectfully looks forward to continuing to work with the Committee, the bill's sponsor, and other stakeholders to ensure SB 504 achieves its intended objectives while providing clear and workable standards for implementation. We appreciate the opportunity to provide input and remain available to assist in further refinement of the legislation.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

William C. Martinez
Counsel, State Privacy & Security Coalition