TECHNET
THE VOICE OF AMERICAN INNOVATION

TechNet Mid-Atlantic | Telephone 717.585.8622
P.O. Box 203, New Cumberland, PA 17070
www.technet.org

February 24, 2026

The Honorable Pam Beidle
Chair
Senate Finance Committee
Maryland Senate
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

RE: SB 504 (Lam) - Data Privacy - Consumer Data, Public Records, and Message Switching System (Data Privacy Act)

Dear Chair Beidle and Members of the Committee,

On behalf of TechNet, I'm writing to share comments on SB 504.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 103 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

Our member companies consistently place a high priority on consumer privacy, and the technology industry is committed to privacy and security. As part of that commitment, transparency and the responsible use of data are pillars of the tech sector. TechNet understands the sponsor's concern regarding the misuse of personal data in ways that may expose individuals, including immigrant communities, to harm. We share that concern and agree that certain categories of personal data merit heightened protections. Our members have long supported targeted safeguards to address such concerns. We approach SB 504 in that same spirit and generally align with its intent.

Our first concern with SB 504 is how it amends Section 14-4712(a)(2) of the state's underlying comprehensive privacy law. Section 14-4712(a)(2) creates an exemption from the privacy law for when a controller or processor is complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental authority. SB 504, however, would create an exception to that exemption when the inquiry in question pertains solely to immigration enforcement. Our concern is that a controller or a processer

receiving lawful process from the government will not always know what the subject matter is behind the request for information. To address that concern, TechNet 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."**

Second, 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 framework 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

[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.

identified or indicated, without altering the underlying statutory trigger. We suggest 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).**

Third, 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.

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.

Finally, should the bill advance, we're requesting an extended effective date of at least a year to allow companies time to address implementation questions and develop guidance.

TechNet supports the intent of this bill – to ensure strong protections for Maryland residents' personal data. The issues addressed in the bill 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.

Thank you for your consideration of our comments. Please don't hesitate to reach out with any questions.

Sincerely,

Margaret Durkin

TECHNET
THE VOICE OF AMERICAN INNOVATION

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic