The Software Alliance

BSA

The Honorable C.T. Wilson
Room 231
House Office Building
Annapolis, Maryland 21401

March 26, 2024

Dear Chair Wilson,

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates the Maryland legislature's work to improve consumer privacy through SB541/HB567, the Maryland Online Data Privacy Act. In our federal and state advocacy, BSA works to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data.

As you advance a comprehensive consumer data privacy bill, BSA urges you to create strong privacy protections that are interoperable with other state laws. Our feedback focuses on three key issues:

- Clarifying that SB541's data minimization provision does not limit companies' ability to develop or improve products and services;
- Ensuring that SB541's data minimization provisions continue to apply to controllers, and not processors; and
- Supporting harmonization with other state privacy laws on enforcement, the role of third parties, and data protection assessments.

I. SB541 should clarify that the bill's data minimization provision does not limit companies' ability to develop or improve products and services.

While we appreciate the legislature's focus on creating privacy protections that are right for Maryland, we are concerned that SB541 creates a data minimization requirement that departs from existing state privacy laws in ways that do not provide clear benefits to consumers and may inadvertently prevent them from accessing updated and improved services. Most notably, the bill's language does not clearly account for companies' need to

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

process personal data to both improve existing products and to create new products that address future consumer needs and replace technologies that become obsolete.

SB541's data minimization provision limits the collection of personal data "to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains." This standard has the potential to significantly impact companies' ability to perform activities reasonably expected by consumers — including both improving existing products and developing new products as current technologies become outdated.

Companies need to use personal data to improve products and better serve customers. For example, banks, retailers, and other companies may use specialized software to route different customer service complaints to different internal teams. That software will work better when it has access to personal data, like the customer's account number and order information. To improve their service, a company may decide to collect new data from consumers to support new functions — like collecting the customer's city or zip code to help connect the customer to a physical bank or store location nearby that could provide additional assistance. Limiting the company's ability to collect new or additional types of information would greatly restrict its ability to deliver effective customer service and lower the quality of the customer experience.

Other state privacy laws recognize the need for companies to improve existing products and develop new products. Failing to account for these activities risks freezing existing technologies where they are today — which will not benefit consumers.

In other states, thirteen state privacy laws require controllers to limit the collection of personal data to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed." California's privacy law similarly requires that a business' "collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." In contrast, SB541 creates a new standard and does not clearly recognize that companies will need to use personal data to improve existing products and services that consumers rely on — and to develop new technologies that will benefit consumers.

Recommendation: To ensure consumers in Maryland continue to benefit from improved products and services, we urge you to adopt the data minimization standard in other state privacy laws. We also urge you to clarify that the bill does not limit companies' ability to develop or improve products and services. This can be done by adding language providing that the obligations imposed on controllers or processors by the bill does not restrict their ability to collect, use, or retain personal data for internal use to develop, improve, or repair products, services or technology.

II. SB541 should continue to apply data minimization obligations to controllers, not processors.

We appreciate that SB541's data minimization provisions (in Section 14-4607) apply to controllers, and not processors, consistent with all other state privacy laws. Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer's personal data. Indeed, all states with comprehensive consumer privacy laws recognize this critical distinction.[2] We applaud SB541 for incorporating this globally recognized distinction, and for its recognition that consumer-facing obligations like data minimization should apply to controllers, which are the businesses that determine the purpose and means of processing a consumer's data.

In contrast, we are very concerned with HB567's approach, which applies data minimization obligations to processors, upending the longstanding and widespread distinction between controllers and processors. While HB567 recognizes the importance of creating a set of obligations for controllers and a set of obligations for processors, HB567's data minimization standard provides that a controller or *processor* shall "limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains." Other parts of Section 14-4607 in HB567 similarly apply obligations designed for consumer-facing companies to processors, including limits on collecting and processing sensitive personal data. That approach disregards the roles of controllers and processors, which underpin privacy and data protection laws worldwide. Because the controller decides how and why to process a consumer's personal data, it is the entity that can effectively implement a data minimization obligation, which requires the company to revisit its decisions on how and why it collects that data in the first place. Those decisions are made by controllers — not by processors. The processor's role is instead to process data in line with the controller's instructions, which reflect the controller's choices in minimizing the amount of data it collects from consumers.[3]

Recommendation: We strongly recommend retaining SB541's approach of applying data minimization obligations to controllers — and not processors — consistent with all other state privacy laws, to avoid upending the distinction between controllers and processors.

[2] BSA | The Software Alliance, The Global Standard: Distinguishing Between Controllers and Processors in State Privacy Legislation, *available at* https://www.bsa.org/files/policy-filings/010622ctlrprostatepriv.pdf.

[3] Applying data minimization obligations to processors also undermines consumer privacy protections, rather than strengthening them. For example, a processor subject to a data minimization requirement may have to review consumer data that its business customers store on its service, to establish that it processes data only as necessary, proportionate, and limited under the law. Without such a requirement, a processor often will not review personal data that is stored on its service — and many cases, processors are contractually prohibited from reviewing this data, as part of their privacy and security commitments. Applying a data minimization obligation to processors therefore has the counterproductive result of requiring the processor to look at more data than it would otherwise — contrary to the goal of data minimization. A more privacy-protective approach, and the one taken in all state privacy laws, is to apply data minimization obligations on controllers. Controllers then engage processors in line with those limitations, so data remains protected when held by processors.

III. SB541/HB567 should promote a harmonized approach on enforcement, third parties, and data protection assessments.

In addition to SB541/HB567's data minimization provisions, there are other sections of the legislation where promoting consistency with other state privacy laws is critical. As the legislature considers SB541/HB567, we urge you to ensure that where Maryland departs from those other laws, it does so in a manner that makes a meaningful contribution to the larger landscape in protecting consumers, rather than diverging without a clear advantage for consumer privacy. Our recommendations focus on three key areas:

- *Enforcement*: SB 541/ HB 567's enforcement provisions should be refined to promote interoperability with other state privacy laws by <u>establishing exclusive enforcement authority in the state Attorney General and clarifying that nothing in the law establishes a private right of action under it or any other law</u>. Effective enforcement is important to protecting consumers' privacy, ensuring that businesses meet their obligations, and deterring potential violations. BSA supports strong and exclusive regulatory enforcement by a state's Attorney General, which promotes a consistent and clear approach to enforcing new privacy obligations. State Attorneys General have a track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. As currently written, SB541/HB567 do not explicitly provide for exclusive Attorney General enforcement.

- *Role of Third Parties*: We appreciate that SB 541/HB 567's definition of "third party" is consistent with the definition in other state privacy laws. However, there are several provisions of the legislation applying to third parties that diverge from other privacy laws in ways that conflate third parties with processors. Most notably, Section 14-4611(B)(3) of both bills provides that controllers are not required to comply with authenticated consumer rights requests if they do not "sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party <u>*other than a processor*</u>." This language is inconsistent with SB 541/HB 567's definition of "third party," which specifically recognizes that third parties do not include processors. In addition, Section 14-4607(D)(4) of both bills requires privacy notices to include the categories of third parties with which the controller shares personal data and "the <u>processing</u> conducted by each third party." But once a third party receives data from a controller, it becomes the controller of that data – and must address its processing in its own privacy notice. Additionally, Section 14-4612(D)(2) in SB541 and Section 14-4612(D) in HB567 refer to a "third-party controller or processor." We recommend revising these provisions to avoid conflating third parties with "third-party controllers" and "third-party processors." Because these sections could raise questions about the classification of controllers, processors, and third parties under the bill we encourage you to revise these provisions in line with other state privacy laws.

- *Data Protection Assessments*: Like other state privacy laws, SB 541/ HB 567 would establish an obligation for controllers to conduct data protection assessments for processing activities presenting a heightened risk of harm to consumers. BSA supports requiring data protection assessments for high-risk activities. However, under both bills, Section 14-4610(B) would require data protection assessments to include "an assessment for *each algorithm* that is used." No other state privacy law establishes this requirement, which if interpreted broadly, could become impractical to carry out in practice because companies can use a wide range of algorithms within a single product or service. Rather than assess the risks of a single algorithm in isolation, data protection assessments should require companies to look at the risk from an overall product, service, or processing activity. Additionally, as multiple states begin to require data protection assessments, promoting consistency in the scope and content of such assessments will help companies invest in strong assessment practices that can be leveraged in more than one state, instead of fragmenting risk-management and compliance efforts across jurisdictions even when those jurisdictions adopt similar substantive requirements.

* * *

Thank you for your leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Olga Medina

Olga Medina
Director, Policy

CC: Members of the House Economic Matters Committee