The Honorable Pamela G. Beidle
Miller Senate Office Building, 3 East Wing
11 Bladen St., Annapolis, MD 21401 - 1991

March 20, 2024

Dear Chair Beidle,

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates the Maryland legislature's work to improve consumer privacy through HB567/SB541, 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 ensure your efforts reflect the fundamental distinction between controllers and processors, which underpins privacy laws worldwide. **We are particularly concerned that HB567's data minimization standard upends this fundamental distinction, by applying the data minimization obligation to processors.** While we recognize the important role of data minimization in protecting consumer privacy, any data minimization provision should avoid undermining the clear distinction between controllers and processors, which is foundational to privacy and data protection laws worldwide.

We strongly recommend any data minimization standard apply only to controllers, not processors, to avoid upending the distinction between controllers and processors. We also encourage you to ensure any data minimization provision recognizes that companies need to collect personal data to continue improving their products as new consumer demands arise and technology evolves.

[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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. HB567's data minimization provision should be revised to apply to controllers, not processors.

Distinguishing between controllers and processors is a foundational aspect of privacy laws worldwide and in every state.[2] Laws that recognize these different roles better protect consumer privacy by crafting different obligations for different types of businesses based on their different roles in handling consumers' personal data. Both HB567 and SB541 appear to recognize the importance of this distinction. Both bills create a set of obligations for controllers, which are the companies that determine the purpose and means of processing consumers' personal data. Both bills also create a set of obligations for processors (sometimes called service providers), which are companies that process data on behalf of a controller and pursuant to its instructions.

HB567's data minimization provision would upend the distinction between controllers and processors by applying this obligation not only to controllers, but also to 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 would similarly apply obligations designed for consumer-facing companies to processors, including limits on collecting and processing sensitive personal data.

This approach undermines the fundamental distinction between controllers and processors and creates new risks to consumer privacy.

Applying data minimization obligations to processors disregards their role in handling consumers' personal data — which is to process that data on behalf of a controller and subject to its instructions. It is the controller that decides how and why to process a consumer's personal data. The controller is therefore the entity that can effectively implement a data minimization obligation, since minimizing the amount of data a company collects requires that 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; those instructions will reflect the controller's choices in minimizing the amount of data it collects from consumers.

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

[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.

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,[3] is to apply consumer-facing obligations like data minimization only to businesses that determine the purpose and means of processing a consumer's data. Controllers then engage processors in line with those limitations, so data remains protected when held by processors.

We strongly encourage you to revise HB567 so that any data minimization obligation applies only to controllers, not processors, consistent with all other state privacy laws.

II. Any data minimization standard should recognize that consumers benefit from improved products and services.

In addition to our concern about undermining the fundamental distinction between controllers and processors, we are concerned that the data minimization standard in both HB567 and SB541 may inadvertently harm consumers by limiting the ability of companies to improve existing products and develop new ones in response to consumer demand. This risk is present even when the bills' data minimization standard is limited to controllers.

HB567'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." Similarly, SB 541 would 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." This standard has the potential to significantly impact companies' ability to perform activities reasonably expected by consumers. Most notably, it does not clearly account for companies' need to collect data to improve existing products or to create new products that address future consumer needs.

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 physical bank or store locations 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.

---

[3] *See, e.g.*, Cal. Civil Code 1798.100(c); Colorado CPA Sec. 6-1-1308(3); Connecticut DPA Sec. 42-520(a)(1); Delaware Personal Data Privacy Act, Sec. 12D-106(a)(1); Florida Digital Bill of Rights Sec. 501.71(1)(a); Iowa Senate File 262 Sec. 7(6)(b); Indiana Senate Enrolled Act No. 5 (Chapter 4, Sec. 1(1)); Montana Consumer Data Privacy Act Sec. 7(1)(a); New Hampshire Senate Bill 255 Sec. 507-H:6(I)(a); New Jersey Senate Bill 332/Assembly Bill 1971 Section 9.a.(1); Oregon CPA Sec. 2(5); Tennessee Information Protection Act 47-18-3204(a)(1); Texas Data Privacy and Security Act Sec. 541.101(a)(1); Virginia CDPA Sec. 59.1-578(A.1).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

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 many cases, companies will need to process personal data to improve the functionality of their products and to develop new products as current technologies become outdated or obsolete.

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, HB567's 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.

In order for consumers in Maryland to continue to benefit from improved products and services, we urge you to adopt the data minimization approach in other state privacy laws and clarify that the bill does not limit companies' ability to develop or improve products and services.

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 Senate Finance Committee

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org