February 12, 2024

The Honorable Sara Love
Lowe House Office Building, Room 210
6 Bladen St., Annapolis, MD 21401

The Honorable Dawn Gile
Miller Senate Office Building, 3 East Wing
11 Bladen St., Annapolis, MD 21401

Dear Delegate Love and Senator Gile:

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates your work to improve consumer privacy through House Bill 567 (HB 567) and Senate Bill 541 (SB 541), 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. At the state level we have supported strong privacy laws in a range of states, including consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We appreciate the opportunity to share our feedback on HB 567/ SB 541. Our recommendations below focus on key priorities in the legislation: interoperability with other state privacy laws, creating obligations for processors that reflect their role of handling data on behalf of other companies, and ensuring any universal opt-out mechanisms work in practice.

[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. BSA Supports an Interoperable Approach to Privacy Legislation.

BSA appreciates your efforts to ensure that HB 567/SB 541 create privacy protections that are interoperable with protections created in other state privacy laws. Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can readily map obligations imposed by a new law against their existing obligations under other laws.

We appreciate the harmonized approach you have taken in aligning many of HB 567/SB 541's provisions with the Colorado Privacy Act and the Connecticut Data Privacy Act, which create a range of new protections for consumers. BSA supported Colorado and Connecticut's privacy laws and has supported strong state privacy laws across the country that build on the same structural model of privacy legislation enacted in both states. In particular, we support HB 567/SB 541's focus on creating new rights for consumers, creating a range of obligations for businesses that require them to handle data responsibly, and focus on consumer-facing data rather than employment data, which can raise distinct and separate privacy concerns.

We highlight four areas in which interoperability of state privacy laws is particularly important:

- *Enforcement*. We encourage you to support consistency with other state privacy laws in HB 567/SB 541's enforcement provisions by giving the state Attorney General exclusive enforcement authority. 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, HB 567/SB 541 do not explicitly provide for exclusive Attorney General enforcement.

- *Data Protection Assessments*: Like other state privacy laws, HB 567/ SB 541 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, Section 14-4610(B) of HB 567/ SB 541 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 these algorithms 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.

- *Role of Third Parties*: We appreciate that HB 567/ SB 541'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 and could result in conflating third parties with controllers and processors. For instance, Section 14-4607(D)(4) requires privacy notices to include the categories of third parties with which the controller shares personal data and "to the extent possible, how each third party may process the personal data." 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) states that "a third-party controller or processor that receives personal data from a controller or processor in compliance with this subtitle is not in violation…for the independent misconduct of the controller or processor." Section 14-4611(B)(3) also 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 other than a processor." These sections are inconsistent with HB 567/ SB 541's definition of "third party," which specifically provides that term covers "persons other than the relevant consumer, controller, processor, or affiliate of the controller or processor." Moreover, these sections could raise questions about the classification of controllers, processors, and third parties under the bill. For these reasons, we encourage you to harmonize the sections relating to third parties with those found in other state privacy laws.

- *Controller Obligations:* We are also concerned that some aspects of the obligations HB 567/ SB 541 would place on controllers in Section 14-4607(A) depart from those established under other state privacy laws. Instead, we recommend aligning the bill's approach to controller obligations with the approach of the Colorado, Connecticut, and Virginia.

II. Distinguishing Between Controllers and Processors Benefits Consumers.

We support HB 567/ SB 541's clear recognition of the unique role of data processors. 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] In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers, while all other state comprehensive privacy laws use the terms controllers and

[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.

processors.[3] This longstanding distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[4] BSA and its members applaud you for incorporating this globally recognized distinction into HB 567/ SB 541.

While the bill includes this important distinction, as noted above, we are concerned that HB 567/SB 541's provisions on third parties create uncertainty about the bill's treatment of processors. As other state laws recognize, processors are not third parties — and are subject to special rules restricting how they process data on behalf of a controller, unlike a third party. We strongly urge you to revise HB 567/SB 541's provisions on third parties and align them with the third-party provisions of the Colorado, Connecticut, and Virginia laws to avoid potential confusion about the distinct roles of processors and third parties

III. The Bill's Provisions Giving Controllers an Opportunity to Object to Processors' Use of Subcontractors Should be Revised.

As noted previously, BSA appreciates HB 567/ SB 541's clear recognition of the unique role of data processors, which process data on behalf of other companies and pursuant to their directions. While provisions in HB 567/ SB 541 robustly address the obligations of processors — which process personal data on behalf of controllers — including by ensuring they assist controllers in responding to rights requests and in implementing data security measures, Section 14-4608(A)(3)(VI) of the legislation creates significant concerns. This section provides that processors shall engage a subcontractor "*after providing the controller an opportunity to object"* and *"in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data*."

We recognize the need for a consumer's data to be protected regardless of whether they are held by a processor or a subprocessor. However, we strongly recommend a different approach: requiring processors to *notify* a controller about the use of a subprocessor and pass on their obligations to that subprocessor — but not requiring controllers have the *opportunity to object* to subprocessors. This edit is particularly important, because of the

[3] *See, e.g.*, Cal. Civil Code 1798.140(d, ag); Colorado CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Delaware Personal Data Privacy Act, Sec. 12D-102(9, 24); Florida Digital Bill of Rights Sec. 501.702((9)(a)(4), (24)); Indiana Senate Enrolled Act No. 5 (Chapter 2, Sec. 9, 22); Iowa Senate File 262 (715D.1(8, 21)); Montana Consumer Data Privacy Act Sec. 2(8,18); New Jersey Senate Bill 332/Assembly Bill 1971 (Section 1); Oregon CPA Sec. 1(8, 15); Tennessee Information Protection Act 47-18-3201(8, 20); Texas Data Privacy and Security Act Sec. 541.001(8, 23); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

[4] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which helps companies that process data demonstrate adherence to privacy obligations and helps controllers identify qualified and accountable processors. In addition, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data. For additional information on the longstanding distinction between controllers and processors – sometimes called businesses and service providers – BSA has published a summary available here.

frequency with which processors engage subcontractors to provide services requested by controllers. In many cases, processors will rely on dozens (or more) of subprocessors to provide a single service, and may need to replace a subcontractor quickly if the subcontractor is not able to perform a service due to operational, security, or other issues. Requiring that controllers have an opportunity to object slows down the delivery of services and products to consumers, without clear benefits to privacy. Instead, we believe a processor should be required to notify a controller about subprocessors and pass on obligations to subcontractors via contract, to ensure consumers' personal data remains protected.

IV. Consider Practical Issues Involved in Creating a System for Recognizing Universal Opt-Out Mechanisms.

We believe that consumers should have clear and easy-to-use methods to exercise new rights given to them by any new privacy law. Like the state privacy laws enacted in Colorado and Connecticut, HB 567/SB 541 include a clear requirement for controllers to honor a consumer's use of a universal opt-out mechanism to exercise new rights to opt out of targeted advertising or the sale of their personal data. Under Section 14-4607(F)(3)(II), controllers must honor these mechanisms no later than October 1, 2025.

If the bill retains this requirement, we strongly encourage you to focus on creating a universal opt-out mechanism that functions in practice. It is important to address how companies will understand which universal opt-out mechanism(s) meet HB 567/ SB 541's requirements. One way to address this concern is by creating a clear process for developing a public list of universal opt-out mechanisms and soliciting stakeholder feedback as part of that process, similar to the approach contemplated under the Colorado Privacy Act.[5] Focusing on the practical aspects of implementing this requirement can help companies develop strong compliance programs that align their engineering and other resources accordingly. We also encourage you to focus on recognizing a universal opt-out mechanism that is interoperable with mechanisms recognized in other states. Interoperability is essential in ensuring that any universal opt-out mechanism is workable and allows consumers to effectuate their rights across state lines.

Finally, as you consider how to ensure any universal opt-out mechanism works in practice, we recommend educating consumers about what universal opt-out mechanisms do in addition to their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer's personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser. Consumers should be aware of this and other limitations.

Thank you for your continued 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,

[5] *See* Colorado Department of Law, Universal Opt-Out Shortlist, *available at* https://coag.gov/uoom/.

Matthew Lenz
Senior Director and Head of State Advocacy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org