The Honorable Michael O. Moore
The Honorable Tricia Farley-Bouvier
Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
24 Beacon Street
Boston, MA 02133

October 21, 2023

Dear Chair Moore & Chair Farley-Bouvier,

BSA | The Software Alliance[1] supports strong privacy protections for consumers. BSA appreciates the Committee's interest in protecting consumer data privacy in the Commonwealth. In BSA's federal and state advocacy, we work 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 across the country, 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, and their business models do not depend on monetizing users' data.

As you consider advancing comprehensive consumer data privacy legislation in the Commonwealth, we would urge the Committee to consider the following priorities. Our recommendations below focus on our core priorities in comprehensive data privacy

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

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

legislation – recognizing the unique role of data processors and creating privacy protections that are interoperable with other state laws.

I. Distinguishing Between Businesses and Service Providers Benefits Consumers.

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. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction. 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 processors.[2] 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.[3] BSA urges the committee to include this distinction in consumer privacy legislation.

We believe that there are two key areas where using intentional language in legislation would significantly reduce the risk of inadvertently undermining consumers' privacy and security and create clear obligations for companies to implement.

- *Definitions*. At the outset, it is critical for any privacy law to define the different types of companies that handle consumers' personal data. Specifically, legislation should distinguish between two roles: (1) companies that decide how personal data is collected, used, shared, and stored – called "controllers" or "businesses" and (2) companies that handle personal data on behalf of those other companies – called "processors" or "service providers." All state consumer privacy laws adopt this critical distinction, separately defining "controllers" and "processors"[4] and

[2] *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); 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.

[3] 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.

[4] *See, e.g.*, 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); Oregon CPA Sec. 1(8, 15); Tennessee Information

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

California calling these roles "businesses" and "service providers."[5] Any privacy law must define both roles, so that it can impose strong – but distinct – obligations on both types of companies.

- *Role-Dependent Obligations*. Legislation should impose strong obligations on all companies to safeguard consumer's personal data – and those obligations must reflect the company's role in handling that data. For example, because controllers under 12 state privacy laws and businesses under California law decide why and how to collect a consumer's personal data, those companies are obligated to provide consumers with certain rights, such as the ability to access, correct, and delete information, and they have the obligation to seek a consumer's consent when required. If those obligations were instead placed on service providers, it would create security risks since consumers and service providers do not generally interact with each other – so consumers may be confused by a consent request sent by a service provider; service providers, in turn, may not know whether to honor consumer rights requests from individuals they don't know. All comprehensive state privacy laws therefore appropriately place consumer-facing obligations such as consent requirements and consumer rights obligations on businesses and controllers. All comprehensive state privacy laws also create a series of obligations tailored to processors, to ensure those companies handle consumers' personal data responsibly. This approach ensures that service providers are subject to strong obligations in handling consumers' personal information and helps build consumers' trust that their personal information remains protected when it is held by service providers. We are including an appendix to this letter setting out the Virginia CDPA's service provider obligations, for your reference.

II. Creating Privacy Protections That Are Interoperable

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. 13 states have now enacted comprehensive consumer privacy laws that create new rights for consumers, impose obligations on businesses that handle consumers' personal data, and create new mechanisms to enforce those laws.[6] We urge the committee to adopt privacy protections that are interoperable with protections included in other state privacy laws, which helps drive strong business compliance practices that can better protect consumer privacy.

In particular, BSA supports strong and exclusive regulatory enforcement by the Attorney General's office, which promotes a consistent and clear approach to enforcement. State

---

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.

[5] *See, e.g.*, Cal. Civil Code 1798.140(d, ag).

[6] BSA | The Software Alliance, 2023 Models of State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/us-2023-models-of-state-privacy-legislation.

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. All state privacy laws provide state attorneys general with enforcement authority,[7] and we urge the Committee to adopt a similar approach.

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,

Matthew Lenz
Senior Director and Head of State Advocacy

[7] *Id*.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Virginia's Consumer Data Protection Act
§59.1-579. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-577.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-580.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org