The Honorable Kesha Ram Hinsdale
Chair
Senate Committee on Economic Development, Housing, & General Affairs
115 State St.
Montpelier, VT 05633-5301

March 28, 2024

Dear Chair Hinsdale,

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates the Vermont legislature's work to improve consumer privacy through House Bill 121 (H.121), the Vermont 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 information — 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 H.121. While we commend the legislature's work in advancing consumer privacy legislation, we are concerned that the bill, as passed the House, departs from other state privacy laws in ways that do not provide clear benefits to Vermont's consumers. As the committee considers H.121, we urge you to ensure that where Vermont 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 below focus on key priorities in the legislation:

[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

- Supporting interoperability with other state privacy laws;
- Supporting strong and exclusive enforcement by the state's Attorney General;
- Supporting strong antidiscrimination provisions focused on unlawful activities;
- Supporting consumers' right to know through practical requirements; and
- Supporting the ability of processors to combine information in ways that benefit consumers.

I. Supporting an Interoperable Approach to Privacy Legislation

BSA appreciates the Vermont legislature's efforts to ensure that H.121 creates privacy protections that are interoperable with protections created in other state privacy laws. Privacy laws around the world need to be consistent enough that consumers can 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 taken in aligning many of H.121's provisions with the Connecticut Data Privacy Act, which creates a range of new protections for consumers. BSA supported Connecticut's privacy law and has supported strong state privacy laws across the country that build on the same structural model of privacy legislation enacted in Connecticut. In particular, we appreciate H.121'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 processors.[3] BSA applauds the incorporation of this globally recognized distinction into H.121.

II. Supporting Strong and Exclusive Enforcement by the State's Attorney General

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

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

[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 Hampshire Senate Bill 255 (507-H:1(IX, XXII); 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.

creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies.

Section 2427(a)(2) of H.121 would establish a private right of action for consumers harmed by violations of the law. In our view, a private right of action is not needed to ensure strong enforcement of a privacy law and can impede consistent enforcement of the substantive protections in a new law. Indeed, none of the states to enact a comprehensive consumer privacy law has created a private right of action for the privacy-related obligations in those laws.[4] We encourage you to support consistency with other state privacy laws in H.121's enforcement provisions by establishing exclusive enforcement authority in the state Attorney general and providing that nothing in the law establishes a private right of action under it or any other law. Effective enforcement is important to protecting consumers' privacy, ensuring that businesses meet their obligations, and deterring potential violations.

III. Supporting Strong Antidiscrimination Provisions Focused on Unlawful Activities

It is also important for H.121 to clarify the bill's antidiscrimination provisions to avoid creating uncertainty about the types of activities covered by these obligations. Section 2419(b)(3)(A) of H.121 prohibits controllers from processing consumers' personal data "in a manner that discriminates against individuals or otherwise makes unavailable the equal enjoyment of goods or services on the basis of an individual's actual or perceived race, color, sex, sexual orientation or gender identity, physical or mental disability, religion, ancestry, or national origin." BSA strongly supports the objective of this provision, and we recognize the importance of ensuring that technology is not used to discriminate. However, as currently written, this provision creates uncertainty for companies implementing a new obligation because it is not clearly tied to activities that are unlawful under state and federal laws. We encourage you to revise this provision prohibit controllers from processing personal data "in a manner that unlawfully discriminates against individuals" on the bases set out in the bill.

IV. Supporting Consumers' Right to Know through Practical Requirements

Additionally, Section 2418(A)(2) of H.121 provides consumers with a right to "obtain a list of third parties" to which the controller has transferred either the consumer's personal data or any personal data. BSA believes that consumers should have clear and easy-to-use methods for exercising new rights given to them by any privacy law. However, privacy laws should also craft those rights so that companies can implement them in practice and prioritize providing meaningful information to consumers.

We recommend focusing this provision to require controllers provide consumers with categories of third parties to whom personal data was disclosed, rather than the specific third parties. This approach ensures consumers have meaningful information about the

[4] The California Consumer Privacy Act, as amended by the California Privacy Rights Act, establishes a limited private right of action in the event of a security breach affecting a consumer's personal information but not for the privacy obligations established under the statute.

types of companies to which a controller discloses their information (e.g., marketing companies, data brokers, etc.) without requiring the controller to identify each third party by name (which can be particularly difficult for medium-sized businesses that rely on third parties to perform services that larger companies could do in-house). Disclosing names of individual companies may actually increase privacy concerns, by encouraging companies to track customer-by-customer data more closely. It also burdens consumers with identifying what type of company each third party is, since it may not be apparent from the company's name that it is a marketing company, or a data broker, etc. The California Privacy Rights Act takes this approach, requiring businesses to disclose to a consumer the "*categories* of third parties to whom the business discloses personal information."

V. Supporting the Ability of Processors to Combine Information in Ways that Benefit Consumers

Section 2421(9) of H.121 provides that a contract between a controller and processor must "prohibit the processor from combining personal data obtained from the controller with personal data that the processor: (A) receives from or on behalf of another controller or person; or (B) collects from an individual." This requirement would inadvertently impact processors' ability to combine information in routine ways that benefit consumers. Indeed, controllers may ask processors to combine personal data with other data sets, or to serve multiple businesses, for a range of purposes that benefit consumers—without monetizing consumers' data or using it for advertising. These include:

- *Providing and improving services.* Controllers may direct processors to use personal information they disclose to the processor to improve services offered to multiple businesses. For example, a controller may direct a processor to use personal information they disclose to the processor to improve services offered to multiple businesses. Services provided at scale will work better if they are improved based on data about how the service performs across different types of customers and in different scenarios; these types of improvements rely on combining data from different controllers. Those improved services will benefit not just the business customers using the service but also the individuals those businesses serve.

- *Protecting and securing services*. In many cases, processors identify cybersecurity threats and bad actors by combining information received from different controllers. For example, an email service that serves thousands of businesses may identify a bad actor attacking email accounts belonging to one business customer. However, by analyzing personal information across its services (by searching and combining elements of the underlying personal information stored on behalf of different controllers) the processor can identify other email accounts of other controllers that may be targeted by the same bad actor. That allows the processor to take steps to safeguard at-risk accounts, increasing the privacy and security of the personal data.

- *Serving businesses that enter into a joint venture.* When two businesses want a processor to act on their behalf, they can do so pursuant to a written contract. H.121's language could be read to prohibit these types of arrangements, which are an important way for businesses to share resources and expertise to better serve consumers.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

- *Facilitating research*. Processors can help entities conducting scientific research by combining multiple sets of data, at the direction of those entities and in line with privacy safeguards they have established. The resulting data could then be used to serve each of the participating entities.

It is important to ensure that controllers can direct a processor to combine information on their behalf and in line with their contract. For these reasons, we encourage you to modify this provision to allow processors to combine personal information to perform purposes specified in their contract with a controller.

* * *

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 Committee on Economic Development, Housing, and General Affairs

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org