December 6, 2021

The Honorable Ivy Spohnholz
State Capitol
120 4th Street
Room 421
Juneau, AK 99801

Dear Co-Chair Spohnholz:

BSA | The Software Alliance[1] is the leading advocate for the global software industry domestically and globally. Our members are business-to-business companies that create the technology products and services that power other companies. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and remote collaboration software. These enterprise software companies are in the business of providing privacy-protective technology products. BSA members recognize that they must earn consumers' trust and act responsibly with their personal data, and their business models do not depend on monetizing consumers' data.

In BSA's advocacy at the federal and state levels of government, we work to advance legislation that ensures consumers' rights over their personal data – and the obligations imposed on businesses – function in a world where different types of companies play different roles in handling that data. At the state level, we have advocated for strong privacy laws in a range of states, including in Virginia and Colorado, the two most recent states to enact comprehensive consumer privacy legislation.

We appreciate your focus on protecting consumers' privacy in HB 159, the Consumer Data Privacy Act, currently under consideration by the House Rules Committee, and write to provide feedback on the legislation. As set out below, our recommendations focus on improving aspects of the legislation to help ensure that all companies have meaningful obligations to safeguard consumers' personal data – and that those obligations reflect a company's role in handling consumers' personal information. Many of the suggestions below build on provisions from the recently enacted Consumer Data Protection Act (CDPA) in Virginia and the Colorado Privacy Act (CPA), both of which BSA supported.

BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

20 F Street NW, Suite 800
P 202-872-5500
W bsa.org

I. Distinguishing Between Businesses and Service Providers Benefits Consumers.

We are pleased that HB 159 separately applies to "business[es]" and "service provider[s]." We strongly support distinguishing between different types of companies that play different roles in handling consumers' personal data. Effective privacy laws worldwide reflect the fundamental distinction between service providers (sometimes called processors), which handle a consumer's personal data on behalf of other businesses, and businesses (sometimes called controllers), which decide how a consumer's personal data will be collected and used. The difference between these different types of companies is foundational not only to privacy laws across the globe, but also to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[2] Distinguishing between businesses and service providers creates clarity for consumers when acting on their rights provided in the legislation and for businesses in implementing their obligations.

However, the Consumer Data Protect Act's definition of "service provider" does not reflect the dividing line between these two different types of entities that is established in leading privacy laws worldwide. Service providers are the companies that process personal information on behalf of businesses, while businesses determine the "means and purposes" of processing personal information. Privacy laws in Virginia, Colorado, and California all recognize the same dividing line. We suggest revising the definition of service provider, so that Alaska's approach to defining these distinct entities adopts the same dividing line used in other privacy laws in the US and globally.

We urge you to amend the definition of businesses as follows:

> *"(22) "service provider" means a person* ***that processes personal information on behalf of a business in accordance with a written contract****."*

We believe that both service providers and businesses must have strong obligations under any privacy law. Those obligations must also be tailored, so that the obligations on these different types of companies reflect their different roles in handling consumers' data.

II. Service Providers Need to Use Personal Information to Provide Services to Businesses and Consumers.

As currently drafted, we have significant concerns with the bill's approach to crafting appropriate obligations on service providers. We appreciate that the limitations on service providers' use of personal information appear to be well-intended efforts to protect consumers' privacy. However, as currently written, the limits service providers' use of personal data included in HB 159, particularly in Sec. 45.49.080(a), do not account for situations in which service providers need to use personal information in ways that do not undermine consumers' privacy – and may actually benefit consumers, businesses, and service providers.

[2] For example, Virginia's CDPA differentiates between "controllers" and "processors," and California's consumer privacy law similarly recognizes the distinct roles of "businesses" and "service providers." 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 help companies that process data demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors. In addition, last year the International Standards Organization published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data.

Particularly in Sec. 45.49.080(a)(2), HB 159 restricts service providers' ability to combine personal information from different sources. Service providers need to combine personal information to help protect and secure services, improve their services, help mitigate potential biases, and serve multiple businesses at one. The following examples illustrate the need for service providers to combine personal information received from different businesses:

- *Combining personal information to help protect and secure services.* In many cases, service providers identify cybersecurity threats and bad actors by combining information received from different businesses. 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 other businesses) the service provider can identify other email accounts of other businesses that may be targeted by the same bad actor. That information allows the service provider to proactively take steps to safeguard the at-risk accounts, and to increase the privacy and security of the personal information, benefitting both the businesses that use the email service and the consumers those businesses serve.

- *Combining personal information to make services work better.* Consumers and businesses often benefit from service providers combining personal information to improve their services. For example, a service provider may use personal information provided by one business to improve a service offered to many businesses—to the benefit of both the business customers and the consumers they serve. For instance, a service provider may create software that helps businesses manage customer service complaints, including by routing consumers with complaints to the employee team responsible for handling each type of complaint. That software will work better—and be more useful to both consumers trying to resolve complaints quickly and to businesses trying to satisfy their customers—if it is designed to identify patterns in how businesses route different types of complaints. By training the software on data collected from all of the businesses that use the software (instead of just on the data of one business), the software can become more efficient and effective, helping both consumers and businesses. The need to improve services based on personal information collected across business customers is not unique—it underpins many of the services that consumers and businesses rely on today.

- *Facilitating research.* Service providers 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.

- *Combining personal information to develop AI systems and to mitigate potential biases.* AI systems are trained with large volumes of data. Their accuracy—and benefits—depend on access to large amounts of high-quality data, which service providers may process at the direction of businesses. For example, a health care business may hire a service provider in connection with developing a fitness app that analyzes a consumer's heart rate to monitor for irregularities and predict whether the person is at risk of stroke or heart disease. To make the technology as accurate as possible, the business may direct the service provider to combine heart rate data from several publicly available health databases with data collected from the company's users in order to train the AI model. Directing the service provider to combine personal information collected by that business—which might disproportionately focus on one age group or ethnicity—with personal information available

from other sources helps to mitigate against the risks of bias, benefitting both the consumers who will eventually use the service and the business customer. Regulations should not prohibit service providers from using or combining personal information for such purposes, at the direction of a business.

- *Combining personal information to serve multiple businesses at once.* There are many common scenarios in which businesses may ask service providers to combine information to provide a service to multiple businesses at the same time. We highlight two examples. First, in the case of a joint venture two businesses may jointly ask a cloud storage provider to store certain personal information together. Second, in the case of benchmarking services, consumers and businesses may seek out services that provide them context or help them understand how their activities fit into bigger trends. Consumers, for instance, may want to sign up for a program that allows their health care provider to combine their information with other sets of data, to better understand potential health risk factors. Similarly, businesses may use benchmarking services to understand industry trends in hiring and human resources management, and to identify areas in which they may need to invest additional resources. Even when these services may only provide consumers and businesses with de-identified or aggregate information, they rely on the ability to combine personal information from which they derive the data to be shared. Regulations should not limit such uses, which continue to be subject to other safeguards in the CPRA.

- *Supporting open data initiatives.* More broadly, there is increasing recognition among governments and companies of the benefits of sharing data—subject to appropriate privacy protections. For example, the United States recently enacted the OPEN Government Data Act, which makes non-sensitive government data more readily available so that it can be leveraged to improve the delivery of public services and enhance the development of AI.[3] In addition, there is broad support for voluntary information-sharing arrangements, including by seeking to develop common terms so that companies that want to share data can more readily do so.[4]

Additionally, we are concerned the provisions in Sec. 45.49.080(a)(3) and Sec. 45.49.080(b) could restrict service providers' ability to engage subprocessors. Service providers frequently engage subprocessors to provide services requested by businesses. In many cases, a service provider will rely on dozens (or more) of subprocessors to provide a single service and may need replace a subprocessor quickly if one is unable to provide service, either because of an operation issue or because of a potential security concern.

Generally, we believe the draft legislation can be improved by aligning the obligations on service providers with those in Virginia's CDPA.[5] The service provider obligations in Virginia's law are also similar to those contained in the CPA and the Washington Privacy Act, which passed that state's Senate earlier this year. Virginia's approach to service provider obligations sets out a fulsome set of responsibilities, to ensure not only that service providers handle data on behalf of businesses and pursuant to a contract, but also addresses data security obligations, requires service providers to assist controllers with consumer rights requests for data held by the service provider, requires service providers impose a duty of confidentiality on persons who process data, and requires service providers to delete or return data to the controller at the end of services,

[3] *See* Public Law No. 115-435, Title II (Jan. 14, 2019).
[4] *See, e.g.,* Linux Foundation Debuts Community Data License Agreement (October 23, 2017, referencing IBM support), https://www.linuxfoundation.org/press-release/linux-foundation-debuts-community-data-license-agreement/.
[5] *See* CDPA, Sec. 59.1-575. *See endnote for full for language.*

requires service providers to engage subprocessors pursuant to a written contract that requires the subprocessor to meet the obligations of the service provider with respect to the personal information, among other obligations. BSA supports these obligations, which we recognize are important to build consumers' trust in ensuring that their personal data remains protected when it is held by service providers.

Rather than prohibiting service providers from using and combining personal information, or allowing the Attorney General to decide the parameters of some prohibitions on service providers' use of personal information, as Sec. 45.49.080(a) would do, we urge you to create a new section in HB 159 to better incorporate the service provider obligations in Virginia's CDPA. These provisions ensure that service providers are subject to strong obligations – with meaningful limits – in handling consumers' personal data. We believe such obligations are important in building consumers trust and ensuring that their personal data remains protected when it is held by service providers.

We have set out the Virginia CDPA's service provider obligations in an appendix to this letter. We urge you to consider incorporating this approach to service provider obligations in Alaska's legislation.

III. The Attorney General Should Be Empowered to Enforce Comprehensive Consumer Privacy Legislation.

We support enforcement by the Attorney General with respect to comprehensive consumer privacy legislation. We believe that a strong, centralized approach – with the state attorney general as the exclusive enforcement authority – is the best way to develop sound practices and investment in engineering that protects consumers. 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. We also believe that if states enact new comprehensive privacy laws, the state attorney general should be provided with the tools and resources needed to carry out this mission effectively.

We are concerned enforcement under Alaska's Unfair Trade Practices and Consumer Protection Act could lead to inconsistent enforcement through private rights of action, which is harmful to consumers whose rights will be inconsistently enforced and to businesses that may face confusion regarding how to implement their obligations under HB 159. We suggest the Attorney General be given the exclusive authority to enforce the Consumer Data Protection Act and be provided with any necessary resources.

Thank you for your thoughtful approach in establishing consumer data privacy protections and your consideration of our perspective. We encourage you and your colleagues on the House Rules Committee to amend the legislation with the recommendations above and would welcome the opportunity to work with you on the Consumer Data Protection Act as it progresses through the legislative process in Juneau.

Sincerely,

Tom Foulkes
Senior Director, State Advocacy

20 F Street NW, Suite 800
P 202-872-5500
W bsa.org

Appendix

Virginia's CDPA

§ 59.1-575. 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 § 59.1-573.

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 § 59.1-576.

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.

Appendix

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 continues to adhere to a controller's instructions with respect to a g of personal data remains a processor.

20 F Street NW, Suite 800

P 202-872-5500
W bsa.org