March 28, 2023

The Honorable Floyd Prozanski
900 Court St. NE, S-413
Salem, Oregon 97301

Dear Senator Prozanski:

BSA | The Software Alliance[1] appreciates the opportunity to share our feedback on Senate Bill 619 (SB 619). BSA members support strong privacy protections for consumers. 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 advocated for strong privacy laws in a range of states and supported the consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create the business-to-business technologies that other companies use. 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' personal data.

As an initial matter, we appreciate your work in revising key aspects of SB 619 since it was first introduced. Many of the recent changes provide important clarity to companies and harmonize SB 619's requirements with existing state privacy laws. That is important because 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 your efforts to make SB 619 interoperable with protections included in existing state privacy laws, which helps drive strong business compliance practices that can better protect consumer privacy.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, 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

Our comments focus on four aspects of the bill:

- Further clarifying the role of processors;
- Encouraging strong and consistent enforcement;
- Supporting consumers' right to know through practical requirements; and
- Harmonizing the bill's exemptions with leading state privacy laws.

I. Further Clarifying the Role of Processors

We commend you for ensuring that SB 619 recognizes the unique role of data processors, which process data on behalf of other companies and pursuant to their directions. As enterprise software companies, BSA members often act as processors that handle data on behalf of their business customers; those business customers, in turn, act as controllers that decide how and why to process consumers' personal data.[2] Both controllers and processors should have strong obligations under any privacy law – but those obligations must fit these different roles in order to fully protect consumers' data.

Although SB 619 reflects this important role, we strongly recommend three changes to better reflect the role of processors in handling consumers' personal data:

First, SB 619 should better reflect the role of processors in fulfilling consumer rights requests. As all existing state privacy laws recognize, controllers should have the obligation to respond to consumer rights requests and processors should have the obligation to assist controllers in doing so. State privacy laws in CO, CT, and VA address this by requiring processors to "assist the controller" in fulfilling the controller's obligation to respond to consumer rights requests by adopting appropriate technical and organizational measures, taking into account the nature of the processing and the information available to the processor.[3] We recommend aligning SB 619's language with this widely-recognized standard.

> **Recommendation**: *Section 6(1)(a) should be modified to state that in assisting the controller, the processor must "~~Enable the~~ Provide appropriate technical and organizational measures, to the extent reasonably practicable, taking into account the nature of the processing and the information reasonably available to the processor for the controller to fulfill its obligation to respond to requests from consumers under section 4 of this 2023 Act ~~by means that take into account how the processor processes personal data and the information available to the processor and that use appropriate technical and organizational measures to the extent reasonably practicable~~;"*

Second, SB 619 should require both controllers and processors to adopt reasonable data security safeguards. Currently, Section 6(1)(b) conflates safeguards adopted by a processor with those adopted by a controller. Specifically, it would require a processor to assist a controller by adopting "administrative, technical and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the controller processes." This provision should refer to the processor, rather than the controller – to clearly require processors to adopt data security measures (and without suggesting a processor could be required to adopt measures to protect the confidentiality of data a controller may process independently).

---

[2] Of course, when BSA members collect data for their own business purposes, they are not acting as a processor but instead become a controller for such activities. For instance, a company that operates principally as a processor will nonetheless be treated as a controller if it collects data for the purposes of providing a service directly to consumers. SB 619 appropriately recognizes that companies may act in these different roles at different times, with respect to different processing activities. Section 6(4)(b) is clear that the determination of a company's role is "fact-based" and must take into account "the context in which a set of personal data is processed." We support this approach, which ensures that companies are only treated as processors to the extent they continue acting on behalf of a controller.

[3] State privacy laws in Colorado, Connecticut, and Virginia establish that processors are to adopt reasonable and appropriate technical and organizational measures to assist a controller in responding to consumer rights requests. *See, e.g.,* Colorado's CPA Sec. 6-1-1305(2)(a); Connecticut DPA Sec. 7(1); Virginia CDPA Sec. 59.1-579(A)(1).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Recommendation: *Section 6(1)(b) should be modified to refer to data security safeguards for data processed by a processor. It should state that the processor must: "Adopt administrative, technical and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the ~~controller~~ processor processes, taking into account how the processor processes the personal data and the information available to the processor;"*

Third, SB 619 should focus the obligation for a processor to provide data to a controller on information within the processor's possession.

Recommendation: Section 6(2)(f) should be modified to state: "Require the processor to make available to the controller, upon the reasonable request of ~~at~~ the controller~~'s request~~, all information in its possession that the controller needs to verify that the processor has complied with all obligations the processor has under sections 1 to 10 of this 2023 Act."

II. Strong and Consistent Enforcement

Our recommendations focus on three aspects of SB 619's enforcement provisions:

First, we support exclusive enforcement by the Attorney General. BSA believes a strong, centralized approach to enforcing a state privacy law is the best way to develop sound practices that encourage companies to invest in engineering that protects consumers in line with regulatory actions and guidance. We support exclusive enforcement by a state's Attorney General, who should have the tools and resources needed to strongly enforce a new privacy law. State attorneys general have a strong track record of enforcing privacy-related laws — and have done so in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. Moreover, empowering state attorneys general to enforce a new privacy law ensures that enforcement rests with an agency that can observe the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses.

We appreciate that Section 9 of SB 619 recognizes a role for Attorney General enforcement. However, Section 10 of the legislation also includes a private right of action. 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 five states to enact a comprehensive consumer privacy law has created a private right of action for the privacy-related obligations in those laws.

Recommendation: *The Attorney General have exclusive enforcement of the new privacy law and be given the tools and resources needed to do so effectively*.

Second, we are concerned that SB 619 would allow a controller's directors, members, officers, employees, or agents to be held liable for acts or omissions resulting in violations of the law.[4] This can harm companies' ability to recruit and retain qualified employees, by creating new legal risks for roles charged with safeguarding consumers' personal data. By creating such liability, Section 9(4)(b) runs counter to the goal of creating strong compliance programs. Consumer privacy laws should encourage businesses to build effective privacy practices. States with comprehensive privacy laws have recognized this by opting to establish robust obligations on controllers and processors without creating liability for individual employees. We encourage you to take a similar approach.

Recommendation: *Section 9(4)(b) should be removed, to ensure that SB 619 promotes strong compliance practices that are not grounded in the establishment of new liabilities for individual employees.*

[4] *See,* SB 619, Sec. 9(4)(b), providing that if "a court finds that a director, member, officer, employee or agent of a controller violated sections 1 to 10 of this 2023 Act through an act or omission, the court may find that the controller committed the violation or the court may find that both the controller and the director, member, officer, employee or agent committed the violation and may impose separate civil penalties on each."

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Third, the right to cure potential violations should apply to both controllers and processors. Currently, Section 9(5) only provides controllers the opportunity to cure violations of the law before the Attorney General initiates legal action.[5] The opportunity to cure an alleged violation should apply to all entities regulated by the bill, including both controllers and processors.

> **Recommendation**: *Section 9(5) should be revised to state: "Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller or processor of a violation of sections 1 to 10 of this 2023 Act if the Attorney General determines that the controller or processor can cure the violation. If the controller or processor fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice."*

III. Supporting Consumers' Right to Know through Practical Requirements

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.

As currently written, SB 619 would require controllers to provide consumers with a list of specific third parties to which they have disclosed the consumer's personal data.[6] We recommend focusing the right to know on providing 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 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) and burdening the consumer with identifying what type of company each third party is (because it may not be apparent from the company's name that it is a marketing company, or a data broker, etc.). The CPRA's right to know takes a similar approach, requiring businesses to disclose to a consumer the "categories of third parties to whom the business discloses personal information."

> **Recommendation**: *Section 3(1)(a)(B) should be revised to state: "A list of ~~specific~~ the categories of third parties, other than natural persons, to which the controller has disclosed the consumer's personal data; and"*

IV. Harmonizing the Bill's Exemptions with Leading State Privacy Laws

We appreciate the need to create a privacy law that is right for Oregon consumers. We also recognize the importance of states in developing consumer privacy legislation that gives consumers rights over their information and imposes obligations on businesses to handle that information in responsible ways.

While states will naturally develop laws that are different in how they protect consumers, we want to emphasize the value of building a set of state privacy laws that work together and share core structural commonalities. This approach not only helps businesses understand how their obligations change across jurisdictions – and map those obligations to one another — but also creates a broader set of shared expectations among consumers. As you refine SB 619, we encourage you to prioritize harmonizing structural and scoping aspects of the legislation with existing state privacy laws — and ensure that where Oregon departs from those other laws is 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.

---

[5] *See,* SB 619, Sec. 9(5) stating that before bringing an action "the Attorney General shall notify a controller of a violation of sections 1 to 10 of this 2023 Act if the Attorney General determines that the controller can cure the violation. If the controller fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice."

[6] *See, e.g.,* SB 619, Sec. 3(1)(a)(B) stating that a consumer may obtain from a controller a "list of specific third parties, other than natural persons, to which the controller has disclosed the consumer's personal data."

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

To promote consistency with existing state laws, we recommend modifying Section 2(2)(e), which exempts employment information from the bill's scope. As other state laws recognize, consumer-facing requirements like those in SB 619 should not apply to employees, who raise a distinct set of privacy concerns from the privacy concerns raised by consumers. We strongly recommend Oregon align the language of its employee exception with existing state laws, like those in Connecticut and Virginia, which focus on excluding data "processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of" a controller, processor, or third party "to the extent the data is collected and used within the context of that role." Aligning SB 619 with existing laws on this important scoping issue will promote consistent treatment of employee information by businesses that work across state lines.

> **Recommendation**: *Section 2(2)(e) of SB 619 should be revised to exempt:* "Information processed or maintained ~~solely~~ in the context of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role ~~connection with, and for the purpose of, enabling~~…"

* * *

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 your office on these important issues.

Sincerely,

Olga Medina
Director, Policy

CC: The Honorable Ellen Rosenblum

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org