June 3, 2022

The Honorable Ellen Rosenblum
Office of the Attorney General
Oregon Department of Justice
1162 Court St. NE
Salem, OR 97301-4096

Dear General Rosenblum:

BSA | The Software Alliance[1] appreciates the opportunity to share our feedback on the Oregon Comprehensive Privacy Law Draft circulated by the Attorney General's office (the "Privacy Law Draft"). 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 new 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.

Our comments focus on four aspects of the Privacy Law Draft:

- Supporting its clear recognition of the different roles of controllers and processors in safeguarding consumers' personal data;
- Supporting a practical approach to implementing global opt out obligations;
- Supporting a harmonized approach to structural and scoping aspects of the Draft Privacy Law, to clarify expectations for consumers and drive strong compliance practices by companies; and
- Supporting strong regulatory enforcement by the Attorney General's office.

We are also submitting a redline with language to implement these recommendations.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, 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

I. The Roles of Controllers and Processors

We commend your office for ensuring the Privacy Law Draft 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]

Every state to enact a comprehensive consumer privacy law has distinguished between controllers and processors. Indeed, this distinction is fundamental to leading privacy and data protection laws worldwide. In the US, new state privacy laws in Colorado, Connecticut, Utah, and Virginia assign important – and distinct – obligations to both processors and controllers.[3] California similarly distinguishes between these different roles, which it terms businesses and service providers.[4]

Privacy laws make this distinction for good reason. Clearly assigning obligations to both controllers and processors helps companies understand their obligations. More importantly, distinguishing between these roles helps consumers by ensuring their personal data is protected not only when it is processed by a consumer-facing company they interact with (acting as a controller), but also when that company uses vendors and service providers (acting as processors) to process the data. BSA supports placing strong obligations on both controllers and processors — but those obligations must fit these different roles in order to fully protect consumers' personal data. For example, we appreciate the Privacy Law Draft's recognition that consumer-facing obligations, such as responding to consumer rights requests and seeking a consumer's consent to process sensitive personal data, are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to processors that handle data on behalf of controllers.[5] Other obligations, such as adopting reasonable security measures to safeguard personal data, are appropriately placed on both types of companies.

Recommendations:

- ***First***, we strongly recommend retaining the definitions of both "controller" (in Sec. 1(7)) and "processor" (in Sec. 1(14)) in the draft legislative language. These definitions reflect the global standard for defining these roles, which is also reflected in the Colorado, Connecticut, Utah, and Virginia laws.

- ***Second***, we strongly recommend retaining the approach of creating a set of specific obligations for processors; these appear in Section 6 of the Draft Privacy Law. BSA recognizes that processor-specific obligations are important to build consumers' trust that personal data will remain protected when it is held by processors, who handle it on behalf of other companies. BSA has therefore supported processor-specific obligations in other state laws, including in Colorado, Connecticut, and Virginia.

---

[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. The Draft Privacy Law appropriately recognizes that companies may act in these different roles at different times, with respect to different processing activities. Section 6(4) is clear that companies are to determine if they are acting as a controller or a processor with respect to specific processing activities based on a "fact-specific" assessment. 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] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1306 (Responsibility According to Role); Connecticut's Personal Data Privacy Act Sec. 7; Utah's Consumer Privacy Act Sec. 13-61-301 (Responsibility According to Role); Virginia Consumer Data Protection Act, Sec. 59.1-577 (Responsibility According to Role; Controller and Processor).

[4] *See, e.g.*, Cal. Civil Code 1798.140(ag) (defining service provider and requiring service providers and businesses to enter into contracts that limit how service providers handle personal information).

[5] For additional information on the distinction between controllers and processors, BSA has published a two-pager available here.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

- ***Third***, we suggest revising Section 6's approach to subcontractors. Specifically, Section 6(b)(D) requires providing controllers an opportunity to object to subcontractors – in addition to requiring that the subcontractor enter into a contract taking on the processor's privacy and security obligations. We recommend modifying this provision to require that controllers be given *notice* of subcontractors, but not an *opportunity to object* to them. This change would not affect the requirement for subcontractors to enter into contracts taking on a processor's obligations, which BSA recognizes is important to ensure that personal data remains protected when handled by subcontractors.

  This recommendation is particularly important because of the frequency with which processors engage subcontractors to provide services to controllers. In many cases, a processor relies on dozens (or more) subcontractors to provide a single service – which is often provided at scale, for use by hundreds (or more) controllers. In these situations, processors may need to replace a subcontractor quickly if one subcontractor is unable to provide services, either because of an operational issue or because of a potential security concern. Requiring controllers to have an opportunity to object can slow down the provision of products and services in these situations, without a clear benefit to consumers (whose data remains protected pursuant to contractual commitments by the subcontractor) or to controllers (which often rely on processors to identify and enlist trustworthy subprocessors). Moving to a standard that requires controllers be given notice of subcontractors, rather than an opportunity to object, helps to ensure processors can quickly and securely engage the subcontractors they need to provide services to their business customers while protecting personal data.

II. Global Opt-Out Requirements

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 laws enacted in Colorado and Connecticut, the Draft Privacy Law includes a clear requirement for controllers to honor global opt-out signals as a method for opting out of sale or targeted advertising.

Although consumers often use the term "global opt out" to refer to the ability to opt out of processing by a range of different companies, any requirements for a global opt out mechanism must also work globally in the geographic sense. There is a real benefit to both consumers and to companies in ensuring that any global opt out mechanisms function not just in a single state but can operate across states. If the Draft Privacy Law retains the requirement for controllers to respond to global opt out mechanisms, we strongly encourage your office to focus on creating a mechanism that functions in practice and that leverages ongoing work by other states and by a broad range of stakeholders on these issues.

Recommendations:

- *First, we support adopting a set of guardrails for global opt-out requirements, like those already included in the Privacy Law Draft*. Section 5(4)(a)(A)(ii) incorporates a list of safeguards on global opt out mechanisms; this list appears to be modeled on the same set of safeguards adopted by Connecticut, including that a signal not make use of a default setting and that it enable a controller to accurately determine whether the consumer is a resident of the state. We appreciate that these guardrails are also substantively similar to the requirements in Colorado's law, which helps to ensure that a mechanism meeting one state's requirements could be used across states – which is a better outcome for both consumers and businesses than a mechanism that only works in a single state. For this reason, we especially support subsection (4), which states that any global opt out mechanism is to be as "consistent as possible" with a mechanism required by any federal or state law or regulation.

- *Second, we encourage you to consult with stakeholders on practical issues — including how a controller will know that a signal meets the law's requirements.* While it is important to require controllers to honor only certain signals — such as those that meet the set of guardrails in Section 5(4)(a)(A)(ii) — it is not clear from the Draft Privacy Law how a controller will be able to determine

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

that a particular signal meets these requirements, or if that determination will be left to each controller. For example, it is not clear whether the Attorney General's office would publish a list of the signals that meet these requirements and thus identify the mechanisms that companies would need to honor. We urge you to work with stakeholders on these types of practical issues. Companies will require time to build tools to respond to global opt out mechanisms — and focusing on practical issues early on will help to foster development of tools that work in practice.

- *Third, we encourage you to prioritize educating consumers about what global opt-out signals do — and what they do not do.* As states adopt global opt out requirements, it is important for consumers to understand the scope of what opt out signals do as well as their limits. For example, if a consumer uses a browser-based mechanism to opt out of sale and targeted advertising, the browser effectuate those requests for activity that occurs within the browser. But the browser-based mechanism may not be able to convey requests to opt out of activities beyond the browser, such as when the consumer uses a mobile device or interacts with a company in person. Consumers should be aware of what these new tools can do, so that they can better use them to exercise their rights.

- *Fourth, we encourage you to adopt a delayed implementation date so that any requirement to honor global opt outs goes into effect after January 1, 2025*. In the next two years, there will be a significant focus among a broad range of industry, government, and advocacy stakeholders in developing methods for complying with global opt out requirements. Much of this activity will be driven by the new laws in Colorado and Connecticut, which will require controllers to honor global opt-out signals starting July 1, 2024 (in Colorado) and January 1, 2025 (in Connecticut). California's Privacy Protection Agency will also address the issue in its upcoming rulemaking.

  Other states can leverage this ongoing activity, and the learnings and mechanisms that come from it, by ensuring that additional global opt out requirements go into effect after the Colorado and Connecticut laws are already in place. This would help to further Oregon's goal of providing easy ways for consumers to exercise their new rights, while allowing Oregon to address issues that may come to light in other state regulatory and implementation processes.

III. Harmonizing the Structure and Scope of the Draft Privacy Law

We appreciate your office's focus on creating 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 the Draft Privacy Law, we encourage you to prioritize harmonizing structural and scoping aspects of the legislation with other leading 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. In particular, we encourage you to consider adopting the same set of activity-based exceptions that are nearly identical in the Colorado, Connecticut, Utah, and Virginia laws. Harmonized activity-based exceptions ensure that companies can build strong compliance practices — including for handling law enforcement requests, responding to security breaches, and improving functionality — that can be leveraged across state lines to better provide the services consumers expect.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Recommendations:

- ***First***, we support retaining the employee exception in the Draft Privacy Law, which mirrors similar exceptions in the Colorado, Connecticut, Utah, and Virginia laws. Like those laws, the Draft Privacy Law both (1) excludes individuals acting in a "commercial or employment context" from the definition of a consumer (in Section 1(6)(b)) and (2) includes a separate exception focused on employee-specific information (in Section 2(2)(i)).[6] We support this approach, which ensures that the focus of a consumer privacy law remains on consumers.

- ***Second***, we recommend revising the activity-based exceptions in Section 2(3) to align with the similar exceptions already in place in other state laws. The new privacy laws in Connecticut, Colorado, Utah, and Virginia adopt a set of activity-based exceptions that are nearly identical, despite significant variation in many other aspects of those laws.[7] If states adopt divergent requirements for handling data sought by law enforcement, or handling data in connection with security incidents, or to using data for internal research purposes, it will fragment efforts by companies to develop products, services, and compliance practices that work across state lines.

  We recommend prioritizing a set of activity-based exceptions that align with similar exceptions in existing laws, including:

  - *Clarifying and broadening Sec. 2(3)(a) to recognize exceptions for compliance with laws, legal demands, and law enforcement agencies.* Section 3(a) is drafted narrowly, to ensure the law does not prevent a controller or processor from "complying with a lawful order or other provision of law." But this narrow phrasing omits important activities recognized in the Colorado, Connecticut, Utah, and Virginia laws, all of which have three provisions directed at law enforcement, to: (1) clearly state the privacy law does not prevent a controller or processor from complying with federal, state, or local laws, rules or regulations, (2) permit compliance with a broader range of regulatory inquiries, beyond "lawful orders," and (3) specifically allow for cooperation with law enforcement agencies regarding activity the company has a good faith belief violates federal, state, or local laws.

  - *Broadening Sec. 2(3)(b) to focus on actions beyond "defending" legal claims*. We recommend expanding this exception to cover investigating, exercising, preparing for, or defending legal claims. The laws in Colorado, Connecticut, Utah, and Virginia each contain a "legal claims" exception that covers all of these activities.

  - *Expanding Sec. 2(3)(c) to encompass a broader range of actions related to data breaches and other illegal activities*. The current text of 2(3)(c) focuses on "preventing, detecting, protecting against or responding to a breach of security with respect to personal data or to other illegal activity." We recommend expanding this in two ways. *First*, rather than limiting the exception to "a breach of security . . . or . . . . other illegal activity" we encourage you to adopt language contained in the Colorado, Connecticut, and Virginia laws that refer to a broader range of harmful actions, namely "security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity." *Second*, we recommend specifically permitting actions to preserve of the integrity or security of systems, and actions

[6] *See* Colorado Privacy Act Sec. 6-1-1303(6)(b) (defining consumer) and Sec. 6-1-1304(k)(excluding data "maintained for employment records purposes"); Connecticut's Personal Data Privacy Act Sec. 1(7) (defining consumer) and Sec. 3(b)(15) (excluding three categories of employment-related data); Utah Consumer Privacy Act Sec. 13-61-101(10)(b) (defining consumer) and Sec. 13-61-102(o) (excluding three categories of employment-related data); Virginia Consumer Data Protection Act Sec. 59.1-575 (defining consumer) and 59.1-576.C.14 (excluding three categories of employment-related data).

[7] *See* Colorado Privacy Act Sec. 6-1-1304(3) ("Applicability of Part"); Connecticut's Personal Data Privacy Act Sec. 10; Utah's Consumer Privacy Act, Sec. 13-61-304 ("Limitations"); Virginia's Consumer Data Protection Act Sec. 59.1-578 ("Limitations").

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

to investigate, report, or prosecute those responsible for any such action. The Colorado, Connecticut, Utah, and Virginia laws contain similar language. A uniform approach to this exception is particularly beneficial to consumers, because it ensures companies may adopt unified approaches to how they handle personal data to quickly address a data breach, identify a malicious actor, or respond to illegal activity.

- *Retaining Sec. 2(3)(d), which ensures companies can identify and repair errors that impair existing and intended functionality*. We support this language, which helps companies take steps to make sure their products and services work as consumers expect. Colorado, Connecticut, Utah, and Virginia all have equivalent exceptions.

- *Retaining Sec. 2(3)(e), which ensures companies can provide a product [or service] specifically requested by a consumer, or take steps at the request of a consumer prior to entering into a contract*. We support this provision, which is designed to ensure that companies may continue to provide the products consumers request. Colorado, Connecticut, Utah, and Virginia have similar exceptions, and all but Colorado contain additional language expressly permitting companies to fulfill the terms of a written warranty.

- *Retaining Sec. 2(3)(f), which ensures companies can act to protect the health and safety of a consumer or other individual*. We support this provision, which appears to be deliberately framed broadly, similar to the equivalent Colorado provision that permits companies to protect the "vital interests of the consumer or of another individual." The Connecticut, Utah, and Virginia laws contain a narrower version of this exception, permitting companies to take "immediate steps" to protect an interest that is essential for the life or physical safety of the consumer or of another individual.

- *Adding an exception permitting assistance to others*. Section 2(3) lacks an exception that permits companies to assist others with the exempted activities. We suggest including language similar to Colorado's law, which includes an exemption for "assist[ing] another person with any of the activities set forth in this subsection."[8] This provision is important to ensure that companies may help others respond to security incidents or comply with legal demands, among other actions.

- *Adding a research exception.* Section 2(3) lacks an exception for public or peer-reviewed scientific or statistical research that adheres to all other applicable ethics and privacy laws. Connecticut and Virginia expressly exempt such research, to ensure the privacy laws do not interfere with research that is already governed by institutional review boards or other independent oversight entities that have determined the expected benefits of the research outweigh privacy risks.[9] We recommend adding a similar exception, to ensure that the privacy law does not inadvertently hinder research that is conducted in the public interest and already subject to other safeguards and oversight. This exemption and the exception below for internal research are both important for facilitating the use of data for research by businesses and other entities, including research collaborations between companies and public health authorities to develop contract tracing applications during COVID-19.

- *Adding an exception on product recalls*. Section 2(3) lacks a provision specifically addressing product recalls. We suggest adding a provision like those in Connecticut, Utah, and Virginia that expressly permit companies to take steps to effectuate a product recall, which helps companies act quickly to protect consumers from potentially harmful products.

[8] Colorado Privacy Act, Sec. 6-1-1304(3)(a)(XII).
[9] Utah has a broader exception for general research, whereas Colorado includes an exception focused on health care research. *See* Colorado Privacy Act, Sec. 6-1-1304(3)(a)(XI) (creating public health exception); Utah Consumer Privacy Act Sec. 13-61-102(2)(j).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

- *Adding an exception on internal research*. Section 2(3) also lacks an exception for internal research to help improve, repair, or develop products, services or technologies. The Colorado, Connecticut, Utah, and Virginia laws all include this exception, which helps companies conduct research to improve the products they offer to consumers. This provision is important to ensure companies can meet consumers' demand for products that get better over time — by allowing companies not only to repair products, but also to improve and develop them. As just one example, a B2B company that offers an AI system that companies can use to route customer complaints to different teams of employees may dramatically improve that system through internal research that identifies when the system routed complaints correctly and when it did not. Although that research is internal, it results in a better overall product — and, as a result, help customers more quickly reach the right employees to handle their complaints.

- *Adding an exception for internal operations*. Section 2(3) similarly lacks an exception for internal operations that are reasonably aligned with the expectations of the consumer. The Colorado, Connecticut, Utah, and Virginia laws contain this separate exception, which focuses on operations that are reasonable based on the consumer's relationship with the controller.

To limit the use of these exceptions, we also suggest considering language that ensures companies minimize the use of these exceptions. In Colorado, Connecticut, and Virginia, the state privacy laws guard against inappropriate expansion of the activity-based exceptions by requiring that personal data processed pursuant to an exception not be processed for any other purpose and be processed only to the extent doing so is adequate, relevant, and limited in relation to the specific purpose of the exception.[10] In addition, the Colorado, Connecticut, Utah and Virginia laws all specifically assign companies the burden of demonstrating they qualify for an exception. Section 2(3) does not currently contain either of these provisions.

- ***Third,*** we support requiring consent for the processing of sensitive personal data. Section 5(1)(a)(D) currently states that controllers shall "not process u data concerning a consumer without obtaining the consumer's consent." While this appears to be a typo in the drafting, we recommend applying this consent requirement only to the processing of sensitive personal data. That approach is consistent with the Colorado, Connecticut, and Virginia privacy laws. The current language could be read to require consent for processing of any personal data – which has significant downsides not just for businesses that may be required to obtain consent in a far wider range of scenarios, but also for consumers who suffer from consent fatigue and value a privacy law that only puts the burden on consumers to consent to sensitive uses of their personal data or unexpected uses***.***

IV. Attorney General Enforcement

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.

[10] *See* Colorado Privacy Act, Sec. 6-1-1304(4)(b); Connecticut Personal Data Privacy Act Sec. 10(f); Virginia Consumer Data Protection Act Sec. 59.1-582.F.

We appreciate that Section 9 recognizes a role for Attorney General enforcement of the Draft Privacy Law. But the Draft Privacy Law also contemplates future discussion about including a private right of action. A private right of action, which punishes technical lapses, is not needed to ensure strong enforcement of a new privacy law, and can distract from strong and consistent enforcement of the substantive protections included 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 privacy-related obligations in those laws.

Recommendation:

- *We recommend the Attorney General have exclusive enforcement of the new privacy law and be given the tools and resources needed to do so effectively*.

* * *

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,

Kate Goodloe
Senior Director, Policy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org