October 29, 2020

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 provide feedback on the two draft proposals for consumer privacy legislation being considered for introduction in Oregon in 2021.

BSA supports a strong, national comprehensive privacy law that provides consumers meaningful rights over their personal data and obligates businesses to handle personal data in line with consumers' expectations. In our advocacy, we have expressed support for consumer protections like many of those included in the legislative drafts. We commend your office's work to ensure that consumers' rights in their personal data – and the obligations imposed on businesses – function in a world where different types of companies play different roles in handling consumers' personal data. We also applaud your efforts to involve a broad range of stakeholders in these important discussions and to seek feedback on two potential legislative drafts before potentially introducing a comprehensive privacy bill.

BSA members are enterprise software companies that create the technology products and services that other businesses use. For example, BSA members provide business-to-business tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and workplace 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.

Our comments focus on two aspects of the legislative drafts: the different roles of companies covered by both drafts, and the different enforcement mechanisms in each draft.

I. Both Drafts Should More Clearly Distinguish Between Companies that Play Different Roles in Handling Consumers' Personal Data

[1] BSA is the leading advocate for the global software industry before governments around the world. Our members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

In any privacy law, it is critical that different types of businesses that may handle a consumer's personal data are: (1) clearly defined, and (2) subject to strong obligations that reflect their different roles in handling consumer data. Both drafts discuss these issues in identical terms — and we recommend both drafts be updated to reflect the important differences between different types of businesses.

- ***Definitions***. Privacy laws worldwide reflect the fundamental distinction between *data processors*, which handle a consumer's personal data on behalf of other businesses, and *data controllers*, which decide how a consumer's personal data will be collected and used. Distinguishing between controllers and processors is important from a privacy perspective because it allows legislation to craft different obligations for different types of businesses based on their different roles in handling consumers' personal data.

  The Attorney General's office has recognized the importance of clearly defining data controllers and data processors, including through the LC draft request materials submitted in connection with both drafts. While those materials use the terms "controllers" and "processors," both drafts refer to controllers as "principals" and to processors as "information managers." We suggest replacing these definitions with the clear definitions in the LC draft request materials:

  - "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

  - "Processor" means a natural or legal person who processes personal data on behalf of a controller.

  This change would accomplish two objectives:

  First, it would align these definitions with the globally accepted standard definition drawn from the European Union's General Data Protection Regulation ("GPDR"), under which a company is a controller if it determines the "purposes and means" of processing. Aligning these definitions with definitions used in privacy laws worldwide will increase the interoperability of any future legislation. Consumers and businesses can more readily understand the rights and obligations created in a privacy law when it maps onto commonly used terms.[2]

  Second, this change would avoid uncertainty introduced by the current language, which treats an "affiliate, employee, agent or other person" acting on behalf of a principal as an "information manager." Under this definition, the employee of a principal could be treated as an "information manager" — a result that would undercut the distinction between the two roles since a principal would almost always act through its employees. Even if the terms "principal" and "information manager" are retained, then, we suggest replacing "affiliate, employee, agent, or other person" with the language from the LC draft request material, which references a "natural or legal person."

- ***Obligations***. Privacy laws better protect consumers' personal data when they impose strong obligations on both controllers and processors — and tailor those obligations to reflect the different roles of these different entities in handling consumers' data.

[2] For the same reason, we support replacing the current definition of "personal data management" with the definition of "process" or "processing" contained in the LC request materials.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

While both drafts seek to define different types of businesses — as principals and information managers — they fail to tailor different obligations to these different types of companies. This approach is in conflict with the clear language in the LC draft request materials, which assigns certain obligations to controllers and others to processors. We accordingly suggest both drafts be amended to align with the thoughtful approach reflected in the LC draft request materials.

- ***Consumer-facing obligations should be assigned to controllers***. Consumers expect to interact with a business that provides them a service — but do not expect to interact with the network of data processors that may store, analyze, and process data at the direction of that consumer-facing business. As a result, consumer-facing obligations like obtaining consent or fulfilling consumer rights of access, correction, deletion, portability, and objection are appropriately placed on controllers, which decide when and how to collect a consumer's data.

  The GDPR and California Consumer Privacy Act ("CCPA") both reflect this approach. If Oregon departed from this standard and required both controllers and processors to honor consumer-facing obligations such as consumer rights requests, individual consumers could be forced to contact the many data processors that handle data on behalf of each consumer-facing company to exercise their new rights — creating even more confusion for consumers.

  Applying the same obligations to both entities also raises significant concerns for data processors, which in many cases contractually commit to privacy safeguards that prohibit them from accessing data they handle on behalf of a controller. To take another example, if both controllers and processers were required to obtain a consumer's consent to process her data, it would not only inundate consumers with duplicative consent requests from multiple companies processing the same data for the same purpose (rendering each request less meaningful) but would create greater security risks (by requiring consumers to grant or deny permissions to data processors they do not know) and create new privacy risks (by potentially requiring data processors to look at data they otherwise would not access).

  For these reasons, we recommend amending the drafts so that consumer-facing obligations including the consumer rights contained in Section 4, are fulfilled by data controllers. Similarly, obligations around processing a consumer's sensitive data (Sec. 3(1) and 3(5)), data minimization and notice obligations (Sec. 3(3)), and the obligation to not process data for discriminatory purposes (Sec.3(6)) should be assigned to controllers, which determine the purposes for which personal data is processed. These changes are in line with the approach set out in the draft LC request materials.

- ***Data security obligations should continue to fall on both data processors and data controllers***. Data processors also have important responsibilities under any data privacy law, including to process data in line with a controller's instructions and to safeguard the data they process. We accordingly support applying the data security provision in the current drafts (Sec. 3(4)) to both controllers and processors. While this is a departure from the LC draft request materials, which suggested these obligations only fall on controllers, BSA members recognize the need for all companies that handle a consumer's personal data to safeguard it appropriately. In addition, we support adding to Section 3(4) language from the draft LC request materials stating the reasonable administrative, technical, and physical security practices required by this section "shall be appropriate to the volume and nature of the sensitive personal data at issue."

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

- ***Processing of data by data processors should be governed by a written agreement that reflects the different obligations of these different entities***. Both drafts would require principals and information managers to execute a "binding written agreement" requiring the companies to engage in personal data protection management in compliance with the Act. However, the drafts as written do not clarify a processor's obligations in processing personal data on behalf of a controller. To the extent you revise the approach to these important issues, we are including potential language in Annex A for your consideration. BSA members developed this language to reflect the important safeguards processors should take when processing personal data, including ensuring those who process data on their behalf are subject to a duty of confidentiality and that processors provide controllers appropriate tools to help them respond to consumer rights requests, insofar as possible.

II. Strong and Consistent Enforcement Does Not Require a Private Right of Action

Effective enforcement of a privacy law is critical to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. BSA members believe that a privacy law can create strong and effective enforcement without including a private right of action, and we therefore encourage your office to focus on the second legislative draft, which would be enforced through the Oregon Department of Consumer and Business Services.

Consumers and companies need clarity in understanding how the rights and obligations created by any new privacy law will be applied. An agency like the Oregon Department of Consumer and Business Services is well-positioned to provide that clarity, because agencies can create a consistent body of enforcement efforts that demonstrate how the agency will apply the new rights and obligations in a variety of contexts, particularly when combined with informal or formal guidance interpreting the new privacy law. In contrast, enforcement structures that rely on private litigation may only provide that clarity after litigants spend significant amounts of time bringing their cases before courts. Even then, differing decisions by different courts may result in a less certain enforcement environment than a cohesive agency-led approach, and provide less useful guidance to companies that want to understand their obligations on the front end.

Thank you for your continued leadership in establishing strong consumer privacy protections, and for your consideration of our views. BSA and its members look forward to working with you.

Sincerely,

Kate Goodloe
Director, Policy
BSA | The Software Alliance

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Annex A
Suggested Legislative Language on Controller/Processor

Definitions [to include in Section 1]

(a) Controller. The term "controller" means the person who, alone or jointly with others, determines the purposes and means of processing personal data.

(b) Processor. The term "processor" means the person who processes personal data on behalf of the controller. A processor should follow the documented instructions of a controller that are agreed to by the parties. Unless otherwise specified, the obligations in this Act apply to controllers.

(c) Process. The term "process" means any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor Obligations [separate new Section]

(a) A processor shall—

(1) taking into account the nature of the processing, assist a controller by appropriate technical and organizational measures, insofar as this is reasonably possible, for the controller to fulfil its obligation to respond to consumer requests to exercise their rights pursuant to Section 4 of this Act [establishing individual rights including access, correction, and deletion];

(2) contractually require that each person processing personal data on behalf of the processor be subject to a duty of confidentiality with respect to such data;

(3) engage a subprocessor for purposes of processing personal data on behalf of a controller only after providing that controller with notice and pursuant to a written contract in accordance with this Section that requires the subprocessor to meet the obligations of the processor imposed on it by this Section with respect to personal data processed on behalf of the controller;

(4) pursuant to the contract required by this Act, provide a controller with reasonable access to information about processing performed on its behalf that is reasonably necessary to enable the controller to conduct any privacy impact assessment required by this Act.

(5) delete, deidentify or return to the controller after the agreed-upon end of the provision of services the personal data transferred on behalf of the controller to the processor or collected by the processor on behalf of the controller in accordance with the contract required by this Act, unless the processor is subject to a legal obligation regarding the retention of such data.

(6) develop, implement, and maintain administrative, technical, and physical safeguards that are reasonably designed to protect the security and confidentiality of personal data it

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

processes. These safeguards shall reflect the size and complexity of the processor, the nature and scope of its activities, the costs of available tools to improve security and reduce vulnerabilities, and its role in processing the personal data.

(b) **Contract Required.** Processing by a processor shall be governed by a contract between the controller and processor that is binding on both parties, sets out the obligations of both parties, and requires that the processor only collect or process personal data on behalf of the controller as directed by the controller. The contract shall also include the requirements imposed by this Section.

(c) **Determination as Controller or Processor**. 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 on the context in which personal data are to be processed. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to such processing.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org