The Honorable Troy Jackson
President of the Senate
3 State House Station
Augusta, Maine 04333

April 10, 2024

Dear President Jackson,

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates the Maine legislature's work to improve consumer privacy through LD 1977, the Maine Data Privacy and Protection 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 in Colorado, Connecticut, and Virginia.

In Maine, BSA has engaged extensively with members of the Joint Judiciary Committee, including Chairs Carney and Moonen. While we appreciate the Committee's efforts to align many aspects of the bill with the Connecticut Data Privacy Act, there are significant issues we believe require further revision to ensure that the bill's requirements function in practice. We urge you to revise LD 1977 in three ways:

1. The anti-discrimination provision should be revised to apply to controllers, which decide how and why to process data, and not to processors, which handle data at the direction of a controller and pursuant to its instructions. This provision should also focus on *unlawful* discrimination.

2. LD 1977 should be revised to ensure that the data minimization obligations apply only to controllers and avoid limiting the internal use exception to data previously collected from a consumer.

3. The bill should create strong and exclusive Attorney General enforcement by expressly prohibiting private actions under other laws.

We explain these concerns below and provide specific recommendations for revisions to address each concern.

1. The anti-discrimination provision should be revised to apply to controllers, which decide how and why to process data, and not to processors, which

[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

handle data at the direction of a controller and pursuant to its instructions. This provision should also focus on *unlawful* discrimination.

Although LD 1977 recognizes the important distinction between controllers (which decide how/why to process a consumer's information) and processors (which act as service providers, and process data on behalf of a controller and pursuant to its instructions), the anti-discrimination provision undercuts this distinction and imposes an obligation designed for controllers on processors.

Section 9606(7) prohibits discrimination in the processing of personal data. BSA strongly supports the objective of this provision, and we recognize the importance of ensuring that technology is not used to discriminate. However, controllers are the entities that decide how and why to process a consumer's personal data — and should therefore be the entities required to avoid processing data for discriminatory purposes. Instead, LD 1977 applies this obligation to both controllers and processors. But processors are not in a position to carry out this obligation, since they do not decide how and why to process a consumer's personal information (those decisions are, by definition, made by a controller) and are not in a position to know if their business customers (i.e., controllers) are using their services to discriminate. In many cases, processors adopt strict privacy and security measures that limit their insight into data that business customers store on their services.

Applying the anti-discrimination provision to processors can undermine important privacy protections, and could force processors to start reviewing data they otherwise would not — a counterproductive result for privacy laws. For example, a lending company could use a cloud storage provider as a processor. If that lending company engages in discriminatory practices, the cloud storage company may store data used in a discriminatory way, as it carries out instructions of the lender. As a processor, the cloud storage company's role is to hold the lender's data securely and privately — without reviewing it. If a processor is subject to the anti-discrimination provision in LD 1977, it could be responsible for the potentially discriminatory actions of their business customers — and would be encouraged or required to start looking at customer information they otherwise would not. That is a counterproductive effect that undermines the broader goals of privacy legislation, including data minimization.

In addition, the anti-discrimination provision raises a separate concern, even if it is limited to controllers, because it is not tied to activities that are *already unlawful* under state and federal laws that prohibit discrimination. The bill's broad language therefore creates uncertainty for companies implementing a new obligation, rather than creating clear direction to companies not to use technology in violation of anti-discrimination laws.

Recommendation: We recommend striking "processors" from this provision and changing "discriminates" to "unlawfully discriminates."

2. **LD 1977 should be revised to: (1) ensure that the data minimization obligations apply only to controllers and (2) avoid limiting the internal use exception to data previously collected from a consumer.**

Although LD 1977's recognizes the different of controllers and processors, Section 9609(6) conflates these roles by applying to both controllers and processors**.** Under this provision, personal data processed by a controller or processor may be processed only to the extent that the processing is "reasonably necessary and proportionate to the purposes listed in this section or, if the controller or processor is processing sensitive data, strictly necessary to the purposes listed in this section."

As other sections of LD 1977 recognize, a processor's role is to handle data on behalf of a controller and subject to its instructions. Because of this role, other state privacy laws apply the substantive provision contained in Section 9609(6)(A) of LD 1977 only to controllers, and not to processors. It is the controller that decides how and why to process a consumer's personal data in the first place. The controller is therefore the entity that can effectively this obligation, since minimizing the amount of data a company collects requires that company to revisit its decisions on how and why it collects that data in the first place. Those decisions are made by controllers — not by processors. The processor's role is instead to process data pursuant to the controller's instructions; those instructions will reflect the controller's choices in minimizing the amount of data it collects from consumers.

- **Recommendation:** Consistent with LD 1977's recognition that a controller is the entity that "determines the purpose and means of processing personal data", we strongly encourage you to revise Section 9609(6) to apply only to controllers, not processors.

Additionally, while we appreciate that LD 1977 does not restrict the ability of controllers or processors to use personal data to conduct internal research to develop, improve, or repair products, services or technology in Section 9609(2)(A), the bill limits the application of this provision to personal data *previously collected* by a company, which will limit companies' ability to use personal data to improve existing products or create new products for new customers. This provision would have the counterproductive effect of encouraging companies to design products or services so that they collect as much data as possible from the outset to comply with the bill's standard of "previously collected" data.

- **Recommendation:** We recommend striking "previously collected" from the internal use exemption.

3. **The bill should create strong and exclusive Attorney General enforcement by expressly prohibiting private actions under other laws.**

While we appreciate that LD 1977 provides for exclusive AG enforcement in Section 9610, it does not explicitly state that no provision of the bill may be construed as creating a private right of action under any other law. We urge you to do so.

- **Recommendation:** We recommend clarifying this provision to provide that no provision of the bill may be construed as creating a private right of action based on a violation of LD 1977 or any other law.

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

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org