



September 30, 2020

The Honorable Reuven Carlyle
233 John A. Cherberg Building
Olympia, WA 98504-0436

Dear Senator Carlyle:

BSA | The Software Alliance¹ appreciates the opportunity to provide feedback on the draft Washington Privacy Act 2021 (“the draft Act”). 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 similar to many of those in the draft Act. We commend your 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.

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 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.

We are writing to express our support for the draft Act’s clear recognition of the unique role of data processors. 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. For example, the European Union’s General Data Protection Regulation (“GDPR”) imposes different obligations on data processors than on data controllers, in light of their different roles in handling personal data. Similarly, the California Consumer Privacy Act (“CCPA”) distinguishes between “businesses” that decide how data will be collected and used and “service providers” that process data on behalf of such businesses. The distinction between data processors and data controllers is foundational not only to privacy laws across the

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.

globe, but also to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.² We commend you for incorporating this global standard into the draft Act, which clearly distinguishes between controllers and processors.

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. That type of role-based responsibility improves privacy protections for consumers. We appreciate the draft Act's recognition that processors and controllers both have important responsibilities to protect consumers' personal data — and that those obligations must reflect their different roles. For example, we agree with the draft Act that both processors and controllers must implement reasonable security measures to protect the security and confidentiality of data they handle. At the same time, we appreciate the draft Act's recognition that consumer-facing obligations like obtaining and responding to consumer rights requests are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to data processors handling data on behalf of those controllers.

Although we believe these aspects of the draft Act are critical to creating a strong privacy law, several BSA members are concerned that the draft Act's clear obligations may be undermined by language that suggests liability between controllers and processors be allocated on the basis of comparative fault. Because the draft Act already allocates responsibilities between controllers and processors, it is unnecessary to import a comparative fault standard to assign liability. Doing so only creates uncertainty about how that standard will be applied — a result that could ultimately harm consumers, who may be forced to wait for it to be applied each time they seek recourse.

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,



Tom Foulkes
Senior Director, State Advocacy

² For example, 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.