February 16, 2022

The Honorable Barbara Dittrich
Wisconsin State Capitol
2 E Main Street
Madison, WI 53703

Dear Chair Dittrich:

BSA | The Software Alliance[1] supports strong privacy protections for consumers such as those in AB957. In our federal and state advocacy, BSA works to advance legislation that ensures Wisconsinites' 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 the new consumer privacy laws enacted in Colorado and Virginia last year.

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 businesses 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' data.

We appreciate the opportunity to share our feedback on AB957. Our recommendations below focus on our core priorities in the legislation – the sections concerning processors, treatment of employment-related information, and enforcement provisions.

I. Distinguishing Between Controllers and Processors Benefits Consumers.

We are writing to express our support for AB957's clear recognition of the unique role of data processors.

[1] *BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.*

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

Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer's personal data. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction. In Virginia and Colorado, new state privacy laws assign important – and distinct – obligations to both processors and controllers.[2] In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers.[3] This distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[4] BSA and its members applaud you for incorporating this globally recognized distinction into AB957.

Distinguishing between controllers and processors better protects consumer privacy because it allows legislation to craft different obligations for different types of businesses based on their different roles in handling consumers' personal data. Privacy laws should create important obligations for both controllers and processors to protect consumers' personal data – and we appreciate AB957 recognition that those obligations must reflect these different roles. For example, we agree with AB957's approach of ensuring both processors and controllers implement reasonable security measures to protect the security and confidentiality of personal data they handle. We also appreciate AB957's recognition that consumer-facing obligations, including responding to consumer rights requests and seeking a consumer's consent to process personal data, are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to processors handling personal data on behalf of those controllers. Distinguishing between these roles creates clarity for both consumers exercising their rights and for companies implementing their obligations.

II. Employment-Related Information Should Be Clearly Excluded from AB957's Scope.

We applaud AB957's focus on focus on consumers, who raise distinct privacy concerns than those raised by employees. We encourage you to retain both the exclusion for individuals acting in a commercial or employment context in the definition of "consumer" and the exclusion for employment-related data in Section 8(c)(15).

---

[2] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1306; Virginia's Consumer Data Protection Act, Sec. 59.1-577.

[3] *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).

[4] 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, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data.

III. The Attorney General Should Be Empowered to Enforce Comprehensive Consumer Privacy Legislation.

We support enforcement by the attorney general and applaud AB957 for providing the attorney general with the exclusive authority to enforce its provisions. We believe that a strong, centralized approach – with the state attorney general as the exclusive enforcement authority – is the best way to develop sound practices that protect privacy and encourage investment by companies in engineering that protects consumers in line with regulatory actions and guidance. State attorneys general have a track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. We also believe that if states enact new comprehensive privacy laws, the state attorney general should be provided with the tools and resources needed to carry out this mission 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 you or a member of your staff on these important issues.

Sincerely,

Tom Foulkes
Senior Director, State Advocacy