February 28, 2023

The Honorable Josh West
2300 North Lincoln Boulevard
Room 205
Oklahoma City, OK 73105

Dear Leader West:

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates your work to improve consumer privacy through HB 1030, the Oklahoma Computer Data Privacy 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 consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. 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 information — 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 HB 1030. Our recommendations below focus on our core priorities in the legislation: the distinction between businesses and service providers, the need to establish robust service provider obligations, the bill's treatment of employment-related information, and its enforcement provisions.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, 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. Distinguishing Between Businesses and Service Providers Benefits Consumers.

As an initial matter, we are pleased that HB 1030 separately applies to "businesses" and "service providers."

We strongly support distinguishing between different types of companies that play different roles in handling consumers' personal information. Effective privacy laws worldwide reflect the fundamental and longstanding distinction between service providers (often called processors), which handle a consumer's personal information on behalf of other businesses, and businesses (often called controllers), which decide how a consumer's personal information will be collected and used.

All states with comprehensive consumer privacy laws recognize this critical distinction — and use the same dividing line recognized in HB 1030, which focuses on companies that decide the "purpose for and means of processing consumers' personal information."[2] This distinction aligns with privacy laws passed in Colorado, Connecticut, Utah, and Virginia, which all assign important obligations to controllers that determine the purpose and means of processing consumers data. Those states also create obligations for service providers, which they term processors.[3] Likewise, California's privacy law for several years has distinguished between these different roles, defining controllers as "businesses" that decide how and why to collect consumers' personal information and processors as "service providers" with distinct obligations in handling that information.[4] This longstanding 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.[5]

BSA and its members applaud you for recognizing this critical distinction in HB 1030.

---

[2] HB 1030 Sec. 3(A)(1)(c) (stating that the legislation applies to a business that "alone or in conjunction with others, determines the purpose for and means of processing consumers' personal information").

[3] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1305; Connecticut Data Privacy Act, Sec. 6-7; Utah Consumer Privacy Act, Sec. 13-61-301-302; Virginia Consumer Data Protection Act, Sec. 59.1-575.

[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 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 helps companies that process data demonstrate adherence to privacy obligations and helps 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. For additional information on the longstanding distinction between controllers and processors — sometimes called businesses and service providers — BSA has published a two-pager available here.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

II. Service Providers Play an Important Role in Protecting Consumers' Personal Information.

Our recommendations are centered on improving aspects of the bill that ensure all companies have meaningful obligations to safeguard consumers' personal information — and that those obligations reflect a company's role in handling that information. Although HB 1030 focuses on businesses that decide how and why to collect a consumers' data, several of its provisions appear to create obligations for service providers, including an obligation to adopt reasonable security measures and obligations to assist businesses in responding to certain consumer rights requests.[6]

A privacy law should impose strong obligations on all companies to safeguard consumer's personal information — yet those obligations must reflect the company's role in handling that information, or the law may end up creating new privacy and security risks for consumers. For example, laws in California, Colorado, Connecticut, Utah, and Virginia all place the obligation to respond to consumer rights requests on the companies that decide why and how to collect a consumer's personal data. If those obligations were instead placed on service providers, it would create security risks since consumers and service providers do not generally interact with each other — so service providers may not know whether to honor consumer rights requests from individuals they don't know. Instead of regulating service providers through such consumer-facing obligations, the Colorado, Connecticut, Utah, and Virginia laws create a series of obligations that are tailored to service providers' role and designed to ensure that service providers handle consumers' personal information responsibly. For example, those obligations include imposing a duty of confidentiality on all persons that process data and passing on contractual obligations to any subprocessors.

These provisions ensure that service providers are subject to strong obligations — with meaningful limits — in handling consumers' personal information. We believe such obligations are important in building consumers' trust and ensuring that their personal information remains protected when it is held by service providers.[7] We are also providing you an appendix to this letter setting out the Virginia CDPA's service provider obligations, for your reference as you further consider the role of service providers under HB 1030.

III. HB 1030 Should Focus on Protecting Consumers' Personal Information.

We also recommend focusing the bill on creating strong protections for individual consumers. As written, HB 1030 sweeps more broadly, because its definition of "personal information" in Section 2(14)(i) includes "professional or employment-related information."

---

[6] See, e.g., HB 1130 Section 11 (creating consumer rights); Section 13.H (creating data security obligations).

[7] For additional information on the distinction between controllers and processors — sometimes called businesses and service providers — BSA has published a two-pager available here and attached to this letter.

This greatly increases the scope of the bill and raises concerns about how substantive protections designed to safeguard consumer privacy would apply to the distinct privacy interests raised by employees. To the extent that HB 1030 is designed to protect consumer privacy, we recommend the bill focus on consumers without also sweeping in employment-related data. We encourage you to adopt the approach taken in state privacy laws in Colorado, Connecticut, Utah, and Virginia, which focus on protecting consumer privacy and therefore exclude individuals acting in a commercial or employment context in their definition of "consumer,"[8] in addition to excluding data processed or maintained in employment contexts[9] from the scope of their application. This approach can help to ensure that HB 1030 focuses on providing strong privacy protections for individual consumers.

IV. HB 1030 Promotes a Clear and Consistent Approach to Enforcement.

Finally, we want to express our support for HB 1030's approach to enforcement, which provides the attorney general with exclusive authority to enforce the bill. 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 and investment in engineering that protects consumers. 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,

Matthew Lenz
Senior Director and Head of State Advocacy

[8] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1303(6)(b); Connecticut Data Privacy Act, Sec. 1(7); Utah Consumer Privacy Act, Sec. 13-61-101(10)(b); Virginia Consumer Data Protection Act, Sec. 59.1-575.

[9] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1304(2)(k); Connecticut Data Privacy Act, Sec. 3(b)(15)(A-C); Utah Consumer Privacy Act, Sec. 13-61-102(2)(o)(i-iii); Virginia Consumer Data Protection Act, Sec. 59.1-576(C)(14)(i-iii).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Appendix

Virginia's Consumer Data Protection Act
§59.1-579. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-577.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-580.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

D. 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 upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org