



January 25, 2023

The Honorable Bo Watson
425 Rep. John Lewis Way N.
Suite 706 Cordell Hull Bldg.
Nashville, TN 37243

Dear Senator Watson:

BSA | The Software Alliance¹ supports strong privacy protections for consumers and appreciates your work to improve consumer privacy through SB73, the Tennessee Information 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 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 are writing to express our support for your bill's recognition of two of our core priorities: recognizing the unique role of data processors and creating privacy protections that are interoperable with other state laws. 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

¹ BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, 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.

this critical distinction. In Colorado, Connecticut, Utah, and Virginia, 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 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.⁴ BSA applauds you for incorporating this globally recognized distinction into SB73.

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 SB 73's recognition that those obligations must reflect these different roles. For example, we agree with the bill'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 the bill'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.

Additionally, we would like to express support for your efforts to ensure that SB73's promotes uniformity and brings clarity with respect to this critical area of state law. Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can readily map obligations imposed by a new law against their existing obligations under other laws. We commend you for drafting SB73's provisions so that they create privacy protections that are interoperable with protections included in other state privacy laws, which helps drive strong business compliance practices that can better protect consumer privacy.

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.

² See, e.g., Colorado's CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

³ See, e.g., Cal. Civil Code 1798.140(d, ag).

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 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.

Sincerely,



Matthew Lenz
Senior Director and Head of State Advocacy