



March 28, 2024

Representative Jacquelyn Baginski
Chair, House Innovation, Internet and Technology Committee
82 Smith Street
Providence, RI 02903

Dear Chair Baginski:

BSA | The Software Alliance¹ supports strong privacy protections for consumers and appreciates the House Innovation, Internet and Technology Committee's work to improve consumer privacy through House Bill 7787 (HB 7787). 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 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 HB 7787. Our recommendations below focus on several of BSA's core priorities in privacy legislation: clearly distinguishing between controllers and processors, establishing practical obligations for processors, and ensuring HB 7787's interoperability with other state laws.

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.*

I. Distinguishing Between Controllers and Processors Benefits Consumers.

We support HB 7787's clear recognition of the unique role of data processors. 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 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 the sponsor for incorporating this globally recognized distinction into HB 7787.

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 HB 7787'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.

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. 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](#).

II. The Bill's Provisions Giving Controllers an Opportunity to Object to Processors' Use of Subcontractors Should be Revised.

While HB 7787 recognizes the important distinction between controllers and processors, we are concerned that some aspects of the bill could inadvertently limit processors' ability to provide consumers and businesses with the products and services they request, reduce their ability to safeguard those services, or even create privacy and security risks for consumers.

Specifically, Section 6-48.1-7(b)(4) creates significant concerns. It requires contracts between a controller and processor give the controller an "opportunity to object" to the processor's subcontractors.

We recognize the need for a consumer's data to be protected regardless of whether the data are held by a processor or by the processor's subcontractor. However, we strongly recommend a different approach: requiring processors to *notify* a controller about the use of a subcontractor and pass on the processor's obligations to that subcontractor — but not requiring controllers have the opportunity to object to subcontractors. This issue is particularly important, because of the frequency with which processors engage subcontractors to provide services requested by controllers. In many cases, processors will rely on dozens (or more) of subprocessors to provide a single service and may need to replace a subcontractor quickly if the subcontractor is not able to perform a service due to operational, security, or other issues. Requiring that controllers have an opportunity to object slows down the delivery of services and products to consumers, without clear benefits to privacy. Indeed, if a processor needs to switch subcontractors quickly because of a security issue, the delay involved in providing a controller the opportunity to object to a new subcontractor may expose consumers' data to security and privacy risks.

Instead of creating an opportunity for controllers to object to a processor's subcontractors, we recommend revising HB 7787 to require a processor to notify a controller about subprocessors and pass on obligations to subcontractors via contract. This approach ensures consumers' personal data remains protected.

III. Promote an Interoperable Approach to Privacy Legislation.

Finally, BSA appreciates the sponsor's efforts to ensure that HB 7787 creates privacy protections that are interoperable with protections created in other state privacy laws. 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 Representative Shanley for drafting HB 7787's provisions in a manner that is interoperable with protections included in other state privacy laws, which helps drive strong business compliance practices that can better protect consumer privacy.

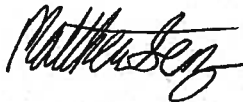
We appreciate the harmonized approach Representative Shanley has taken in aligning many of HB 7787's provisions with the Connecticut Data Privacy Act (CTDPA). BSA supported the

Connecticut privacy law and consumer privacy laws adopted in Colorado and Virginia, which share the same structural model of privacy legislation as Connecticut's law. In particular, we support HB 7787's focus on protecting the privacy of consumers and excluding employment data from the bill's scope and in its definition of "consumer." We also support HB 7787's approach to enforcement, which provides the Attorney General with exclusive authority to enforce the bill, which we believe will help promote a consistent and clear approach to enforcement.

At the same time, we are concerned that the bill provides an effective date of nine months. We strongly encourage you to revise this provision of the bill, to ensure that businesses have at least a year to comply with the bill after enactment. All comprehensive consumer state privacy laws establish such effective dates,⁵ which are important to drive businesses towards strong compliance practices that can better protect consumer privacy

Thank you for your thoughtful approach in establishing strong consumer privacy protections, and for your consideration of our perspective. BSA would be happy to provide further perspective on this legislation as it progresses through the legislative process.

Sincerely,



Matthew Lenz
Senior Director, State Advocacy

CC: Rep. Evan Shanley; members of the House Innovation, Internet, and Technology Committee

⁵ BSA | The Software Alliance, Models of State Privacy Legislation, available at https://www.bsa.org/files/policy-filings/09192023stateprivlaw_0.pdf.