January 17, 2024

Senator President Jeb Bradley
State House Room 302
107 North Main Street
Concord NH 03301

Dear President Bradley:

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates the New Hampshire Senate's work to improve consumer privacy through Senate Bill 255 (SB255). 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.

We appreciate the opportunity to share our feedback on SB255 as the Senate considers whether and how to align SB255 with the bill as amended and passed by the House on January 4, 2024. Our recommendations below focus on BSA's core priorities in privacy legislation: creating privacy laws that are interoperable with other state privacy measures, clearly distinguishing between controllers and processors, and establishing practical obligations for processors, creating workable universal opt-out mechanisms.

[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, 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. Promote an Interoperable Approach to Privacy Legislation.

BSA appreciates efforts to align of many of SB255's provisions with the Connecticut Data Privacy Act (CTDPA). 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. Aligning key features of SB 255 with Connecticut's privacy law can promote strong compliance programs that benefit consumers. However, we are concerned that SB 255 departs from existing state models in three ways that may ultimately weaken consumer protections and confuse individuals who exercise their new privacy rights.

First, Section 507-H:4(II) of the bill authorizes the Secretary of State to establish a secure and reliable means for consumers to exercise their privacy rights. No other state privacy law puts a government official in this role. Instead, state privacy laws recognize that controllers must establish secure and reliable mechanisms for their consumers to exercise new rights, including the rights to access, correct, and delete the personal data that controller holds. As a practical matter, this obligation must fall on each controller — and not on a state actor — because the controller is the company that collects data from an individual consumer, and that will be able to provide, correct, or delete that consumer's information. The Secretary of State does not have access to that information and should not be charged with creating a way for consumers to exercise these new rights. We strongly recommend this language be removed, and controllers be required to establish the means through which consumers will exercise their new privacy rights.

Second, the bill also requires controllers to provide privacy notices that meet standards established by the Secretary of State.[2] Again, this requirement departs from existing laws – which require controllers to provide privacy notices that meet statutory requirements. Those requirements are then enforced by the state's attorney general. It is unclear why SB255 departs from this existing model. By establishing the requirements for privacy notices in a statute, rather than leave them to later agency proceedings, SB255 can create clear expectations for both consumers and companies. We recommend removing this requirement, to align these provisions of SB255 with requirements in other state privacy laws.

Third, as passed by the House, SB255 includes language addressing potential conflicts with other laws. Specifically, Section 507-H:12 provides that, if there is a conflict between two statutes, "the individual or entity shall comply with the statute that provides the greater measure of privacy protection to individuals" and notes that for purposes of the section, "an 'opt in' procedure for an individual to grant consent for the disclosure of personal information shall be deemed to provide a greater measure of protection of privacy than the 'opt out'

[2] SB255, As Amended by the House (Section 507-H6(III), requiring controllers to provide consumers "with a reasonably accessible, clear, and meaningful privacy notice meeting standards established by the secretary of state; Section 506-H:6(V)(a), requiring controllers to establish a privacy notice "consistent with the requirements of the secretary of state"), available at https://www.gencourt.state.nh.us/bill_status/billinfo.aspx?sy=2024 &id=865.

procedure established under this chapter." While we understand that this provision is meant to account for potential new requirements in related privacy legislation, it creates confusion about how a new measure would affect the consumer opt-out rights established in Section 507:H:4(I)(e) of SB255. We encourage you to ensure the new rights to opt out of processing for purposes of targeted advertising, sale, and profiling, remain rights to opt out of these activities, rather than creating opt-in rights that would depart from the opt-out procedures recognized in all other state privacy laws.[3] We encourage you to either strike this language or clarify that this provision does not apply to consumers' rights to opt-out of processing for purposes of targeted advertising, the sale of personal data, or profiling.

As New Hampshire's legislature continues to consider SB255, we encourage you to prioritize harmonizing these requirements with other leading state privacy laws — and ensure that where New Hampshire departs from those other laws it does so in a manner that makes a meaningful contribution to the larger landscape in protecting consumers, rather than diverging without a clear advantage for consumer privacy.

II. Distinguishing Between Controllers and Processors Benefits Consumers.

We want to express our support for SB255'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 by assigning important — and distinct — obligations to both processors and controllers.[4] In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers.[5] 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.[6] BSA applauds the incorporation of this globally recognized distinction into SB255.

---

[3] BSA | The Software Alliance, 2023 Models of State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/us-2023-models-of-state-privacy-legislation.

[4] *See, e.g.,* Colorado's CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Delaware Personal Data Privacy Act, Sec. 12D-102(9, 24); Florida Digital Bill of Rights Sec. 501.702((9)(a)(4), (24)); Iowa Senate File 262 (715D.1(8, 21)); Indiana Senate Enrolled Act No. 5 (Chapter 2, Sec. 9, 22); Montana Consumer Data Privacy Act Sec. 2(8,18); Oregon CPA Sec. 1(8, 15); Tennessee Information Protection Act 47-18-3201(8, 19); Texas Data Privacy and Security Act Sec. 541.001(8, 23); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

[5] *See, e.g.*, Cal. Civil Code 1798.140(d, ag).

[6] 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,

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 SB255'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.

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

While SB255 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 507-H:7(II)(d) 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.

---

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.

Instead of creating an opportunity for controllers to object to a processor's subcontractors, we recommend revising SB255 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.

IV. Consider Practical Issues Involved in Creating a System for Recognizing Universal Opt-Out Mechanisms.

We believe that consumers should have clear and easy-to-use methods to exercise new rights given to them by any new privacy law. Like the state privacy laws enacted in Colorado and Connecticut, SB255 includes a clear requirement for controllers to honor a consumer's use of a universal opt-out mechanism to exercise new rights to opt out of targeted advertising or the sale of their personal data. Under Section 507-H:6(V)(a)(1)(B), controllers must honor these mechanisms no later than January 1, 2025.

If the bill retains this requirement, we strongly encourage you to focus on creating a universal opt-out mechanism that functions in practice. It is important to address how companies will understand which universal opt-out mechanism(s) meet SB255's requirements. One way to address this concern is by creating a clear process for developing a public list of universal opt-out mechanisms and soliciting stakeholder feedback as part of that process, similar to the approach contemplated in Colorado's draft privacy regulations.[7] Focusing on the practical aspects of implementing this requirement can help companies develop strong compliance programs that align their engineering and other resources accordingly. We also encourage you to focus on recognizing a universal opt-out mechanism that is interoperable with mechanisms recognized in other states. Interoperability is essential in ensuring that any universal opt-out mechanism is workable and allows consumers to effectuate their rights across state lines.

We also appreciate that SB255 includes an effective date that recognizes the ongoing work surrounding the implementation of global opt-out mechanisms in Colorado and Connecticut. Ensuring that SB255's obligation to honor a universal opt-out mechanism does not take effect until after January 1, 2025, will help companies leverage that ongoing work to better serve consumers in New Hampshire — and help to ensure that consumers in New Hampshire can use opt-out mechanisms they may already be familiar with in other states.

Finally, as you consider how to ensure any universal opt-out mechanism works in practice, we recommend educating consumers about what universal opt-out mechanisms do in addition to their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer's personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser. Consumers should be aware of this and other limitations.

[7] *See* Colorado Attorney General's Office, Colorado Privacy Act Rules (final rules) (Mar. 15, 2023), available at https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.

Thank you for your thoughtful approach in establishing strong consumer privacy protections in New Hampshire and for your consideration of our perspective. BSA would be happy to provide further perspective on this legislation.

Sincerely,

Matthew Lenz
Senior Director, State Advocacy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org