June 25, 2026

Senator Cynthia Creem
Majority Leader
24 Beacon St., Room 312-A
Boston, MA 02133

State Representative Michael Moran
Majority Leader
24 Beacon St., Room 343
Boston, MA 02133

Senator Barry Finegold
Chair, Joint Committee on Economic Development and Emerging Technologies
24 Beacon St., Room 109-D
Boston, MA 02133

State Representative Tricia Farley-Bouvier
Chair, Joint Committee on Advanced IT, the Internet & Cybersecurity
24 Beacon St., Room 274
Boston MA, 02133

Senator Patrick O'Connor
Assistant Minority Leader
24 Beacon St., Room 419
Boston, MA 02133

Representative David Vieira
Third Assistant Minority Leader
24 Beacon St., Room 167
Boston, MA 02133

Sent via email

RE: Conference Committee for Privacy Legislation in Massachusetts

Dear Members of the Conference Committee:

The Business Software Alliance[1] supports strong privacy protections for consumers and appreciates the legislature's work in advancing consumer privacy in Massachusetts. BSA is the leading advocate for the global software industry. Our members create the business-to-business technologies used across industry sectors. For example, BSA members provide cloud storage services, customer relationship management software, and collaboration software.

As the Conference Committee considers privacy bills passed in both chambers, we want to highlight key concerns with both bills, including how they apply to processors, which handle data on behalf of business customers. We appreciate that S. 2619 and H. 5479 recognize the roles of both *controllers*, which decide how and why to collect a consumer's personal data, and *processors*, which handle data on behalf of another company and pursuant to that company's instructions. The distinction between controllers and processors dates back more than 40 years, underpins privacy laws worldwide, and is in all state comprehensive consumer privacy laws.

[1] BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

BSA is concerned with provisions in both the Senate and House bills, including:

- Enforcement provisions in the House bill that create a private right of action;
- Broad definitions of processors in both bills, which expand the bill in unique and untested ways to regulate not just consumer privacy but also government contracting; and
- Obligations for processors in both bills that do not fit a processor's role — and that may inadvertently undermine security or harm services provided at scale.

We expand on these concerns below and would welcome an opportunity to further discuss these issues with you and your staff as you work to adopt consumer privacy legislation.

1. Enforcement Should be Led by Regulators, Not Private Litigants.

While we recognize and share the Legislature's goal of increasing privacy protections, we have significant concerns with the House bill's enforcement provisions, which create a private right of action against large data holders. BSA supports robust and exclusive enforcement by a state Attorney General, because Attorney Generals are well positioned to provide clear guidance to companies and to prioritize enforcement actions that consistently address the most significant risks to consumers. In contrast, a private right of action leads to differing opinions across courts and creates incentives to focus on vague or ambiguous portions of a law, rather than prioritizing core safeguards that protect consumers.

The House bill raises this concern. BSA supports the Senate bill's approach.

- S. 2619: Sec. 10(a) provides the Attorney General with exclusive authority to enforce the legislation and does not create a private right of action.
- H. 5479: Sec. 14(a)(2) allows individuals to bring a private right of action against large data holders.

BSA Recommendation: The enforcement provisions should give exclusive authority to the Attorney General and not create a private right of action, in line with the Senate bill Sec. 10(a).

2. A Consumer Privacy Bill Should Focus on Private Entities, Not Government Contractors.

Both bills adopt a concerning and expansive definition of processors, which extend the scope of the bills beyond creating consumer privacy protections and into regulating government contracting. The definitions of processors in the House and Senate bills are at odds with the globally-recognized definition of processor, as a person "who processes personal data on behalf of a controller."[2] Instead, both bills would regulate processors that handle data not only on behalf of controllers, but also processors that handle data on behalf of government agencies — even though government agencies are not themselves regulated by either bill. We strongly recommend against this unique, expansive, untested approach.

Both bills raise this concern.

- S. 2619: Sec. 1 defines a processor as "a person who collects, processes or transfers personal data on behalf of, and at the direction of, a controller or another processor *or a federal, state, tribal or local government entity*" (emphasis added).

[2] *See* Business Software Alliance, Controllers and Processors: A Longstanding Distinction in Privacy (last revised April 2, 2025), *available at* https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

- H. 5479: Sec. 1 defines a processor as "a person who collects or processes personal data on behalf of, or at the direction of: (i) a controller; (ii) another processor; or *(iii) a federal, state, tribal or local government entity*" (emphasis added).

BSA Recommendation: The definition of processor should be narrowed to "a person who processes personal data on behalf of a controller." It should not include persons acting on behalf of government entities.

3. Processors Should Have Incentives to Store Data Securely — Not to Look Through Their Business Customers' Data.

Companies hire processors to keep their data secure —– and privacy laws should not encourage processors to look through their business customers' data when they otherwise would not. Both the House and Senate bills create incentives for processors to start looking at more data, by putting an obligation on the processor not to handle personal data if its customer (the controller) violates the law. To comply with this type of obligation, a processor may need to start looking through its business customers' data to second-guess whether its business customers are compliant with the law. That results in more companies looking at consumers' data, not less, and is fundamentally at odds with the role of a processor, which is charged with handling personal data on behalf of a controller and pursuant to its instructions.

Both bills raise this concern, with the Senate language even more concerning than the House language.

- S. 2619: Sec. 6(f) raises this concern by forbidding processors from processing personal data on behalf of a controller if it has "reason to believe" the controller has violated the law.
- H. 5479: Sec. 9(e) raises this concern by forbidding processors from processing personal data on behalf of a controller if the processor has "actual knowledge" the controller has violated the law.

BSA Recommendation: This provision should be stricken from the final bill.

4. Processors Need to Combine Data to Provide Services at Scale.

A privacy law must support companies' ability to provide services at scale. Processors often provide the same service to hundreds or thousands of business customers at scale — creating more affordable, accessible technologies. Updating those services requires combining data from multiple customers, so the service works better for all who use it. For example, a processor that provides cloud storage to thousands of businesses may combine data about how the service functions across business customers — to create improvements that benefit all customers. Both the House and Senate bills restrict processors from combining data received from different sources, which can inadvertently harm services provided at scale. The House language is meaningfully better than the Senate language, however, by clearly allowing processors to combine personal data at the direction of a controller.

The Senate bill raises this concern. BSA prefers the House bill's language.

- S. 2619: Sec. 6(b)(v) raises this concern by prohibiting a processor "from combining personal data that the processor receives from or on behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual."
- H. 5479: Sec.9(b)(2)(v) raises similar concerns but with significantly improved language, by prohibiting a processor "from combining personal data that the processor receives from or on

behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual *unless directed to do so by the controller*" (emphasis added).

BSA Recommendation: If this provision is retained in the final bill, the House language should be used, from Sec. 9(b)(2)(v).

5. Processors' Role in Handling Consumer Rights Requests Should be Clearly Addressed.

Consumers must be able to exercise their new rights when data is held by processors, but we are concerned with language in the Senate bill that affects this process. When consumers request personal data held by a processor, the processor's role is to assist the controller in fulfilling the request. The processor and controller can either work together to respond to requests one-by-one, or the processor can provide a scalable tool for the controller to use in accessing and updating data. All state consumer privacy laws recognize this proven approach with very specific language. We are concerned with language in the Senate bill that erroneously suggests processors must "utilize" such measures, rather than providing measures to controllers for the controller to utilize.[3]

The Senate bill raises this concern. BSA supports the House bill's approach.

- S. 2619: Sec. 6(a)(i) raises this concern by stating that processors' assistance to controllers shall include "*utilizing* appropriate technical and organizational measures" (emphasis added).
- H. 5479: Sec. 9(a)(1) does not raise this concern, because it aligns with the language already used across other states to ensure that consumer rights requests function in practice. It states: "taking into account the nature of processing and the information available to the processor, by appropriate technical and organization measures, insofar as is reasonable, to fulfil the controller's obligations to respond to consumer rights requests."

BSA Recommendation: The final bill should adopt language in the House bill, Sec. 9(a)(1).

6. Controllers Should Not Have a Right to Object to Subprocessors.

Processors often rely on a network of subprocessors to provide products and services their business customers expect. Sometimes the processor will need to change subprocessors quickly, such as when a subprocessor suffers a data breach or cannot provide the underlying service. Creating a right for controllers to object to subprocessors slows down these services — and can be unworkable when subprocessors are used to provide services at scale to thousands of businesses and a single business customer objects. Instead, processors should ensure that data remains protected when it is handled by a subprocessor by passing on their obligations to subprocessors and notifying the controller a subprocessor is being used.

Both bills raise this concern.

- S. 2619: Sec. 6(b)(iv) raises this concern by giving controllers an opportunity to object to subcontractors.

[3] For more information on the role of processors in fulfilling consumer rights requests, *see* Business Software Alliance, Consumer Rights to Access, Correct, and Delete Data: A Processor's Role, *available at* https://www.bsa.org/policy-filings/consumer-rights-to-access-correct-and-delete-data-a-processors-role.

- H. 5479: Sec. 9(b)(2)(iv) raises this concern by giving controllers an opportunity to object to subcontractors.

BSA Recommendation: This provision should be stricken from the final bill.

7. Controllers Should Not Be Required to Provide a List of Third Parties with Which They Share Personal Data.

A privacy law should not require controllers to start tracking new information about consumers. We are concerned that giving consumers a right to obtain a list of specific third parties to which a controller transfers their personal data will do just that — and require controllers to create extensive lists that may end up undermining privacy protections, instead of providing transparency to consumers. While both the Senate and House bills raise this concern, the House language is markedly better by focusing this right only on data that is "sold" rather than "transferred" and by allowing controllers to provide a list of third parties to which any personal data is provided, instead of requiring a consumer-by-consumer list that will result in even more granular data collection about individual consumers.

Both bills raise this concern, but BSA prefers the House language

- S. 2619: Sec. 4(a)(ii) raises this concern by giving consumers the right to "obtain from a controller a list of third parties to which the controller has *transferred* the consumer's personal data."
- H. 5479: Sec. 4(a)(2) raises this concern by giving consumers the right to obtain "a list of third parties, other than natural persons, to which the controller has *sold* either: (i) the consumer's personal data; or (ii) any personal data, provided, however, that such conformation or access shall not require the controller to reveal a trade secret."

BSA Recommendation: If the final bill retains this provision, the House language should be used.

* * *

As you consider how to protect consumer privacy in Massachusetts, we would welcome the opportunity to discuss these issues with you and to provide our views on other aspects of consumer privacy legislation.

Sincerely,

Kate Goodloe
Managing Director, Policy
Business Software Alliance