Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

SIIA

July 7, 2026

The Honorable Cynthia Stone Creem
State House–321 A
Boston, MA 02133

The Honorable Michael J. Moran
State House–Room 343
Boston, MA 02133

The Honorable Barry R. Finegold
State House–Room 109-D
Boston, MA 02133

The Honorable Tricia Farley-Bouvier
State House–Room 274
Boston, MA 02133

The Honorable Patrick M. O'Connor
State House–Room 419
Boston, MA 02133

The Honorable David T. Vieira
State House–Room 167
Boston, MA 02133

Delivered via email

RE: Comments on the Committee of Conference on the Disagreeing Votes of the Two Branches on Senate, No. 2619 and House, No. 5479, both entitled, "An Act Establishing the Massachusetts Data Privacy Act."

To the Honorable Chairs and Members of the Conference Committee:

On behalf of the Software & Information Industry Association (SIIA) and the Computer & Communications Industry Association (CCIA), we write to share concerns and recommend targeted workability amendments to H.5479 and S.2619, *An Act establishing the Massachusetts consumer data privacy act*. We appreciate the Senate and House of Representative's work to advance comprehensive privacy protections, and we offer these comments for the conference's consideration.

Our associations collectively represent over 400 companies of all sizes, from startups and growth companies to global providers of software, data analytics, educational technology, digital services, internet platforms, and communications technologies, including many

companies that do business in Massachusetts. We share the Commonwealth's goal of ensuring that Massachusetts residents are protected from genuine privacy harms.

We also share a core priority with the legislature: that privacy protections should shift the burden away from individuals and toward organizations that collect, use, and disclose personal data. However, highly prescriptive or Massachusetts-specific requirements can inadvertently push that burden back onto consumers through more pop-ups, more notices that few people read, and more "consent theater" – and can further divert resources away from meaningful risk reduction measures, such as data minimization, security, and effective enforcement.

For that reason, our proposed amendments focus on: 1) avoiding unintended consequences that can reduce privacy in practice or create consumer confusion, 2) clarifying obligations in a way that the Attorney General can enforce consistently, and 3) ensuring operational feasibility so protections can be implemented quickly. These include enabling organizations to extend existing, proven privacy programs to Massachusetts without reinventing the wheel within the Commonwealth, particularly for companies testing and scaling newer data driven products. We respectfully request that the Conference Committee incorporate these workability changes in its report.

I. Scope and applicability

We believe the Conference Committee Report should focus on entities with substantial personal data activities, while avoiding coverage triggers that can sweep in small businesses, nonprofits, and entities with incidental sensitive data processing. Overbreadth is not just a business concern, but can also become a consumer privacy issue. Covering low risk entities makes compliance "checklist" driven and dilutes enforcement attention away from actors and practices most likely to cause harm. These fixed burdens also fall especially hard on startups and growth stage firms that are still deciding where to hire, pilot products, and scale new services.

Recommendation: Align applicability thresholds and common exemptions with widely adopted state privacy frameworks so the law is targeted, enforceable, and immediately implementable (S. 2619, Section 2, lines 159–166 (applicability thresholds and sensitive data affiliate trigger); H. 5479, Section 2, lines 223–232 (applicability thresholds, including sensitive data trigger)). A focused scope improves the Attorney General's ability to prioritize meaningful harms and deliver timely consumer protection.

II. Sensitive data and teens: avoid compliance incentives that can reduce privacy

S. 2619 include expansive sensitive data and teen related requirements that could unintentionally increase data collection (S. 2619, lines 132–145 (sensitive data definition,

including “knows or should have known is a child” at lines 141–142); lines 353–354 (known child/COPPA); H. 5479, page 10, line 187 et seq. (sensitive data definition); lines 438–439 (known child/COPPA)). If broad teen protections effectively require age gating services, many organizations, including small businesses, will again feel pressure to collect additional information to determine age or to build new verification workflows. Age verification regimes can themselves be intrusive to privacy and increase security risk by concentrating government IDs, biometric signals, or other sensitive account information in new databases and vendor relationships. Several of the most devastating recent data breaches have arisen directly from age verification requirements.

Age verification also incentivizes online services to reduce their offerings. Companies that cannot reliably determine age without collecting more data may overblock features, apply teen defaults to all users, or withdraw lower risk offerings altogether, which can reduce access to beneficial services without meaningfully improving safety. Those pressures are especially difficult for newer providers offering education, productivity, and creative tools to mixed age audiences. A clearer, risk-based rule tied to actual knowledge will protect young people without infringing on the privacy of all.

Recommendation: Calibrate sensitive-data and teen provisions so they protect minors without encouraging unnecessary age verification or identity collection. A risk based, “actual knowledge” approach (paired with strong default limits on targeted advertising and sale of sensitive data) can better protect young people without producing new privacy risks.

III. Right-size data minimization

We support strong procedural data minimization. But S.2619’s “requested product/service” and strictly necessary framing risks being read to prohibit routine, privacy protective activities (S. 2619, lines 347–349 (sensitive data processing limited to what is strictly necessary for a consumer-requested product or service)) such as cybersecurity, fraud prevention, quality assurance, accessibility, debugging, and reasonable product improvements that benefit consumers. These are not peripheral uses– they make services safer, more reliable, and less invasive over time. This is especially true for AI-enabled services, where debugging, evaluation, and iterative improvement are very often essential to safety and accuracy.

The bill’s current rigidity will likely also incentivize collecting more consumer data. If companies must prove after the fact that every processing activity was strictly necessary to a consumer requested product or service, many will respond by collecting extra information to document necessity, retaining data longer to preserve an audit trail, or limiting beneficial service improvements that reduce errors, abuse, and security risk. It also favors the largest firms that can build state specific controls and documentation layers, while making it harder for smaller

and emerging companies to extend existing privacy programs in Massachusetts quickly, consistently, and effectively. For small or midsize firms, that uncertainty can also delay or narrow availability of products or service to residents while companies assess how ordinary product iteration fits within a nationally consistent compliance framework.

Similarly, restrictions on data processing that do not enhance consumer privacy should be avoided. Prohibiting data processing even after a consumer has consented does not improve privacy and introduces unnecessary compliance burdens that diminish smaller businesses' ability to compete.

Recommendation: Use a well-understood, enforceable minimization standard that limits collection and processing to what is adequate, relevant, and reasonably necessary for disclosed purposes, while requiring heightened protections for sensitive data and incompatible processing. This protects consumers while ensuring organizations can implement the law quickly and consistently.

IV. Publicly available information: reduce consumer confusion and constitutional risk

H.5479's treatment of publicly available information can create consumer confusion (H. 5479, lines 132–146 (definition of publicly available information, with exclusions for inferences revealing sensitive data, biometric/genetic/neural data, and nonconsensual intimate images)), including the mistaken impression that individuals can delete public records or other lawfully published material from circulation. It also blurs the line between private data practices that this bill properly regulates and information that has already been made lawfully available through government records, court filings, journalism, and other widely distributed sources.

That ambiguity creates both legal and practical problems. Organizations use publicly available information for fraud prevention, identity and business verification, sanctions and safety screening, security research, and other legitimate functions that consumers often expect. That includes emerging tools that rely on public sources for verification, safety testing, and research. When the statute treats publicly available information unclearly, entities may overrestrict useful, low risk practices, while consumers receive rights notices that imply remedies the law cannot realistically deliver. That dynamic is confusing for residents, difficult for the Attorney General to enforce consistently, and more likely to generate avoidable First Amendment-related disputes than meaningful privacy gains.

Recommendation: Align the definition of publicly available information with prevailing approaches that include information lawfully made available through government records or widely distributed media, while avoiding requirements that are unclear or difficult to apply in practice. Clear treatment of publicly available information helps ensure consumers receive accurate expectations and enables enforceable rules.

V. Access rights: inferences and third party identification

We agree that meaningful access rights are foundational to any privacy legislation. But requiring access to all "inferences" and requiring controllers to name specific third parties (S. 2619, Section 4(a)(i)–(ii), lines 234–240; H. 5479, Section 4(a)(1)–(2), lines 325–331) can be operationally difficult if not impossible "inferences" and requiring controllers to name specific third parties can be operationally difficult if not impossible, can create security and trade secret risks, and may not provide consumers information that is actually usable. Long lists of specific recipients are more likely to overwhelm consumers than inform them, while also requiring organizations to create new tracking and retention systems to generate the lists, at times increasing data retention simply to comply.

Recommendation: Remove the "inferences" access requirement and replace specific third-party identification mandates with disclosure of categories of third parties. This improves consumer comprehension, reduces incentives to retain more data, and produces clearer, more enforceable obligations.

VI. Deletion and correction propagation: focus on feasible, privacy protective outcomes

Deletion and correction rights are core consumer protections, but overly expansive "downstream propagation" obligations can create infeasible requirements across complex service provider chains (S. 2619, Section 4(a)(iv), lines 243–245, and related response obligations lines 295–300; H. 5479, Section 4(a)(4), lines 334–336 (delete right, including derived data)).” obligations can create infeasible requirements across complex service provider chains. If obligations are impossible to satisfy, the result can be a compliance posture that is more paperwork than privacy, and it can ironically discourage deletion if organizations feel compelled to retain data to sensibly document attempted propagation.

Recommendation: Ensure the statute requires controllers to delete or correct data in their systems and to direct processors to assist, while using a reasonableness standard for notifying third parties where applicable. This approach protects consumers without creating requirements that are difficult to implement, audit, or enforce.

VII. Data protection assessments: protect candor and avoid overwhelming enforcement capacity

H.4746 and S.2619's approach to data protection assessments risks creating a high volume pipeline (S. 2619, lines 531–570 (data protection assessment requirements for heightened risk processing, confidentiality protections); H. 5479, Section 10 (data protection assessments)). that can overwhelm enforcement capacity and reduce the quality of assessments. Mandatory submission of assessments (and public summaries) can chill candid internal analysis, encourage

generic box checking documents, and expose sensitive security information. Especially for smaller teams building newer products, a state specific filing regime can also slow internal review cycles. Furthermore, these assessments require companies to share their subjective views regarding content-based harms, which federal courts have deemed compelled speech.

Recommendation: Require controllers to conduct and retain impact assessments and provide them to the Attorney General upon request, subject to strong confidentiality protections. This supports genuine accountability and enables targeted enforcement, without turning DPIAs into a public filing exercise. Notably, even GDPR based systems are actively exploring ways to simplify and standardize compliance artifacts to reduce administrative burden and improve practical outcomes.

VIII. Enforcement: prioritize consistent remedies and rapid remediation of real harms

We support robust enforcement. A strong, well resourced Attorney General is best positioned to prioritize the highest risk conduct, obtain appropriate remedies, and drive statewide compliance. In contrast, broad private litigation exposure can divert resources toward defensive legal strategy rather than privacy improvements (enforcement generally through Attorney General in both bills; recommend retaining cure opportunities and removing any private right of action or unworkable remedies such as data retrieval).. It can also lead to inconsistent interpretations that confuse consumers rather than delivering them meaningful privacy protections or compensation.

Private rights of action do not replicate the advantages of public enforcement. The Attorney General can prioritize the most serious harms, distinguish technical violations from conduct that creates real consumer risk, and press for statewide remedies that improve practices across the market. Private litigation generally does the opposite. It tends to reward one-off suits over coordinated remediation, encourages claims based on technical or debatable compliance theories, and can push businesses to spend money on motion practice, settlement pressure, and duplicative discovery rather than on fixing underlying practices. Consumers may wait years for uncertain relief, while the main immediate result is often greater litigation cost and less predictable compliance.

Nor do broad private rights effectively create a network of accountable “private attorneys general.” Private plaintiffs and class counsel are not charged with setting enforcement priorities for the Commonwealth, issuing coherent guidance to the market, or ensuring that limited compliance resources are directed toward the highest value privacy protections. The result is more likely to be fragmented litigation and uneven judicial interpretation than faster remediation of genuine harms. For consumers, that means less consistency, less clarity, and less confidence that the law is targeting the practices most worth stopping. Additionally, these

lawsuits generally turn on fact-specific questions related to individual companies' practices, making them difficult to resolve quickly. The high costs of such litigation will ultimately be passed on to Massachusetts taxpayers.

Recommendation: Maintain enforcement through the Attorney General with a reasonable opportunity to cure for good faith compliance efforts, and remove remedies that are unclear or operationally unworkable (such as "retrieval" of data). This reinforces meaningful consumer protection by emphasizing remediation of genuine privacy harms and consistent, accountable enforcement.

* * *

We appreciate your consideration of these recommendations and would welcome the opportunity to discuss practical amendments that strengthen consumer privacy in Massachusetts. Please feel free to contact us if we can be helpful as the Commonwealth continues its work on comprehensive privacy legislation.

Respectfully submitted,

Anton van Seventer
Counsel, Privacy and Data Policy
Software & Information Industry Association (SIIA)
Email: avanseventer@siia.net

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association
Email: ksepe@ccianet.org

Cc: The Honorable Karen E. Spilka, President of the Massachusetts Senate
The Honorable Ronald Mariano, Speaker of the Massachusetts House of Representatives