

October 19, 2023

Representative Tricia Farley-Bouvier, Chair
Joint Committee on Advanced Information
Technology, the Internet and Cybersecurity
State House, Room 274
Boston, MA 02133

Senator Michael Moore, Chair
Joint Committee on Advanced Information
Technology, the Internet and Cybersecurity
State House, Room 109-B
Boston, MA 02133

Dear Chair Farley-Bouvier and Chair Moore,

On behalf of the Greater Boston Chamber of Commerce and our 1,200 members, I write to offer testimony on H.60, *An Act establishing the Massachusetts Information Privacy and Security Act*, and H.83/S.25, *An Act to establish the Massachusetts data privacy protection act*. The Chamber understands the importance of protecting consumers' personal data and privacy. However, legislation that regulates data use and protection must balance adequate protections with legitimate use and customer demand, and the Chamber strongly prefers that be implemented by the federal government.

However, to the extent the Legislature considers state-specific regulation, we urge consistency and requirements that closely mirror those adopted in the majority of other states. Because this legislation will create costs for businesses, and will impact how they execute their services, data privacy is ultimately a competitiveness issue. Harsh regulations have demonstrable impacts on both employers and consumers, and this is playing out in other states. As a leader in innovation and technology development, the Commonwealth must avoid adopting unnecessary obligations that are incompatible with regulations in other states or federal, sector specific standards. Given these competitiveness concerns, we urge the committee to view data privacy standards through the below guiding principles to avoid profound negative consequences.

Competitiveness and Interoperability

Thirteen states enacted comprehensive state privacy legislation in recent years. The majority of these laws take a consistent approach to regulating personal data and reflect an emerging national trend on the protection of data across state lines. As the committee considers data privacy legislation, it should prioritize ensuring a Massachusetts law is as consistent as possible with how most states regulate data privacy. Every Massachusetts obligation that substantially differs from other states puts our innovation economy at a disadvantage, ultimately costing jobs and services. These impacts are not hypothetical – consumers in states with overly burdensome regulations, such as Illinois, lost access to products and services. Businesses will not add jobs or invest in states where they cannot operate or deploy products in a reasonable manner.

In a similar vein, any state-level data privacy legislation should also be consistent with the many federal rules that already adequately protect the use of personal or sensitive data. For instance, data privacy legislation should exempt a variety of health data already protected by HIPAA and other federal laws. The committee should exempt health care institutions and other sectors, such as financial services providers that are already regulated by the Gramm-Leach-Bliley Act, to ensure consistency and avoid duplicious requirements.

Avoid Ad-Hoc or Incremental Steps

We urge the committee to approach data privacy regulations comprehensively, rather than in an ad-hoc or incremental way that targets specific categories of data, such as location data services. Other data privacy bills focus on specific data categories, and while well-intended, do not account for the widespread

and different data uses and protections that exist for other purposes. Instead of addressing data privacy in increments, we urge a nuanced, comprehensive approach.

Understand the Broad Impact and Costs on Businesses

H.60, H.83, and S.25, as drafted, will impact every major employment sector in Massachusetts, not just large technology businesses that often come to mind when we think about data use and privacy. By including low thresholds that trigger certain protections, registration obligations, and other requirements, the potential for unintended consequences is high. Even small- and mid-sized businesses collect data to improve customer service and products by evaluating business operations, offering new and enhanced customer benefits, and receiving supplier and customer feedback. As a result, these bills will create new costs for small- and mid-sized businesses. We urge the committee to consider the unique needs, impacts, and costs to employers where technology development is not the primary focus.

Avoid Ambiguity, Duplication, and Unnecessary Burdens on Employers

Data privacy legislation deals with complex and technical topics, so the specific definitions and details are especially important to successful compliance and implementation. Ambiguous general principles – that may have no legal effect – only muddle new requirements on businesses. Terms such as “adequate,” “reasonable,” and “highly offensive” are subjective and provide no roadmap for compliance. These types of terms occur throughout the bill, and the committee should reconsider any provisions that don’t achieve specific outcomes.

Given the technical nature of the legislation and its potential widespread impact, technical experts from businesses should be at the table to minimize unintended consequences. These experts will also help the committee to ensure the bill is targeted; reflects current data technology, security, and uses; and achieves specific, concrete goals.

Specific Recommendations

1) Private Right of Action

The Chamber strongly opposes Section 14 of the proposed Chapter 93L (in H.83 and S.25) and section 26 of proposed Chapter 93M (in H.60) as it relates to creating a private right of action for breaches of security. A private right of action invites a maelstrom of litigation that will not further the consumer protections proposed by this bill. Rather, the Attorney General’s office is the most appropriate and best situated to enforce the statute.

2) Financial Services Entity Level Exemption

Data privacy protections for personal information collected by financial institutions are regulated by the federal government. It is therefore more appropriate to exempt all financial institutions subject to such regulation from state legislation. The Chamber supports the following exemption language:

A financial institution or an affiliate of a financial institution as defined by and that is subject to the federal “Gramm-Leach-Bliley Act”, 15 U.S.C. SEC. 6801 et seq., as amended, and implementing regulations, including regulation P, 12 CFR 1016.

3) Arbitrary and Excessive Fine Structure

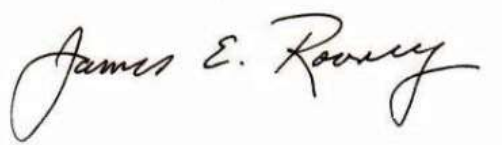
H.83 and S.25 allow a court to impose a civil penalty between .15% and 4% of annual global revenues, or between \$15,000-\$20,000,000 per violation, whichever is greater, along with attorneys’ fees. These fines are extreme in nature and unreasonably punitive – the type of provision that will drive our businesses to other states. H.60, in contrast, allows a court to impose a civil penalty that “exceeds the economic benefit

realized by an entity for noncompliance.” This phrase is wholly undefined and is in addition to \$10,000 fines per violation, injunctive relief, and attorneys’ costs. Fines should be structured in a fair and predictable manner and this unprecedented fine language should be removed from the bills.

In addition, the legislation allows the Attorney General to enforce data privacy protection resulting from similar facts under both Chapter 93A as well as the proposed Chapter 93M. Enforcement of data privacy protection should proceed under one unifying set of regulations, and not be subject to different requirements under different statutes within the same state. The existing draft creates confusion about the rules employers should follow, the resulting obligations, and potential penalties.

We appreciate the committee’s consideration of the Chamber’s comments and encourage committee members to prioritize the state’s competitiveness and ability to support an important and dynamic technology ecosystem in Massachusetts’s economy.

Sincerely,

A handwritten signature in black ink that reads "James E. Rooney". The signature is written in a cursive style with a large, looped initial "J".

James E. Rooney
President and CEO