October 19, 2023

Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
Attn: Christopher Smith
24 Beacon St
Boston, MA 02133

CCIA Comments on MA Data Privacy Legislation (S. 227/H.60, H. 83/S.25, H.63/S. 195)

Dear Co-Chair Moore, Co-Chair Farley-Bouvier, and Members of the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully raise concerns with the slate of data privacy legislation currently being considered by the Committee.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.[2]

CCIA strongly supports the protection of consumer data and understands that Massachusetts residents are rightfully concerned about the proper safeguarding of their data. As the Legislature considers the best path forward, CCIA would urge the body to strongly consider adopting a comprehensive data privacy bill, which includes additional protections for sensitive data (such as biometric data), as opposed to a standalone bill on a single type of data. If the Legislature were to separate out certain aspects of data via the passage of standalone legislation, businesses and consumers may be left uncertain as to what standards are in place,

[1] For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf

and of course there may be unforeseen gaps in privacy protections, which could ultimately result in the legislature having to undertake additional legislative work to address those areas.

When examining key aspects of a comprehensive data privacy proposal, a vital component is promoting interoperability. Consistency among state data privacy laws would avoid the need for significant statutory interpretation and compliance difficulties for businesses covered under the law and allow those businesses to develop one uniform data privacy compliance framework, avoiding significant additional costs. Therefore, a model privacy law, like Connecticut's, which was the first in the New England region to pass a comprehensive data privacy law, should be considered. Since its passage, Connecticut's law has served as a model for other states in the region, with states like Rhode Island, New Hampshire, and Vermont all considering comprehensive data privacy proposals that align with Connecticut's law. If Massachusetts were to follow suit, New England could be poised to essentially create a uniform data privacy standard throughout the region. This would tremendously benefit consumers who would know that their data is protected in the same manner throughout the region. Currently, the two different comprehensive data privacy proposals before the legislature (S. 227/H.60 and H. 83/S.25) differ greatly from any other existing state data privacy law, and therefore CCIA would have concerns if the Legislature were to move forward with either proposal in their current form.

While we believe that efforts to protect biometric data would be better suited being incorporated into a comprehensive data privacy bill, in the interim we offer the following comments on H. 63 and S. 195, in which we highlight several areas of concern.

1. Investing enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

Both H. 63 and S. 195 permits consumers to bring legal action against companies that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Massachusetts' courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Massachusetts, disproportionately impacting smaller businesses and startups across the state. Additionally, studies have shown that law firms are the primary financial beneficiaries from biometric privacy-related lawsuits, as in the eight case settlements involving alleged harm to consumers in Illinois, plaintiffs' lawyers received an average settlement of $11.5 million per firm per case, while individuals received an average settlement of $506 per case.[3] This would likely be magnified in H.63/S.195 as the definition of "harm"

[3] Kaitlyn Harger, *Who Benefits from BIPA? An Analysis of Cases Brought Under Illinois' State Biometrics Law* (April 2023) https://progresschamber.org/new-study-exposes-impact-of-illinois-biometric-privacy-law/

included in the legislation is far from specific, and therefore would likely create unnecessary confusion and challenges for businesses complying with the act. Furthermore, investing sole enforcement authority with the state attorney general allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA recommends that the legislation be amended to include a cure period of at least 30 days. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government's limited resources on enforcing the law's provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential privacy changes rather than shifting focus to defending against litigation.

2. The terms defined in the bill should be amended to promote interoperability with other states.

Several definitions included in H. 63 and S. 195 should be amended in order to align with privacy laws that are already in place throughout the country. First, the definition of "biometric information" should be amended to include language that addresses data generated by the automated measurements of a consumers' biological characteristics, in order to align better with language from Virginia, Colorado, and Washington's laws. Additionally, the "biometric information" definition in H. 63 should fully exempt photos and videos, as to match the language included in the laws in the three aforementioned states. Proposed amended language is included below:

"Biometric information" or "biometric data" means information or data generated by automatic measurements of an individual's measurable biological or behavioral characteristics ~~of an individual~~ that is used singularly, or in combination with each other, or with other information, for verification, recognition, or identification of a specific individual. Examples include but are not limited to fingerprints, retina and iris patterns, voiceprints, D.N.A. sequences, facial characteristics and face geometry, gait, handwriting, keystroke dynamics, and mouse movements.

Biometric information does not include writing samples, written signatures, mere photographs or videos, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

* * * * *

We appreciate the Joint Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Alexander Spyropoulos
Regional State Policy Manager - Northeast
Computer & Communications Industry Association