



**June 26, 2023**

Joint Committee on Consumer Protection and Professional Licensure  
Attn: Marissa Dakin and Dana Mascari  
24 Beacon Street  
Boston, MA 02133

**Re: S. 184/H.386 - An Act relative to consumer health data.**

Co-Chair Cronin, Co-Chair Chan and Members of the Joint Committee on Consumer Protection and Professional Licensure:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully raise concerns with S. 184 and H. 386, acts relative to consumer health data, as currently drafted.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.<sup>1</sup> 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.<sup>2</sup>

CCIA strongly supports the protection of consumer data and understands that Massachusetts residents are rightfully concerned about the proper safeguarding of their data, particularly when it comes to their health information. However, as currently written, S. 184 and H. 386 include several provisions that raise concerns. We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

**1. Amend and add to the definitions included in the bill.**

***“Consumer health data” should be more narrowly defined.***

While CCIA understands and supports the intent of the legislation, S.184/H.386 defines “consumer health data” so broadly that it would include data about daily consumer activities and purchases, by including “efforts to research or obtain health services or supplies” and any data that relates to “bodily functions”. This broad

<sup>1</sup> 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>.

<sup>2</sup> 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>



definition could apply to regular purchase items such as feminine care products, sexual health products, undergarments, or items as simple as toilet paper. By including routine purchases such as hygienic products within the scope of this legislation, consumers would constantly be required to provide consent in the course of normal transactions. This would inevitably lead to consent fatigue while not actively contributing to accomplishing the legislation’s intent.

Additionally, the definition of “consumer health data” should focus on the “health condition” of the consumer, specifically any personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a regulated entity uses to identify the past, present or future health status condition of the consumer.

***“Biometric data” should be more narrowly defined.***

Biometric Data should be narrowed to focus on automatic measurements and data used to identify a specific individual. The definition should also clarify that biometric data does not include a digital or physical photograph, audio or video recording; or any data generated from either unless such data is generated to specify a specific person. We suggest utilizing the following language, which mirrors definitions used in Montana, Iowa, and Virginia.

“Biometric data” means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual.

***“Sale” should be more amended to expand the list of what does not constitute a sale.***

The list of what does not constitute a “sale” should be expanded to include the following:

- With a processor in a manner consistent with the purpose for which the consumer health data was collected;
- With a third party for the purpose of providing a product or service requested by the consumer to whom the consumer health data pertains;
- With an affiliate of the person who is providing or disclosing the consumer health data;
- As directed by the consumer to whom the consumer health data pertains or where the consumer to whom the consumer health data pertains intentionally uses the person who is providing or disclosing the consumer health data to interact with the third party to whom the consumer health data is provided or disclosed;
- Where the consumer has intentionally made the consumer health data available to the general public through mass media that was not restricted to a specific audience.

Each of these provisions align with the consumer’s preferences and interests and therefore would not inhibit the overall goal of the legislation of limiting unapproved sharing of consumer health data.



### ***“Share” should be more amended to align with existing privacy laws.***

The definition of “share” as included in the bills should align with the exceptions that are included in other privacy laws. CCIA suggests that “share” not include the following: (i) disclosure of biometric identifiers to a third party when it is considered as part of a merger, acquisition, bankruptcy, or other transaction in which another third party assumes control of all or part of a person’s assets; (ii) by a person to a processor that processes the biometric identifiers on behalf of a person; (iii) to a third party for purposes of providing a product or service requested by the consumer; (iv) the disclosure or transfer of a biometric identifier to an affiliate of the person; (v) where the consumer directs the person to disclose the biometric identifier or intentionally uses the person to interact with a third party; or (vi) that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience.

### **2. Establish a timeline for operators to respond to consumer requests.**

As currently drafted, S. 184/H.386 provides operators with 30 days to respond to a consumer’s request to exert their rights as established under the act. We suggest that the language be amended to provide operators with the option to extend their respond window by 45 days based on the complexity and number of requests for the same consumer. This would provide operators with the ability to fully comply with consumer requests in a comprehensive manner without fear of being subject to a penalty, and many states with privacy laws provide an extension period for operators when responding to and processing consumer requests.

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

S.184/H.386 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. Further, every state that has established a comprehensive consumer data privacy law – California, Colorado, Connecticut, Indiana, Iowa, Utah and Virginia – has opted to invest enforcement authority with their respective state attorney general. This 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.

**4. A clear and sufficient timeline should be established in order to allow covered entities to understand and comply with newly established requirements.**

S. 184/H.386 currently does not provide any timeline by which the proposed act would take effect. CCIA recommends that any legislation advanced in Massachusetts include sufficient lead time to allow businesses to establish systems to bring themselves into compliance with the new regulations. Therefore we suggest an effective date of no earlier than January 1, 2025 be included in the legislation, mirroring timelines established by other states, such as California, Connecticut, and Colorado, who have passed similar data privacy laws.

\* \* \* \* \*

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

Sincerely,

Alex Spyropoulos  
Regional Policy Manager, Northeast  
Computer and Communications Industry Association