October 29, 2021

The Honorable Mark C. Motigny
State House
24 Beacon St., Room 312-C
Boston, MA, 02133

The Honorable Michael O. Moore
State House
24 Beacon St., Room 109-B
Boston, MA, 02133
Via Email

RE: MA S.220, An Act to Protect Personal Biometric Data

Dear Senator Motigny and Senator Moore:

The Software & Information Industry Association (SIIA) writes to provide testimony on S.220, "An act to protect personal biometric data," which was subject to a hearing on October 13, 2021. SIIA is the principal trade association for the software information and digital content industry representing more than 450 technology companies, including the global industry leaders for the digital age: software, data analytics, and information service companies. SIIA's members reflect the broad and diverse landscape of digital content, including B2B and B2C services, specialized providers, and large multinational industry leaders.

We appreciate the legislature's leadership on protecting consumer rights and strengthening data privacy safeguards, with a focus on biometric data. We also appreciate the special risks that misuse of biometric data poses to consumers and applaud your attention to this important issue. Biometrics have grown in use and availability, because of their high level of accuracy in identifying and authenticating individual human traits and their potential to further safeguard consumers' security and safety. We agree that consumers should have the right to appropriate notices and consents concerning the collection, retention, destruction, and disclosure of their biometric information in business operations, as stated in the bill.

While we understand the need for strong consumer protections with regard to sensitive biometric data, we address two important concerns with S.220. First, we are concerned that the scope of the proposed act is not tailored to the many current and unknown future uses of biometric data. Related to this, the definitions of "biometric identifier" and "biometric information" do not reflect the current state of technology and the myriad uses of biometric data in private, commercial and public settings. Tailoring implementation and consumer consent procedures to a risk-based and use-based reasonableness standard would help address problems that consumers face without creating unintended problems based on how

technology is used in many practical ways today, including for routine authentication purposes. Second, we are concerned that including a private right of action (PROA) in the bill, which deviates from common practice in other privacy laws, will create unforeseen problems and lead to increased costs for consumers. We believe that addressing these concerns will create harmony for businesses and consumers in the policy's efficiency and effectiveness.

1. Adopting Biometric Policies that are Flexible and Future-Proof

As noted, our first concern broadly focuses on the fact that S.220, in merely a single legislative effort, would govern a complex array of issues and applications of biometric technology and biometric data, running the gamut from personal and commercial applications to law enforcement activities. In its current form, the legislation would both restrict everyday uses of this beneficial (and in many cases non-invasive) technology, and risks being quickly outmoded by changes in consumer expectations surrounding its use.

As written, the definitions of "biometric identifier" and "biometric information" should not include digital photographs, audio recordings, and speech-to-text services, which are derived from biometric data and are fairly routine in both commercial and private settings. Because there are numerous openings for the existing legislative definitions to be misapplied, we recommend that the legislature provide additional opportunities for public input and stakeholder consideration, including practical examples of valuable, low-risk uses of biometric data, so as to create flexibility for the definitions in draft. We therefore recommend that the legislation allow more flexibility to use biometric data, depending on the context and setting of the application.

In addition, we recommend that the act focus on particular uses and/or decision-based outcomes of concern to legislators, rather than, broadly, to any technology that generates "biometric information" or "biometric identifiers." Focusing on the technologically-neutral harms that can flow from particular uses and decision-based outcomes will result in a more stable and predictable regime rather than a blanket burden on a particular technology that may be upgraded, obsolete or become fairly common in days or years. A risk-based focus on outcomes rather than technology limits potential overbreadth and chilling effects on new technologies..

Illinois's Biometric Privacy Act (BIPA) law serves as an example of the ill effects of overbroad, technology-specific regulation.[1] Since the law took effect in 2008, it has led to numerous unintended consequences. In July 2017, for example, twenty-six class action lawsuits were filed by employees who claimed their employers violated BIPA's consent, notice, and disclosure policies because their time clocks required employee fingerprints.[2]There were no allegations that their biometric information was shared outside the confines of that relationship, that the employer used sub-standard security, or that their privacy was materially violated in any way. This kind of liability serves only to make legitimate uses of the

[1] 740 ILCS 14/ Biometric Information Privacy Act. (ilga.gov)

[2] Illinois employers flooded with class-action lawsuits stemming from biometric privacy law. IllinoisPolicy.org.

technology (in this case, ensuring accurate wage and hour records) more expensive without any meaningful privacy benefit.

2. Limiting Private Right of Action (PROA) to Cases Involving Injury in Fact

These harms are compounded by the presence of private rights of action with statutory damage multipliers. Section 3 of S.220 permits any "person aggrieved" to recover no less than $5000 per violation, even without any proof or evidence of actual harm. Given the standards in the bill and the ability to aggregate claims into a class action under Massachusetts law, this provision would potentially create staggering liability for technical violations, which impose no harm on consumers, and which are typically quickly rectified by the business. Any person whose information was kept in an "unreasonable manner" would have standing to sue. Given that information is routinely processed in the thousands, this will lead to crippling liability. This provision would create a pathway to abuse and have significant unintended consequences.

We are concerned that our members will be threatened with lawsuits that they will be forced to settle meritless claims not due to any violations of the statute, but because of the fact-specific nature of the word "unreasonable" and the multiplying effect of statutory damages. This kind of litigation tactic has become more common, yet it neither advances innovation nor protects consumer privacy. What it will do, however, is to chill the beneficial uses of this technology; potentially drive software, data analytics, and information service companies out of the state or deter them from entering the state; and increase the costs to the consumer to insulate against this kind of risk. We believe exclusive Attorney General enforcement with a 30-day right to cure, which will by its nature involve the exercise of discretion, will focus on those instances most likely to create risk or cause actual harm and not create the plaintiff's bar feeding frenzy that statutory damages have caused in other areas.

We therefore strongly recommend that Massachusetts follow the lead of other states that have rejected private rights of action in their consumer privacy legislation. For example, the Virginia Consumer Data Protection Act (VCDPA) is a consumer privacy law that recently passed and is widely considered as a model for other states. VCDPA defines biometric information as one subset of sensitive personal information and defines the parameters for businesses to gather customer consent for use of sensitive personal information. To simplify implementation, VCDPA does not include a private right of action. We recommend following this guidance and removing this provision.

Biometrics are now integral to authenticating customer identities in many daily operations: banking and retail activities, airport security, law enforcement and more. Removing the private right of action closes the door to unnecessary and immaterial cases being brought without an injury in fact. It allows the digital ecosystem to continue to leverage safe, secure and high-quality technology that benefits consumers, without stifling innovation.

We appreciate your willingness to accept this statement in regard to this bill on protecting biometric data. If you have further questions, please contact Divya Sridhar, at dsridhar@siia.net.

Sincerely,

Divya Sridhar, Ph.D.

Senior Director, Data Policy