March 7, 2022

Senate Committee on Ways and Means
Sen. Michael J. Rodrigues, Chair

Re: S.2687, An Act establishing the Massachusetts Information Privacy and Security Act

Dear Chairman Rodrigues and members of the Ways and Means Committee,

The undersigned consumer, privacy, and workers' rights groups write to encourage you to advance and strengthen S.2687, An Act establishing the Massachusetts Information Privacy and Security Act ("MIPSA"). Our organizations strongly supported the original version of this legislation (S.46/142) filed by Senator Creem and Reps. Vargas and Rogers, and we hope we can continue to be involved in its development going forward.

We applaud the Chairs of the Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity for prioritizing legislation regarding consumer data privacy and acknowledge their significant effort to advance a comprehensive privacy bill. Overall, the bill retains good and reasonable provisions, and it remains an improvement over certain other bills that are being filed across the country. However, we were disappointed to see some provisions removed that would ensure the legislation would have a more meaningful and long-lasting impact on Massachusetts' residents' privacy rights. We encourage you to reinstate some of the core principles from the original text into this bill as it moves forward.

A twenty-first century data privacy law should provide baseline protections for data privacy as a rule, not an exception. It should lay out rules and limitations on what companies can and cannot do with personal data, rather than putting the burden on ordinary people to individually protect their data, website by website, app by app.

<u>What does MIPSA get right?</u>

To begin, we want to highlight provisions of MIPSA that would meaningfully advance personal privacy in the Commonwealth. Specifically, the bill:

- Establishes that the acceptance of broad terms of use cannot be considered lawfully given consent for purposes of collecting and processing personal information;
- Includes important principles for the collection and processing of personal information from established European data privacy law;

- Recognizes foundational privacy rights (i.e., right to data portability, right to delete, right to correct personal information) and regulates their exercise;
- Regulates data brokers so that Massachusetts residents can understand who is who in the personal information marketplace;
- Opens the door to ban pay-for-privacy schemes in the Commonwealth;
- Grants robust enforcement and investigative authority to the Attorney General ("AGO"), and provides for a funding architecture to ensure the AGO has the resources it needs to enforce the law; and
- Establishes the new privacy law as a "floor" that should not preempt stronger municipal privacy protections.

How can we strengthen MIPSA?

The Senate Committee on Ways & Means should build upon what the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity did and strengthen MIPSA in the following ways:

- Require companies to comply with strict data minimization provisions;
- Generally prohibit profiteering from the sale of sensitive data, such as location information and biometric information;
- Protect workers against inappropriate electronic monitoring on the job; and
- Strengthen the enforcement provisions of the bill.

To this end, we offer the following recommendations:

- **MIPSA should be amended to incorporate stronger data minimization provisions.** In the absence of a complete opt-in framework for consent, the bill should incorporate stricter data minimization rules. Companies should not collect and process an indefinite amount of information. Instead, they should be legally limited to collecting, processing, maintaining, and disclosing only the amount of information necessary to achieve a limited purpose like offering a service or a good to an individual. Section 12 of Senator Markey's Privacy Bill of Rights Act provides a good example of strong data minimization provisions.[1]

- **MIPSA should be amended to forbid the sale and trade of our location data on the open market.** Knowing a person's every movement can not only expose sensitive details about their activities and habits, but can also put them in grave danger of severe physical harm or psychological harm. It seems as though the intent of the Joint Committee was for MIPSA to enable people to restrict companies' use of location information and other sensitive information, but clarifying language should be added to make this unambiguous. Section 6(e) explicitly requires opt-in consent from minors to sell their personal information. A similar provision prohibiting the sale of *all* sensitive information —and not only personal information relative to minors—without express, affirmative opt-in consent should be added, at a minimum. As currently drafted, the specificity for minors, and lack thereof regarding sensitive information pertaining to everyone else, is likely to be used by companies to interpret the intent of the statute narrowly.

[1] S. 1214 (116th Cong.). https://www.congress.gov/116/bills/s1214/BILLS-116s1214is.pdf.

- Location information reveals the most intimate things about each of us: where we live, where we work, where we socialize, with whom we visit, our religious affiliation, our political views and habits, our healthcare needs and choices, and more. Unfortunately, we've seen how such information has been sold and abused. For example, in 2017, anti-abortion groups in Massachusetts used location data to target ads to people that were near health care facilities with the intent of interfering with the exercise of their reproductive rights.[2] In 2019, AT&T was accused of selling customers' real-time location data to credit agencies and bail guarantors, along with bounty hunters and stalkers.[3] At the federal level, Senator Ron Wyden has introduced federal legislation called "The Fourth Amendment is Not for Sale Act" to rein in this out-of-control market for personal location data, but that federal legislation has not moved. Massachusetts must intervene to protect consumers from this dangerous and unregulated activity. This is particularly true given that many companies engaged in the collection and sale of location data are not household names, and are unknown to most people.

- **MIPSA should be amended to prevent companies from collecting and selling biometric data without specialized consent.** Biometric data like our face prints and other biometric identifiers are especially sensitive and deserve strong protection in the law. The nation's gold-standard biometric privacy law, the Illinois Biometric Information Privacy Act (BIPA), requires companies to obtain affirmative consent before even *collecting* a person's biometric information. Unfortunately, MIPSA contains no such provision, so if it advances we urge the Committee to restore this important protection that was present in the original version of the bill. And, similar to the issue with location data raised above, clarifying language needs to be added to make clear the Joint Committee's intention to prohibit the *sale* of biometric data without express, affirmative opt-in consent, at a minimum.

- **MIPSA should be amended to provide employment protections against excessive electronic monitoring and management in the workplace**. The original language of S.46/H.142 inserted a new section in G.L. 149 that would protect workers against excessive electronic monitoring and limit the use of this monitoring as the sole basis of employment decisions. That language should be restored.

    - The limitation on excessive electronic monitoring in workplaces is necessary because employers have already begun using a variety of monitoring systems that—if left unchecked—will continue to harm workers. These systems span a wide array of industries. Warehouse workers faced automated firings due to unrealistic productivity quotas,[4] call center workers were wrongly penalized by faulty voice recognition software,[5] and remote tech workers risked losing pay if they failed to

---

[2] Curt Woodward and Hiawatha Bray, A Company Sent Anti-Abortion Ads By Phone. Massachusetts Wasn't Having It, The Boston Globe, April 2017. https://www.bostonglobe.com/business/2017/04/04/healey-halts-digital-ads-targeted-women-reproductive-clinics/AoyPUG8u9hq9bJUAKC5gZN/story.html

[3] Allison Matyus, AT&T Accused Of Selling Customers' Location Data To Bounty Hunters And Stalkers, Digitaltrends, July 18, 2019. https://www.digitaltrends.com/news/att-accused-of-sharing-customers-location-data/

[4] Colin Lecher, How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity', The Verge, April 25, 2019. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

[5] Josh Dzieza, How Hard Will the Robots Make Us Work?, The Verge, February 27, 2020. https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon

meet a daily minimum threshold for mouse clicks.[6] Excessive electronic monitoring is also likely to blame for higher rates of worker injuries and turnover. In 2021, the Washington State Department of Labor and Industries noted a direct connection between excessive worker surveillance, discipline systems, and serious workplace injuries at an e-commerce warehouse[7]—a finding that was later supported with nationwide data.[8] Another 2021 report, which aligns with broader workplace surveillance research,[9] found turnover among remote workers was higher at employers that required productivity surveillance software.[10]

- **MIPSA should be amended to strengthen its enforcement provisions by adding a private right of action and expanding the Attorney General's authority.**

    - The rights established under the new Chapter 93M created by MIPSA are no less important than the rights of Chapter 93A, under which a private right of action is available. A private right of action is essential to give ordinary people the power to hold accountable companies that violate their rights.[11]
    - The bill should strengthen the civil action granted to the AGO in these ways:
        i. limit companies' ability to avoid accountability by "curing" their violations of the law after the fact;
        ii. broaden their investigatory powers so that companies cannot refuse to cooperate;
        iii. mandate that the AGO prioritize formal adjudication over informal agreements;
        iv. establish cooperation mechanisms with privacy enforcers in other states; and
        v. increase civil penalties and provide maximum and minimum fines in terms of the percentage of a company's annual global revenue.
    - The bill grants the AGO significant authority in section 25. We welcome the possibility of the AGO monitoring and researching issues like eye-tracking technology, targeted advertisement, and the data broker industry. That said, the bill should strengthen this authority of the Attorney General, granting specific rulemaking and regulatory authority on these issues.
    - The bill should incorporate public transparency provisions. For example, section 21 mandates companies to produce risk assessments but does not require that these become public. Another example is the information that has to be made public by the Attorney General pursuant to section 25(n). The report about companies being investigated because of alleged privacy violations should not withhold the name of

---

[6] Danielle Abril and Drew Harwell, Keystroke Tracking, Screenshots, and Facial recognition: The Boss May Be Watching Long After the Pandemic Ends, The Washington Post, September 24, 2021. https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/

[7] Citation/Inspection # 317961850, Washington State Department of Labor and Industries, May 4, 2021. https://s3.documentcloud.org/documents/20787752/amazon-dupont-citation-and-notice-may-2021.pdf

[8] Jay Greene and Chris Alcantara, Amazon Warehouse Workers Suffer Serious Injuries at Higher Rates Than Other Firms, The Washington Post, June 1, 2021. https://www.washingtonpost.com/technology/2021/06/01/amazon-osha-injury-rate/

[9] Kristie Ball, Electronic Monitoring and Surveillance in the Workplace, Publications Office of the European Union, 2021. https://publications.jrc.ec.europa.eu/repository/handle/JRC125716

[10] Employee Surveillance Measures Could Threaten Trust and Increase Staff Turnover, VMware Research Finds, VM Ware, November 10, 2021. https://news.vmware.com/releases/virtual-floorplan

[11] See Becky Chao et. al., A Private Right of Action is Key to Ensuring that Consumers Have Their Own Avenue for Redress, Enforcing a New Privacy Law, New America, November 2019. https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress/ and Adam Schwartz, You Should Have the Right to Sue Companies That Violate Your Privacy, EFF, January 2019. https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy

the companies under investigation. The public has the right to know how companies comply, or do not comply, with the law.

Thank you for your consideration. We would welcome the opportunity to discuss this matter further and collaborate with you to most effectively protect the personal digital data of Massachusetts residents.

Sincerely,

ACLU of Massachusetts
Access Now
Center on Privacy & Technology at Georgetown Law
Consumer Federation of America
Digital Fourth
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
MASSPIRG
SEIU Local 509
United for Respect