November 10, 2021

Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
Sen. Barry R. Finegold & Rep. Linda Dean Campbell, Co-Chairs

Re: Correcting the Record on H.142 and S.46, the Massachusetts Information Privacy Act

Dear Senator Finegold, Representative Campbell, and members of the committee,

Thank you for a productive hearing on October 13, 2021, regarding Data Use & Privacy. We write today to provide further input in support of H.142 and S.46, *the Massachusetts Information Privacy Act (MIPA)*, sponsored by Representatives Vargas and Rogers and Senator Creem, in response to testimony from tech industry lobbyists.

During the hearing, the committee heard powerful testimony from civil, consumer, privacy, and worker rights organizations and academic experts in support of this legislation. The entirety of the opposition came from industry lobbyists. The arguments put forward by these industry representatives were misleading, and in some cases flatly wrong. We provide the following additional information in direct response to some of the more troubling claims presented to the committee about this important legislation.

Cost of Compliance

We share the concern raised by industry lobbyists that it would be unfair to impose unreasonable, outsized fines on big and small businesses. MIPA takes care to address this issue.

First, **the bill does not apply to small businesses.** MIPA treats small firms differently from large corporations that process huge quantities of personal information. **Companies covered by the legislation are limited to large-scale, for-profit corporations** that process personal information by themselves or by contracting with a data processor, and (i) have earned 10 million or more dollars of annual revenue through 300 or more transactions, or (ii) process or maintain the personal information of 10,000 or more unique individuals during the course of a calendar year.

MIPA would not impact small businesses in Massachusetts. According to the Massachusetts Association of Community Development Corporations, about 86 percent of businesses in Massachusetts employ fewer than 20 people, and 75 percent employ fewer than 10.[1] According to Intuit, firms employing fewer than 20 people have average annual revenue of significantly less than $10 million per year, meaning the legislation would not

[1] Fact Sheet, Small Businesses in Massachusetts, Massachusetts Association of Community Development Corporations. https://www.macdc.org/sites/default/files/documents/Small_Business_in_Massachusetts.pdf

apply to them.[2] Thus, **MIPA would apply only to the less than 15% of businesses in the Commonwealth that earn tens of millions of dollars in revenue or process the personal data of tens of thousands of residents.**

The current lack of privacy regulations actually benefit big corporations to the detriment of small businesses that cannot compete because the Goliaths leverage data to manipulate the market and lock in customers. An example of this is how Amazon uses the data collected through its marketplace to unfairly compete with other merchants.[3]

Second, **the bill contains several exceptions to make it less burdensome on companies**:

- While MIPA generally requires a company to obtain an individual's consent to collect and process their personal information, it's not necessary to obtain express consent when the primary purpose is to fulfill a specific transaction. So, for example, if a shop sells its products online, it does not need to take special actions under MIPA when collecting your shipping address or credit card number;
- MIPA does not apply to personal contact information shared in the workplace or other social, political, or similar settings where the purpose of the information is to facilitate communication among individuals; and
- MIPA does not apply to information covered under the federal Health Insurance Portability and Accountability Act of 1996.

Third, **fines for non-compliance are scaled according to the size of the violating corporation.** The dollar amount of any civil administrative penalties and court awards in MIPA are set as a percentage of the annual global revenue of an offending company. Therefore, companies will pay fines relative to their size and wealth.

"Privacy Pledges"

Industry lobbyists argue that the public and the legislature shouldn't worry too much about privacy because companies have taken their own "privacy pledges." However, self-regulation is insufficient to address what everyone agrees are real privacy problems. Self-regulation got us to where we are now; it has utterly failed because companies and their trade associations have at best a troubling view of what constitutes privacy-preserving policy and procedure.[4]

The reality is that **if companies are required to be transparent and clear in their terms of service and privacy policies, people will not be confused about their rights**. MIPA has several provisions that push companies to be clear and transparent. One of them is the creation of short and long-form privacy policies. Another is the prohibition of common mechanisms known as dark patterns[5] that mislead individuals by confusing user interfaces and other techniques that coerce consent. If companies don't want people to be confused, they should start by not actively trying to confuse people on purpose.

Opt-In Consent

Corporations that profit off of our personal information always follow the same script: consent for data collection must be opt-out and not opt-in, even for biometric information. Their main argument is that asking for individual consent causes fatigue and confusion. But MIPA addresses these issues head on.

First, **MIPA includes provisions designed to prevent privacy fatigue.**[6] The solution to the problem of privacy fatigue is not to avoid asking for consent altogether. Rather, privacy legislation should encourage

---

[2] Sandi Leyva, How Does Your Revenue Stack Up to Other Small Businesses?, Intuit, March 2015. https://quickbooks.intuit.com/r/money/how-does-your-revenue-stack-up-to-other-small-businesses/

[3] Javier Espinoza, EU Accuses Amazon of Breaching Antitrust Rules, The Financial Times, November 2020. https://www.ft.com/content/4908995d-5ba4-4e14-a863-bcb8858e8bd2

[4] Arisha Hatch, Big Tech companies cannot be trusted to self-regulate: We need Congress to act, TechCrunch, March 2021. https://techcrunch.com/2021/03/12/big-tech-companies-cannot-be-trusted-to-self-regulate-we-need-congress-to-act/

[5] Jasmine McNealy, What Are Dark Patterns? An Online Media Expert Explains, The Conversation, August 2021. https://theconversation.com/what-are-dark-patterns-an-online-media-expert-explains-165362

[6] Hanbyul Choi et al., The Role Of Privacy Fatigue In Online Privacy Behavior, Computers in Human Behavior, Volume 81, 2018. https://www.sciencedirect.com/science/article/abs/pii/S0747563217306817

people to take consent seriously without being bombarded with notices and pop-ups. For example, under MIPA, if an individual refuses to provide consent, the covered entity shall not try to obtain consent again unless a period of at least six months has passed. This would prevent companies from constantly asking consent from individuals that have already refused it.

In fact, one of the reasons why MIPA moves away from the traditional notice-and-consent framework and imposes fiduciary duties on companies is that the traditional model has proven to be ineffective for these very same reasons. Therefore, it is necessary to start taking the pressure off consent as the sole mechanism of enacting privacy rights in the modern era.

Second, **consent must be freely given, specific, informed, unambiguous, and opt-in**. People must actively consent to any collection and processing of their personal information just as they do in other areas of their private life, namely health or sexual practices. Presuming consent by default, which underpins an opt-out model, is problematic and does not live up to today's privacy challenges or expectations in other important areas of our lives.[7]

Third, **biometric information is too precious to be left to the dictates of the market**. The requirement for handwritten consent to collect these data is specifically designed so that people take providing such consent seriously. The purpose of the collection is irrelevant, and should not have any relationship to the consent mechanism. After all, if someone's biometric data is hacked, misused, or stolen, the reason for the initial collection is immaterial. Thus, if companies want to use biometric data for security purposes, as we heard during the hearing, they should still be required to get this special consent.

Sale of Personal Information

Some industry lobbyists asked legislators to reject MIPA because they want to continue the business-to-business sale of information. **But MIPA does not outlaw the sale of most personal information (only biometric and location information)**. Instead, MIPA establishes that individuals have the right to know the names of third parties to which the covered entities or data processors will disclose their personal information and to refuse consent for such disclosure.

For too long, we have accepted a free-for-all situation that permits companies to do whatever they want with data. MIPA's purpose is to set rules that put people and privacy rights in the center.

State Legislation vs. Federal Legislation

We cannot wait for federal legislation to address these problems. And the suggestion that MIPA would trigger "interstate commerce issues" is simply a red herring. These arguments are wrong and dangerous.

First, **any potential future federal law should be the floor and not the ceiling of privacy legislation**. Generally, complying with the most privacy-protective laws, in this case MIPA, would imply complying with less privacy-protective frameworks, whether from other states or the federal level.

Second, **the U.S. is a vast country with many significant variations in state-level consumer protection laws**, and companies can and do comply with them. Frequently, companies do so by providing consumer benefits required in one state to consumers in all states. You have most likely read cancer-warning labels on cosmetics, furniture, and other consumer goods. Those warnings are printed on products sold in Massachusetts because California has a law mandating them, so companies adjusted their operations accordingly. In this way, Massachusetts residents benefit from environmental and health benefits that exist thanks to California state law. The same will be true if Massachusetts enacts MIPA.

Third, **the federal government is unlikely to act to protect data privacy and is even less likely to pass robust privacy law.** Pro-privacy legislation has languished for decades in Congress because tech companies have been spending unprecedented amounts of money lobbying against it.[8] As we saw at the hearing, the tech

[7] Editorial Board, America, Your Privacy Settings Are All Wrong, The New York Times, March 2021. https://www.nytimes.com/2021/03/06/opinion/data-tech-privacy-opt-in.html

[8] Jane Chung, Big Tech, Big Cash: Washington's New Power Players, Public Citizen, March 2021. https://mkus3lurbh3lbztg254fzode-wpengine.netdna-ssl.com/wp-content/uploads/Big-Tech-Big-Cash-Washingtons-New-Power-Players.pdf

industry's vision of appropriate regulation couldn't be more different from the vision articulated by consumer and civil rights advocates. As in many other areas, state innovation may eventually spur federal action, but Massachusetts residents are unlikely to benefit from Congress passing a meaningful data privacy law any time soon.

Private Right of Action

Corporate interests always oppose legislation that would allow people to redress violations of their rights by means of a private right of action. At the hearing, industry lobbyists complained about the Illinois Biometric Information Protection Act ("BIPA") for this reason. They complained that "hundreds of lawsuits" have been filed in that state since that law was passed nearly ten years ago, implying that this is a bad thing.

To put it simply: **Companies don't like a private right of action because, unlike regulatory agencies (and legislatures), individuals harmed by illegal corporate data abuses cannot be lobbied into submission**. Individuals cannot fall victim to regulatory capture.

There is no reason to hinder individuals from having their day in court when companies violate their rights and use their personal information in unlawful ways. Experts[9] and privacy[10] advocates here and elsewhere are in clear agreement on this point. But, more importantly, real-world practice shows that private rights of action work. The "hundreds of lawsuits" filed under BIPA include groundbreaking cases to protect biometric information from companies that willfully and boldly violate the law.[11] These cases are effectively forcing companies to change their policies and redress harms.[12]

Conclusion

MIPA approaches information privacy issues holistically, addressing the entirety of the information privacy ecosystem and learning from previous experiences of privacy regulation. Private companies will try to direct the discussion towards issues already addressed while avoiding taking responsibility for all the problems that self-regulation has caused.

We once again respectfully urge this Committee to advance H.142 and S.46 with a favorable report, and we would welcome the opportunity to work with you on this legislation. Thank you.

Access Now

ACLU of Massachusetts

Consumer Federation of America

Digital Fourth

Electronic Frontier Foundation

Electronic Privacy Information Center

Encode Justice

Fight for the Future

Massachusetts Jobs with Justice

Surveillance Technology Oversight Project (S.T.O.P.)

National Employment Law Project

United for Respect

Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University (affiliation is for identification purposes only)

[9] 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/

[10] 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

[11] Illinois Court Rejects Clearview's Attempt To Halt Lawsuit Against Privacy-Destroying Surveillance, ACLU, August 2021. https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying

[12] Judge Approves $650M Facebook Privacy Lawsuit Settlement, AP News, February 2021. https://apnews.com/article/technology-business-san-francisco-chicago-lawsuits-af6b42212e43be1b63b5c290eb5bfd85