ACLU of Massachusetts
One Center Plaza, Suite 850
Boston, MA 02110
617-482-3170
www.aclum.org

October 19, 2023

Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
Senator Michael O. Moore and Representative Tricia Farley-Bouvier, Co-Chairs

Testimony in Support of H.83 and S.25

An Act to Establish the Massachusetts Data Privacy Protection Act

Dear Senator Moore, Representative Farley-Bouvier, and members of the committee,

The ACLU of Massachusetts strongly supports H.83 and S.25, *An Act to Establish the Massachusetts Data Privacy Protection Act,* sponsored by Representatives Vargas and Rogers and Senator Creem. This legislation is critically needed to protect Massachusetts consumers in the digital age.

Commercial entities have long sought information about their customers because of its value to business operations. But the digital age is different. The widespread use of the Internet and smartphones, cheap data storage, the explosion in computing power and "smart" devices of every stripe, and increasingly complex algorithms and machine learning processes have resulted in substantial and ever-growing privacy harms.[1]

An old saying says that when something is free on the Internet, consumers are the product. However, as Shoshana Zuboff observes in her book *The Age of Surveillance Capitalism,* we are not only the product—we are also the raw material. [2] Companies collect and process all sorts of personal data: the mundane, the intimate, and everything in between. These include our online searches, health conditions, business and personal associations, daily habits, physical locations, and much, much more. Yet lack of regulation leads to countless harms for individuals and our democracy. These harms are well understood by those in the industry, but absent meaningful law reform to protect the public interest, they persist.[3]

Consumer facing surveillance poses extremely serious threats to individual privacy and our collective ability to govern ourselves in a free and democratic society. The rise of artificial intelligence and machine learning raises the stakes considerably: much of this information is also now used, secretively and without proper regulation, to train models that too often reproduce existing harms of discrimination against groups of people.[4] Companies can use these tools to offer different pricing to different groups and determine the quality of goods and services different people receive. These decisions limit our choices in ways that are not immediately apparent to ordinary technology users, and often have racial justice and civil rights implications. For example, in an infamous case unearthed

---

[1] Solove, Daniel J. &Keats Citron, Danielle, Privacy Harms, GW Law Faculty Publications & Other Works, 1534 (2021). https://scholarship.law.gwu.edu/faculty_publications/1534

[2] See Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York, 2019, p.8.

[3] An investigation of the Wall Street Journal found that employees and executives at Facebook (now Meta) are aware that its platforms are riddled with flaws that cause harm (e.g., Instagram is harmful and toxic for teenage girls) in ways only the company fully understands. See Jeff Horwitz et. al., The Facebook Files, Wall Street Journal, September 2021. https://www.wsj.com/articles/the-facebook-files-11631713039

[4] Sam Biddle, The Internet's New Favorite AI Proposes Torturing Iranians and Surveilling Mosques, The Intercept, December 8, 2022. https://theintercept.com/2022/12/08/openai-chatgpt-ai-bias-ethics/

by Harvard professor Latayna Sweeney, Google directed search engine users with Black-sounding names to bail bonds websites while offering mortgage ads to others.[5]

Unfortunately, Massachusetts privacy law does not reflect the vast technological changes our world has seen in recent decades. Today, ordinary people are being harmed in countless ways, some obvious, some hidden. The few existing laws and regulations dealing with information privacy rights are extremely limited and inadequate to meet the present need.[6]

We need a comprehensive information privacy framework that establishes protections against the unwitting and unwelcome collection, use, processing, manipulation, and monetization of personal information. We also need special protections for the most sensitive types of personal information, including location and biometric data. The law must also include safeguards to protect vulnerable people and communities against digital redlining and discrimination.

Those motivated by their stock price and bottom line insist that Massachusetts pass a law with limited protections and weak enforcement, like those won by industry lobbyists in Virginia and Connecticut. But that would fail to meet the challenge of protecting ordinary technology users; it would put private profits over the public interest. Here in Massachusetts, the Massachusetts Data Privacy Protection Act offers us an opportunity to lead by putting our people and our communities first.

Modeled on Federal Legislation with Insights from Global Privacy Leaders

MDPPA is modeled after successful privacy frameworks, emerging reforms, and best practices. It aims to bring our statutes up to speed with existing and future technologies, level the playing field between individuals and corporations, and protect both individual rights and our larger society.

The bill holistically approaches information privacy, addressing each segment of information flow and borrowing from what has —and has not—worked in other states and countries. The MDPPA's primary inspiration is the American Data Privacy Protection Act ("ADPPA"), a federal bill that passed out of the Energy and Commerce Committee 53-2 in 2022 with broad support from the technology industry and civil rights organizations.[7]

Other frameworks MDPPA takes inspiration from include the California Consumer Privacy Act ("CCPA"),[8] the Illinois Biometric Information Protection Act ("BIPA"),[9] and the European General Data Protection Regulation.[10]

The legislation has two substantive sections. Section 1 creates a new chapter in the General Laws, Chapter 93L, to establish comprehensive information privacy regulations for the Commonwealth and their enforcement. Section 2 introduces new protections for privacy in the workplace.

---

[5] Google Searches Expose Racial Bias, Says Study Of Names, BBC News, February 2013. https://www.bbc.com/news/technology-21322183

[6] All we have are general consumer rights under the state consumer protection law (Chapter 93A), provisions on data security breaches (Chapter 93H), and a vague one-line statement of principle describing a general right to privacy (Chapter 214, Section 1B).

[7] Joseph Duball, American Data Privacy and Protection Act heads for US House floor, IAPP, July 21, 2022. https://iapp.org/news/a/american-data-privacy-and-protection-act-heads-for-us-house-floor/

[8] California Consumer Privacy Act (CCPA), Office of the Attorney General, California. California Consumer Privacy Act (CCPA). https://www.oag.ca.gov/privacy/ccpa

[9] Illinois Compiled Statutes, Biometric Information Privacy Act, 740 ILCS 14. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[10] General Data Protection Regulation. https://gdpr-info.eu/

This testimony provides a broad overview of the provisions of the bill and highlights elements that are key to a robust and protective privacy framework. Attached to this testimony is a section-by-section summary.

Data Minimization: The Gold Standard for Protecting Personal Information

Like the federal legislation that inspired it, MDPPA rejects the failed consent framework for governing data collection and use. Instead, the bill sets a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to either (1) provide or maintain a product or service requested by the individual or (2) effect a purpose expressly permitted by the legislation.

Today, consumers' use of online products and companies' collection and use of individuals' personal information is governed by industry-developed terms of service agreements and privacy policies. This is known as a notice and consent framework. In California, for example, this *de facto* arrangement has been written into law as the basis for the CCPA.[11]

However, the notice-and-consent framework fails to protect privacy.[12] There are four basic reasons for this failure.

First, individual technology users are not capable of reading or understanding all the various Terms of Service and privacy policies that govern their use of technology services. These documents are often lengthy, filled with legal jargon, and take significant time to read. Even if one were to invest the time and energy to attempt to read all these documents, they are not always transparent or clear about all the types of personal information companies collect or how companies will use, manipulate, or share that information.

Second, individuals cannot provide meaningful consent.[13] Even if privacy policies were understandable and comprehensive, the practical reality of how people use technology services makes it impossible for individuals to give meaningful consent. That is in large part because individuals cannot influence or understand the terms set by third parties who collect data. The sheer number of companies and entities collecting, using, and sharing personal data is overwhelming, and many times people do not directly engage with these entities. As a result, individuals cannot accurately assess the risks and benefits of allowing companies to collect their personal data.

Third, technology users lack bargaining power. Under the notice and consent model, consumers have little to no choice: too often, they face the choice to either consent to a company's terms or decline and lose access to the service entirely. This is a false choice that renders ordinary people powerless to protect their personal information.

Fourth, there is little to no accountability for what happens to people's information after they click "Agree" to access a service. Even if consumers understand the privacy policies and even if they provide meaningful consent, consumers do not have any way to assess whether the companies comply with those policies, let alone a recourse if companies violate those terms.

MDPPA avoids these pitfalls of the consent model by imposing data minimization rules to **limit data collection to what is reasonably necessary and proportionate** to carry out a specified

---

[11] S. 227, *An Act establishing the Massachusetts Information Privacy and Security Act* sponsored by Representative Finegold follows this framework.

[12] Amber Sinha & Scott Mason, A Critique of Consent in Information Privacy, The Centre for Internet & Society, January 2016. https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy

[13] N. Richards, W. Hartzog, The Pathologies of Digital Consent, 96 Washington University Law Review 1461 (2019)

purpose. These minimization rules supersede any individual "Terms of Service" document by limiting what data a company can and cannot collect and under what circumstances.

Entities cannot misuse, abuse, wrongfully manipulate, or accidentally leak data they do not collect in the first place. Data minimization is, therefore, a crucial element of any meaningful and impactful data privacy law. Again, the bill sets a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to either (1) provide or maintain a product or service requested by the individual or (2) effect a purpose expressly permitted elsewhere by the MDPPA. The bill provides an extensive list of permissible purposes, including completing a transaction requested by an individual, authenticating users, fulfilling a product or service warranty, and complying with a legal obligation. The legislation therefore ensures companies are able to offer impactful services consumers desire without sacrificing user privacy. But crucially, the legislation shifts the privacy burden away from the individual and onto the corporation collecting and processing personal information.

In addition to these data minimization rules, MDPPA includes some specific provisions that allow users to consent to particular types of processing and disclosure of their data. MDPPA regulates consent practices and how companies can request consent for these cases. Notably, the legislation prohibits manipulative design tricks, commonly known as "deceptive" or "dark" patterns, that some entities use to obtain consent.[14]

Providing Special Protections for Sensitive Data

Not all data is equal. Some kinds of information, such as location and biometric data, pose especially severe threats to personal privacy, autonomy, and even safety. The bill therefore gives specific subsets of personal data heightened legal protections because of the severe harms arising from its misuse and abuse. "Sensitive covered data" under the MDPPA includes government-issued identifiers, information related to an individual's physical or mental health, finance services-related identifiers, biometric information, genetic information, and location information, among others.[15]

By its very nature, sensitive data is especially revealing. Private companies should not be allowed to sell,[16] monetize, or exploit[17] it. To address this, MDPPA includes the following provisions:

First, the bill establishes especially protective data minimization rules for sensitive data collection, use, and transfer. Under the bill, companies cannot collect or process sensitive covered data except where such collection or processing is **strictly necessary** to provide or maintain a specific product or service requested by the individual to whom the data pertains.[18]

---

[14] Brignull, Harry, et al., Deceptive Patterns – User Interfaces Designed to Trick You, 25 Apr. 2023, https://www.deceptive.design.

[15] Sensitive covered data includes location data, for which we have advocated for a standalone bill called the *Location Shield Act* that bans the sale, rent, trade, and lease of such data. We think this category of data should have its standalone regulation, apart from any general consumer privacy regulation that exists or may exist, because of its serious implications for people seeking healthcare here in the Commonwealth.

[16] Sara Morrison, Verizon, T-Mobile, Sprint, and AT&T could be facing big fines for selling your location data, Vox, February 2020. https://www.vox.com/recode/2020/2/27/21156609/verizon-t-mobile-sprint-att-fined-location-data

[17] Bennet Cyphers, Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It, EFF, March 2020. https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

[18] MDPPA also provides that companies cannot collect, process, or transfer a Social Security number, except when necessary to facilitate an extension of credit, authentication, fraud, and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by state or federal law.

Second, the bill prohibits the use of sensitive data for targeted advertising.

Third, the legislation limits to a narrow and defined set of circumstances the transfer of sensitive data to a third party. These include obtaining affirmative express consent for data transfers and complying with a legal obligation imposed by state or federal law.

Acknowledging the Different Actors in the Industry

Massachusetts must be careful not to enact laws that harm small companies by entangling them in complicated compliance requirements. The MDPPA recognizes this and proposes comprehensive regulation only for the largest companies that routinely collect, store, and manage personal data; it is not a shotgun approach.

First, **the bill does not apply to most Massachusetts businesses**, but rather only applies to those that consistently earn more than $20M a year and collect the data of more than 75,000 people.[19]

Second, for mega-sized companies where data collection and processing play an outsized role, the bill appropriately establishes stricter requirements for "large data holders" ("LDH")[20] and "covered high-impact social media companies."[21]

Protecting Civil Rights in the Digital Age

The MDPPA aims to protect not only privacy, but civil rights. Today, massive amounts of personal information collected by private companies are being used to feed algorithmic decision systems shielded from public view. The rise of big data and the ubiquitous use of systems powered by machine learning have had pernicious consequences for everyone. But as with many other problems, algorithmic harms are not borne out equally.

While they are often marketed as mathematical fixes to address human biases, algorithmic decision systems often produce unfair consequences and calcify historical discrimination and harm. For

---

[19] The bill does not apply to companies that meet the following criteria for the three prior years: annual revenues less than $20 million; on average, the entity did not annually collect or process the covered data of more than 75,000 individuals; and no portion of the entity's revenue came from transferring covered data during any year. According to MassBudget, most small businesses in Massachusetts are worth less than $1 million. https://massbudget.org/2022/10/24/fsa-small-business-sales/

[20] Defined as companies that in the most recent calendar year, meet the following criteria

- had annual gross revenues of $250,000,000 or more; and
- collected, processed, or transferred the covered data of more than 5,000,000 individuals (excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service), and
- the sensitive covered data of more than 200,000 individuals.

These companies are mandated to conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data collecting, processing, and transfer practices against the potential adverse consequences of such practices, including substantial privacy risks to individual privacy.

[21] Defined as a company that provides any internet-accessible platform where:

- such covered entity generates $3,000,000,000 or more in annual revenue;
- such platform has 300,000,000 or more monthly active users for not fewer than 3 of the preceding 12 months on the online product or service of such covered entity; and
- such platform constitutes an online product or service that is primarily used by users to access or share, user-generated content.

These companies are held to a higher standard when it comes to assessing whether they had "knowledge" of, for example, minors using their services.

example, last year, a group of consumers sued the insurance company State Farm, alleging the company's use of automated decision systems discriminates against Black customers.[22] In another instance of similar harm, a Black homeowner sued Wells Fargo alleging that the lending algorithms used by the bank unfairly discriminated against him when refinancing his loan.[23]

In other instances, platforms are built in a way that enables illegal discrimination. Facebook, for example, was targeted by repeated legal actions after the company facilitated illegal discrimination in employment, housing, and credit advertising.[24]

These are just a few of the ways technology companies are using their access to copious amounts of data to train algorithms that often lead to unfair consequences for people of color, those with low incomes, women, and other marginalized groups.

A comprehensive approach to advancing digital rights and democracy must therefore address digital redlining[25] and algorithmic discrimination. Towards that end, the MDPPA includes language meant to protect civil rights and establishes that covered entities may not collect, process, or transfer covered data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services based on race, color, religion, national origin, sex, sexual orientation, gender, or disability.[26]

Other Privacy Provisions

The bill also incorporates basic provisions found in most modern-day privacy laws. The most significant of these are:

- Privacy by design principles: Companies must implement reasonable policies, practices, and procedures for collecting, processing, and transferring data.
- Data rights: Individuals have the right to access, correct, delete, and take with them to different services their covered data.
- Prohibition of retaliation. Covered entities may not retaliate against an individual for exercising their rights or refusing to agree to collect or process their data for separate products or services.
- Advanced data rights: Individuals may opt out of (1) transferring data to a third party and (2) targeted advertising for those covered data that are not sensitive.
- Data brokers. Data brokers must annually register in a public registry with the Office of Consumer Affairs and Business Regulation ("OCABR") and place a clear and

[22] Emily Flitter, New Suit Uses Data to Back Racial Bias Claims Against State Farm, The New York Times, December 14, 2022.
[23] Tamaryn Waters, Wells Fargo Bank Sued for Race Discrimination in Mortgage Lending Practices, USA Today, April 2022, https://www.usatoday.com/story/money/2022/04/26/wells-fargo-being-sued-discriminating-against-black-borrowers/7451521001/
[24] Galen Sherwin & Esha Bhandari, Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform, ACLU, March 2019. https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping. Further reporting showed that, even after settling one of these discrimination cases, the platform was still facilitating discriminatory ad targeting. See Ava Kofman & Ariana Tobin, Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement, ProPublica, December 2019. https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement
[25] Will Oremus, A Detroit Community College Professor Is Fighting Silicon Valley's Surveillance Machine. People Are Listening, The Washington Post, September 2021. https://www.washingtonpost.com/technology/2021/09/16/chris-gilliard-sees-digital-redlining-in-surveillance-tech/
[26] This does not prevent covered entities from diversifying an applicant, participant, or customer pool.

conspicuous notice on their website or mobile application informing individuals they are data brokers.

Enforcing the Law and Holding Companies Accountable

Laws are only as good as the paper they are written on without robust enforcement mechanisms. Accordingly, **the MDPPA provides two means of enforcement: a private right of action and enforcement by the attorney general.**

Enforcement of privacy regulations should not be left only to government agencies with limited budgets and staff resources. To ensure compliance with the law and redress for violations, individuals must be allowed to have their day in court when companies violate their rights and use their personal information in unlawful ways.

The industry opposes a privacy right of action for one simple reason: because it works. Private rights of action are the silver bullet of privacy laws because they are effective deterrents. Experts and privacy advocates here and elsewhere agree.[27] Providing individuals with a tool to enforce their legal rights encourages companies to obey the law.[28]

A 2011 research study about the comparative deterrence of private enforcement *vis-à-vis* criminal enforcement by the Department of Justice ("DOJ") of antitrust laws found that "there is evidence that private antitrust enforcement does more than DOJ criminal enforcement to deter anticompetitive behavior." Moreover, the research concluded that "the high success rate of government litigation suggests that in the absence of private litigation, many bad actors would get away with violating the antitrust laws."[29]

Today, Massachusetts residents cannot seek redress for or halt many of the most severe data privacy harms. The MDPPA proposes a 180-degree turn and grants individuals[30] the right to bring a civil action in court against a covered entity that does not comply with the law.[31]

Conclusion

Today, Massachusetts residents suffer extreme privacy violations daily and have no opportunity to defend themselves except by refusing to use modern technology—a sad state of affairs for a state that prides itself on being a worldwide technological leader. The MDPPA approaches these issues holistically, addressing the entirety of the information privacy ecosystem. If enacted, this landmark

---

[27] 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/. See also 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

[28] See Fitzpatrick, Brian T., Do Class Actions Deter Wrongdoing?, The Class Action Effect (Catherine Piché, ed., Éditions Yvon Blais, Montreal, 2018), Vanderbilt Law Research Paper No. 17-40, September 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020282

[29] Robert H. Lande and Joshua P. Davis, Comparative Deterrence from Private Enforcement and Criminal Enforcement of the U.S. Antitrust Laws, 2011 BYU L. Rev. 315, 2011, pp. 348-349. https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=1739&context=all_fac

[30] The bill also incorporates by reference the enforcement action on behalf of the Attorney General pursuant to Section 4, Chapter 93A.

[31] If the plaintiff prevails, the court may award liquidated damages of not less than 0.15% of the annual global revenue of the covered entity or $15,000 per violation, whichever is greater, as well as punitive damages, equitable relief, and reasonable attorney's fees and costs.

bill will protect Massachusetts residents' interests against commercial and personal exploitation and establish the Commonwealth as a leader in information privacy.

We respectfully urge this committee to advance H.83 and S.25 with a favorable report, and we welcome the opportunity to partner with you to make Massachusetts a global privacy and digital civil rights leader. Thank you.

Kade Crockford
Director
Technology for Liberty Program
ACLU of Massachusetts

Emiliano Falcon-Morano
Policy Counsel
Technology for Liberty Program
ACLU of Massachusetts

Massachusetts Data Privacy Protection Act

SECTION 1. The General Laws are amended by inserting after chapter 93K the chapter 93L, named Massachusetts Data Privacy Protection Act

Section 1. Definitions

Section 2. Duty of Loyalty

Provides the lawful basis for collecting and processing covered data

Protects freedom of speech rights

Section 3. Sensitive covered data.

Regulates the collection and processing of sensitive covered data. A covered entity or service provider shall not, among other things, transfer an individual's sensitive covered data to a third party, unless: -

- the transfer is made pursuant to the affirmative express consent of the individual, given before each specific transfer takes place;
- the transfer is necessary to comply with a legal obligation imposed by state or federal law, so long as such obligation preexisted the collection and previous notice of such obligation was provided to the individual to whom the data pertains;
- the transfer is necessary to prevent an individual from imminent injury where the covered entity believes in good faith that the individual is at risk of death, serious physical injury, or serious health risk;

Moreover, covered entities cannot process sensitive covered data for purposes of targeted advertising.

Section 4. Consent practices

Regulates how consent can be solicited and given.

Section 5. Privacy by design

Establishes that a covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data

Section 6. Pricing

Establishes protections by prohibiting companies from retaliating against consumers when they exercise their rights. Prevents pay-for-privacy schemes.

Section 7. Privacy policy

Describes the elements of the privacy policy.

Section 8. Individual data rights

Provides for individual data rights of access, correction, and deletion.

Section 9. Advanced data rights.

Provides for two opt-out rights:

- Right to opt-out of covered data transfers.
- Right to opt-out of targeted advertising.

Section 10. Minors

Establishes that a covered entity may not engage in targeted advertising to any individual if the covered entity has knowledge that the individual is a covered minor.

Section 11. Data Brokers

Regulates data brokers:

- Creates a registry within the Office of Consumer Affairs and Business Regulation.
- Imposes obligations with regard to their relationship with consumers
- Imposes penalties

Section 11. Civil rights protections

Establishes that a covered entity or a service provider may not collect, process, or transfer covered data or publicly available data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services (i.e., has a disparate impact) on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity or disability.

Requires large data holders to conduct impact assessments of algorithms in use and development. Results shall be submitted to the AG and a summary of the findings must be public.

Section 12. Miscellaneous

Establishes that:

- the OCABR shall develop a centralized way to provide an opt-out mechanism;
- covered entities or service providers that are not a small business shall designate data privacy and security officers; and
- large data holders are mandated to conduct annual privacy impact assessments.

Section 13. Service providers.

Regulates service providers and their relationships with covered entities.

Section 14. Enforcement. Private Right of Action and Attorney General enforcement.

Two mechanisms of enforcement:

- Private right of action against covered entities that are not small businesses.
- AG enforcement.

Section 15. Enforcement - Miscellaneous

Establishes that the rights are non-waivable.

Section 16. Transparency

Establishes transparency provisions regarding government requests for disclosure of personal information received by covered entities.

Section 17. Non-applicability

Excludes from the bill:

- Health information protected by HIPAA;
- individuals sharing their personal contact information, such as email addresses, with other individuals in the workplace, or other social, political, or similar settings where the purpose of the information is to facilitate communication among such individuals; and
- covered entities' publication of entity-based member or employee contact information.

Section 18. Relationship with other laws

Establishes that nothing in this chapter shall diminish any individual's rights or obligations under the Massachusetts Fair Information Practices chapter and its regulations.

Section 19. Implementation

Grants the Attorney General with rulemaking and enforcement authority.

Section 20. Severability

SECTION 2. Establishes protections for workers against electronic monitoring by adding section 204 to the labor code.

SECTION 3. Effective date.

- The provisions of the Act shall take effect 12 months after this Act is enacted
- The enforcement of chapter 93L shall be delayed until 6 months after the effective date.