



AFT Massachusetts



National Council of Jewish Women Massachusetts



RE: LETTER IN SUPPORT OF S. 2516 (THE MASSACHUSETTS DATA PRIVACY ACT)

June 12, 2025.

Dear President Spilka, Speaker Mariano, and the Chairs, Vice-Chairs and Members of the Senate and House Ways and Means Committees:

As organizations who value the rights and safety of all Massachusetts residents, we appreciate the fact that the Senate Committee on Steering and Policy dedicated its May 28 hearing to ensuring that access to reproductive and gender-affirming care in Massachusetts remains private and protected from prosecution by other states. Information related to our medical care is not just available through our medical records. It is gleaned from our web searches, the clinics that we frequent which are geolocated by our phones, and our social media communications. We believe that the best protections for vulnerable groups are those that will strongly protect all Massachusetts residents. In this vein we are greatly encouraged by the Senate members of the Advanced IT, the Internet, and Cybersecurity Committee's commitment to residents' privacy rights, by speedily voting out [S.2516](#), the Massachusetts Data Privacy Act ("MDPA"), and [S.197](#), the Location Shield Act ("LSA"), whose provisions are incorporated in the MDPA.

We urge you in your planning regarding privacy legislation to not focus exclusively on a particularly vulnerable population, nor on a single exploitable type of data, but instead to take the opportunity to follow Maryland's lead and pass a privacy bill that protects those most vulnerable by protecting everyone. The MDPA is that bill. The dangers and abuses of people's

data are well-known, and have been getting worse now for a full generation. It is long past time for Massachusetts to act. **Please take every necessary action to bring MDPA to the floor, and in the case of the House, to ensure that a substantially similar bill is reported out by the House members of the Joint Committee on Advanced IT, the Internet, and Cybersecurity, through Ways and Means to the floor.**

Massachusetts residents innocently use their cell phones every day to check the weather or the traffic, find a store, buy products and services, post on social media, and research their interests or medical questions. But with every action, their phone's Mobile Advertising ID enables companies to collect their data and sell it to data brokers or market it in the real-time bidding stream, [where it is purchased or freely intercepted](#) to target advertising to them and to [create dossiers](#) on nearly all Massachusetts residents.

The companies participating in this abuse of Americans' data [include](#) well-known companies like Acxiom, LexisNexis, Nielsen, Experian, Equifax, CoreLogic, Verisk, Oracle and Epsilon, and a whole ecosystem of less-recognized companies like [Babel Street](#), [Gravy Analytics/Venntel](#), [Mobilewala](#) and [Outlogic/X-Mode](#). They package and sell consumer data [without scrutinizing](#) either the origin of the purchasing companies or their purpose. A number of companies have been selling precise geolocation data on everyone from [people entering medical and reproductive health clinics](#) to [protesters](#). [Amazon](#), [Meta \(Facebook\)](#), [Google](#), [ByteDance](#) and [X](#) all collect our sensitive personal data, including medical, financial, precise geolocation data and more, from numerous apps. Out-of-state law enforcement can subpoena Web searches and social media communications from commercial platforms to investigate whether a traveller to or student in MA has received gender-affirming or abortion care here, or has participated in a protest. **In short, whether we're seeking sensitive types of medical care or not, we all need reasonable privacy protections, of the kind the MDPA would provide.**

Our [college students](#), [election workers](#), [journalists](#), [judges](#), [librarians](#), [police officers](#), [public health workers](#) and [teachers](#), along with members of [Jewish](#), [Muslim](#) and [LGBTQ](#) communities, have all been victims of doxing. Many of these have received threats to harm them or their family members. [Our active duty troops](#) are sitting ducks because of the [ease](#) with which their [precise location](#) can be identified. Our government workers, from members of Congress and of the intelligence community on down, including workers for the state government, are at risk of being targeted by foreign governments that access sensitive information about [them and their family members](#), including their [financial situation](#), [medical](#) and [mental health conditions](#). What data brokers have on us can include whether we have [participated in alcohol or drug rehab](#), our [religious affiliation](#) and even the [bars, clubs](#) and [brothels](#) Massachusetts residents may frequent. This data is increasingly analyzed using AI to infer characteristics that are [frequently](#)

[inaccurate](#) and can negatively impact everything from, [employment and housing opportunities](#), [eligibility for government benefits](#) or [loans](#), decisions about [criminal sentencing, probation and parole](#) and more. Victims of domestic abuse face a [higher risk of being stalked](#), harassed and attacked because of the ease with which their data can be [purchased from people-search websites](#) such as [Spokeo and Intelius](#). **In short, we are all vulnerable, in ways that go well beyond whether our real-time location in particular is collected, bought or sold.**

The massive volume of data being collected by data brokers and sold to both companies and agencies of the U.S. government vastly expands the attack surface for hackers. According to the [Identity Theft Research Center's 2024 Annual Data Breach Report](#), 3,158 data compromises affected Americans in 2023 necessitating 1,350,835,988 victim notifications owing to the large number of victims affected by several of these breaches. These data breaches affected Americans' ability to access healthcare, and paralyzed infrastructure for shipment of oil and fossil fuels. Other hackers exposed the [communications of our Treasury Secretary](#) and of [candidates for President and Vice President](#), and the [campaign staff for another Presidential candidate](#), among those of many other Americans. Companies must do far more to secure their [data](#). **A piecemeal, sectoral approach has been tried and has failed. Companies are not doing enough to secure Americans' data. The only real way to rein in the collection and sale of our data and to protect it from security breaches is via regulation, oversight and enforcement.**

The MDPA facilitates all of these, through the following provisions.

1. Strong data minimization provisions which limit
 - a. the collection and use of **personal data** to what is **reasonably necessary** for a company to provide the data or service requested by a consumer
 - b. The collection and use of **sensitive data** to what is **strictly necessary** to provide the data or service requested by a consumer
2. A clear list of all of the kinds of data that must be regarded as sensitive.
3. Prohibition on the sale of sensitive data.
4. Requires affirmative consent of a consumer before each transfer of their personal data.
5. Provides every consumer with the right to see, correct verifiable inaccuracies in, and delete their personal data that has been collected by a company.
6. Gives consumers the right to opt out of targeted advertising or automated profiling.
7. Requiring that companies provide a clear and obvious privacy notice about their data collection practice and security measures and method to contact them for execution of all of a consumer's rights.
8. Establishes a free automated mechanism whereby consumers can learn whether a data broker possesses their data and can request that their data be deleted.

9. Requires Data Brokers to be audited to ensure that they are removing data as requested or at least no longer selling the data.
10. Enforces all of the provisions through both civil action by the Attorney General and a private right of action so that consumers and groups representing them can sue companies with gross annual revenues of over \$20 million that violate their rights for injunctive relief and damages.

We ask that you do everything possible to advance [S.2516](#). MA residents should be able to rest easier, without having to factor into every interaction with the modern economy, an increased risk of being doxed, stalked, breached, exploited, or mischaracterized by data profiles and black-box AI systems operating on that data.

We are attaching the more detailed file “The Urgent Need for the Effective Comprehensive Data Privacy Protection Created in the Massachusetts Data Privacy Act (S.2516)”. This document:

- Describes the major provisions of [S.2516](#);
- Provides details on the abuses of U.S. consumer data as documented by the Consumer Financial Protection Bureau and the Federal Trade Commission;
- Explains that these agencies will no longer be pursuing data privacy abuse cases;
- Describes impacts of major data breaches occurring in the U.S. just in the last 2 years;
- Provides information on how law enforcement at the local, state and federal levels are all freely purchasing our sensitive personal data and have used it to predict people at risk of committing crimes and to warrantlessly identify protesters and others engaged in legal and protected activities; and
- Provides evidence as to how the enforcement of state data privacy bills can have a major impact in reining in the abuses of our private data.

If you have questions or concerns about this bill, please reach out to Digital Fourth Co-Chair Julie Bernstein, at julie.bernstein.borhani@gmail.com. Thank you very much for your consideration of this important comprehensive data privacy legislation.

Sincerely,

Digital Fourth
AFT Massachusetts
Check My Ads Institute
Clinic to End Tech Abuse (CETA) at Cornell
Tech
Fight for the Future

Manchester Democratic Town Committee
(Manchester-by-the-Sea, MA)
Massachusetts AFL-CIO
National Council of Jewish Women
(Massachusetts)
YW Boston