epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

April 9, 2025

The Honorable Michael O. Moore, Chair
The Honorable Tricia Farley-Bouvier, Chair
General Court of the Commonwealth of Massachusetts
Joint Committee on Advanced Information Technology, the Internet and Cybersecurity

Dear Chair Moore, Chair Farley-Bouvier, and Members of the Committee:

EPIC writes in support of H.78, the Massachusetts Consumer Data Privacy Act (MCDPA), and S.45/S.29/H.104, the Massachusetts Data Privacy Act (MDPA). EPIC appreciates the leadership of Chairs Moore and Farley-Bouvier in their sponsorship of these bills, as well as the leadership this Committee has shown in recent years on the issue of privacy.

The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC has long advocated for comprehensive privacy laws at the state and federal levels.[2]

The MCDPA and MDPA build on existing state privacy laws already enacted in nineteen states, provide predictability and clarity for Massachusetts businesses, and incorporate essential provisions to provide Massachusetts consumers with the protections they need to stay safe online.[3] Key provisions of the MCDPA and MDPA include:

- **Data minimization:** The MCDPA and MDPA establish limits on the unfettered processing of personal data by setting a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to provide or maintain a product or service requested by the individual. The Maryland Online Data Privacy Act, enacted last year, includes data minimization rules, as does legislation filed this session by the original sponsor of the Connecticut Data Privacy Act to update that law.

- **Strong protections for sensitive data:** The MCDPA and MDPA set heightened protections for sensitive data (i.e., biometrics, location, health data) such that its collection and use must be strictly necessary for the product or service the consumer is asking for. The MCDPA bans

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See* e.g. EPIC, *The State Data Privacy Act: A Proposed Model State Privacy Bill*, https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/.
[3] *See* EPIC and U.S. PIRG Education Fund, *The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better* (Jan. 2025), https://epic.org/state-of-privacy-2025/.

the sale of sensitive data, a protection included in the recently enacted Maryland Online Data Privacy Act.

- **Strong enforcement mechanisms:** By providing consumers with the option to vindicate their rights via a private right of action, the MCDPA and MDPA give consumers the same strong enforcement options for privacy violations that they have long had for other violations of their rights as consumers.

- **Preventing discrimination:** The MCDPA and MDPA extend civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, sexual orientation, gender, or disability.

- **Protections for children and teens:** The MCDPA and MDPA prohibit targeted advertising to minors under age 18 and bans the sale of minors' data, which is also included in Maryland's law.

- **Rulemaking authority:** Attorney General rulemaking authority in a privacy law is essential to allow the law to keep pace with constantly evolving technologies and to effectively implement the technical requirements under the bill.

In my testimony, I will discuss why it is so critical that Massachusetts enact a strong privacy law, the current state of state privacy laws, and go into detail on a few key protections that are crucial to keep Massachusetts consumers safe online.

Data Abuse is Hitting Your Constituents' Wallets

Advertisers and data brokers track our move online, and our data is used against us in ways that harm our wallets, opportunities, and rights. At a time when policymakers are concerned about cost-of-living issues for their constituents, the impact of mass data collection and abuse on those costs cannot be ignored. A few examples of these harms include:

1. **Increased insurance premiums.** Texas Attorney General Ken Paxton recently sued insurance giant Allstate and its subsidiary Arity for unlawfully collecting, using, and selling data about the location and movement of Texans' cell phones through secretly embedded software in mobile apps, such as Life360 and GasBuddy. Paxton alleged that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.[4]

[4] Press Release, Att'y Gen. of Texas, *Att'y Gen. Ken Paxton Sues All-state and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Cos.* (Jan 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

2. **Increased pricing on consumer goods**. The Federal Trade Commission recently released initial findings from a study on surveillance pricing, a practice that uses data about consumers' characteristics and behavior to alter prices. "Initial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage," said then-FTC Chair Lina M. Khan.[5]

3. **Targeted advertisements can be predatory and harmful.** Targeted ads can be predatory and harmful, using people's online behavioral data to reach vulnerable consumers who meet specific parameters. People searching terms like "need money help" on Google have been served ads for predatory loans with staggering interest rates of over 1,700%.[6] An online casino targeted ads to problem gamblers, offering them free spins on its site.[7] A precious metals scheme used Facebook users' ages and political affiliations to target ads to get users to spend their retirement savings on grossly overpriced gold and silver coins.[8]

Small businesses are harmed by these systems as well. For years, they've been told that success hinges on pouring money into online behavioral advertising, controlled by a handful of tech giants. They enter bidding wars against corporate behemoths. This isn't a level playing field. It's a digital black hole—swallowing resources and crushing entrepreneurial spirit, all to facilitate targeted advertising that is of dubious efficacy.

The State of State Privacy Law: Existing Laws Don't Do Enough

Because there is not a federal comprehensive privacy law in the U.S., states have been passing laws to fill this void. Since 2018, 19 states have passed comprehensive privacy laws. EPIC, in partnership with U.S. PIRG, recently released a report grading these state laws.[9] Of the 19 laws enacted, eight received Fs, and none received an A. These laws provide few meaningful privacy rights for consumers and do little to limit mass data collection and abuse.

---

[5] Press Release, Fed. Trade Comm'n, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[6] Shanti Das, *Google Profiting from 'Predatory' Loan Adverts Promising Instant Cash*, The Guardian (Mar. 13, 2022), https://www.theguardian.com/technology/2022/mar/13/google-profiting-from-predatory-loan-adverts-promising-instant-cash.

[7] Rob Davies, *Online Casino Advert Banned for Targeting Problem Gamblers*, The Guardian (Oct. 9, 2019), https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling.

[8] Jeremy B. Merrill, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives*, Quartz (Nov. 19, 2019), https://www.yahoo.com/video/facebook-fueled-precious-metal-scheme-110044886.html.

[9] EPIC and U.S. PIRG Edu. Fund, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC and U.S. PIRG (Jan. 2025), https://epic.org/state-of-privacy-2025/.

Many of these state laws closely follow a model initially drafted by tech giants.[10] This draft legislation was based on a privacy bill from Washington state that was modified at the behest of Amazon, Comcast, and Microsoft.[11] An Amazon lobbyist encouraged a Virginia lawmaker to introduce a similar bill, which became law in 2021. Virginia's law received an F on our scorecard. Unfortunately, this Virginia law became the model that industry lobbyists pushed other states to adopt. In 2022, Connecticut passed a version of the Virginia law with some additional protections, which has now become the version pushed by lobbying groups doing the bidding of Big Tech companies in select states. Privacy laws, which are meant to protect individuals' privacy from being abused by Big Tech, should not be written by the very industry they are meant to regulate.

Laws based on industry's model bill provide very few protections for consumers. These laws do not meaningfully limit what data companies can collect or what they can do with that data — they merely require that companies disclose these details in their privacy policies, which consumers rarely read or understand. Companies should not be allowed to determine for themselves what are the permissible purposes of collecting and using consumers' personal information. Without meaningful limitations, companies can, and do, claim that they need nearly unlimited data collection, transfer, and retention periods in order to operate their businesses. Unfortunately, the limitations on data collection in the Connecticut Data Privacy Act allow companies to do just that. The CTDPA reads:

> A controller shall […] Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.

This reinforces the failed status quo of "notice and choice" — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. In fact, it incentivizes companies to list as many purposes as possible, and as broadly as possible, to cover every conceivable reason they would ever want to collect your data. And the only "choice" the consumer has is to not use the service at all. The clearer limits on data collection and use in the MCDPA and MDPA are critical because they require companies to better align their data practices with what consumers expect, allowing Massachusetts consumers to use online services without being forced to sacrifice their privacy.

[10] Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, Reuters (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/.

[11] Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), https://www.protocol.com/policy/virginia-maryland-washington-big-tech; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law* (Apr. 2019), https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/.

Data Minimization, Sensitive Data Protections, and Strong Enforcement: The Keys to a Strong Privacy Law

Data Minimization

The MCDPA and MDPA rely on a concept that has long been a pillar of privacy protection: data minimization.

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. Yet these business practices are widespread. Nearly every online interaction is tracked and cataloged to build detailed profiles and target consumers with ads. Even offline, credit card purchases, physical movements, and "smart" devices in homes create countless data points that are logged and tracked without consumer awareness or control.

To incentivize better data practices, the MCDPA and MDPA set a baseline requirement that entities only collect, use, and transfer data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the consumer. This standard is referred to as "data minimization" and it better aligns business practices with what consumers expect.

Data minimization is not a new concept. Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization.

The Maryland Online Data Privacy Act, which was enacted last year, and the California Consumer Privacy Act also include provisions requiring a form of data minimization. The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in its privacy policy.

Lobbyists representing Big Tech interests will typically fight against a strong data minimization provision by arguing that it would block specific data uses or harm the online ecosystem by blocking advertising. But a strong data minimization standard will not prevent businesses from advertising. Rather, these laws will encourage ad tech providers to innovate on privacy-protective forms of advertising so that small businesses can continue connecting with customers in a trustworthy way.

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data.

A Ban on the Sale of Sensitive Data Prevents Some of the Worst Data Harms

The MCDPA and MDPA set heightened protections for sensitive data such that its collection and use must be *strictly necessary* to provide the product or service the consumer is asking for. This is a critical provision that protects the data we all consider to be the most sensitive, such as our location, health, and financial data. H.78 bans the sale of sensitive data entirely, a protection included in the recently enacted Maryland Online Data Privacy Act.

Many an app has likely prompted you to request access to your location. Sometimes, the app has a legitimate reason to access the information, like displaying your local weather. Sometimes, it doesn't. In either case, the app may be selling your location data to a third party. A top Catholic Church official was forced to resign a few years ago after a Catholic media site used cellphone data to show that the priest was a regular user of the queer dating app Grindr and visited gay bars.[12]

Apps are not the only way your location data ends up on the open market. Earlier this year, General Motors (GM) and its subsidiary OnStar agreed not to sell drivers' location data for five years following an investigation by the Federal Trade Commission. "GM monitored and sold people's precise geolocation data and driver behavior information, sometimes as often as every three seconds," said FTC Chair Lina M. Khan. The FTC's complaint alleged that GM and OnStar were selling drivers' precise geolocation to consumer reporting agencies and other third parties.

The location data market is a multi-billion-dollar industry[13] centered on collecting and selling people's everyday comings and goings, often collected from people's mobile devices and often without their knowledge or explicit consent. This can lead to harms such as scams, stalking, data breaches, or even prosecution for those traveling to Massachusetts to seek gender-affirming or reproductive health care.

We encourage the Committee to include a ban on the sale of sensitive data in any Committee report on comprehensive privacy legislation. Additionally, EPIC requests that the Committee give a favorable report to H.86/S.197, the Location Shield Act so that if the Legislature is not willing to advance a strong privacy bill, it can consider at minimum protecting precise geolocation data.

[12] Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.
[13] Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

Enforcement is Critical

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority is an essential component of a strong privacy law, and funds should be appropriated to ensure the Attorney General can meaningfully enforce the law.

However, while government enforcement is essential, the scope of online data collection is simply too vast for one entity to regulate. A private right of action ensures controllers have strong financial incentives to comply with privacy laws. We have seen evidence of this in Illinois,[14] where a biometric privacy law passed in 2008 includes a private right of action. Lawsuits under that law have led to changes to harmful business practices, such as forcing facial recognition company Clearview AI to stop selling its face surveillance system to private companies.[15] In contrast, in states where Attorneys General have sole enforcement authority, we have seen little enforcement of (and compliance with) privacy laws.[16]

Many privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations.[17] Massachusetts consumers have had the right to vindicate their consumer rights in court under Chapter 93A for decades. There is no reason privacy violations should be treated differently than other violations of consumer rights. We encourage the Committee to retain this provision.

* * *

Privacy is a fundamental right, and it is time for business practices to reflect that reality. Massachusetts has an opportunity to provide real privacy protections for Massachusetts residents while allowing Massachusetts businesses to thrive. EPIC asks that you advance a Committee report that includes the strong protections set out in the MCDPA and MDPA. I am happy to be a resource to the Committee as it navigates this complex topic and can be reached at fitzgerald@epic.org.

Sincerely,

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
Deputy Director, EPIC

---

[14] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf.
[15] Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database*, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.
[16] *See generally* Consumer Reports, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws* (Apr. 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf.
[17] *See* Lauren Henry Scholz, *Private Rights of Action in Privacy Laws*, 63 Wm. & Mary L. Rev. 1639 (2022), https://scholarship.law.wm.edu/wmlr/vol63/iss5/5.