October 24, 2025

The Honorable Ronald Mariano
Speaker of the House of Representatives
State House, Room 356
Boston, MA 02133

The Honorable Aaron Michlewitz
Chair, House Ways & Means Committee
State House, Room 243
Boston, MA 02133

Re: Massachusetts Comprehensive Data Privacy Legislation

Dear Speaker Mariano and Chair Michlewitz,

Consumer Reports[1] strongly supports S. 2619, the Massachusetts Data Privacy Act (MDPA), comprehensive privacy legislation that would create critical protections to safeguard the privacy of Massachusetts consumers' personal data and that the Senate unanimously approved earlier this session. The bill would require businesses to abide by strong data minimization provisions, which would prevent them from collecting personal information that is not necessary to provide the specific product or service requested by consumers. It would also extend to Massachusetts consumers important new protections relating to their personal information, including prohibitions against selling sensitive data (including precise geolocation) outright, a ban on the use of sensitive data for targeted advertisements, restrictions against targeting advertisements to children, and more.

S. 2619 reflects the progress made in states around the country that have attempted to tackle comprehensive privacy legislation. Its underlying structure is very similar to one already utilized by more than a dozen other states—while including targeted improvements already adopted in other state privacy laws and incorporating feedback from regulators tasked with enforcing existing laws.[2] Consumer Reports also supports similar legislation in the House, H. 78, the

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] See, e.g., Connecticut Office of the Attorney General, Updated Enforcement Report Pursuant To Connecticut Data Privacy Act (recommending the legislature adopt data minimization provisions), Conn. Gen. Stat. § 42-515, Et Seq, (April 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privac

Massachusetts Consumer Data Privacy Act (MCDPA), which would accomplish many of the same objectives.

Under current Massachusetts law, consumers possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, companies have amassed massive amounts of data about consumers, which is often combined with their offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is often retained for indeterminate amounts of time, sold as a matter of course, and is used to deliver targeted advertising, facilitate differential pricing, and enable opaque algorithmic scoring—all of which, aside from reducing individual autonomy and dignity, can result in concrete harms for consumers, financial and otherwise.[3]

S. 2619 corrects that imbalance by establishing strong privacy protections over consumers' personal information. We urge you to act swiftly to advance privacy legislation that contains the below principles:

Strong Data Minimization Provisions

By far, S. 2619's most important contribution to consumer privacy is the prohibition in Section 5 against businesses collecting personal information unless "reasonably necessary" to provide or maintain "a specific product or service requested by the consumer to whom the data pertains." In today's digital economy, consumers are often faced with an all-or-nothing proposition: they may either "choose" to consent to a company's data processing activities, or be forced to forgo the service altogether if they do not approve of any one of a company's practices (which often allow the business to sell the consumer's information to vaguely defined third-parties or build future artificial intelligence products using their information).

A strong privacy law should limit the data companies can collect to match what consumers expect based on the context of their interaction with the business. For example, a mobile flashlight application should not be permitted to collect troves of personal information because such information is not necessary to provide the service requested and the collection of that data is unlikely to be in the consumer's interest.

---

y-act-conn-gen-stat--42515-et-seq.pdf; Oregon Department of Justice, Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months, (March 2025), https://www.doj.state.or.us/wp-content/uploads/2025/03/OCPA-Six-Month-Enforcement-Report.pdf

[3] See, e.g., Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

In contrast, the core of the framework currently favored by industry is "notice-and-choice," which focuses on disclosures in privacy policies. The law allows businesses to continue collecting whatever personal data they want and using it for any reason they want as long as they disclose those practices in their privacy policies and allow consumers to opt out. However, very few consumers have the time to read privacy policies in practice, and would likely struggle to decipher their lengthy legalese even if they did.

Moreover, the notice-and-choice framework offloads all of the burden of consumer protection onto consumers themselves, while absolving companies of the responsibility to engage in responsible data collection. This very dynamic was highlighted by the Connecticut Office of the Attorney General in its recent enforcement report, where it recommended legislative amendments to strengthen the CTDPA, stating that the: "notice-and-consent model sets an exploitable standard— businesses can seek to justify unnecessary data collection by deeming such collection 'adequate, relevant and reasonably necessary' to the purposes disclosed to consumers."[4]

S. 2619 would resolve this tension by ensuring consumers' privacy by default and reducing the responsibility individuals must take to protect themselves. At the same time, the bill preserves the ability for businesses to use personal data that was responsibly collected in order to market to consumers, make recommendations, or personalize services. The bill simply states that businesses must provide consumers with the ability to opt-out of targeted advertising, as is the case with all of the other comprehensive state privacy laws that have passed to-date.

Sensitive Data Protections

Companies should not be profiting from the sale of consumers' most personal data, such as children's data or data about a consumer's race, religion, sex life, finances, precise geolocation, or health. The bill appropriately bans this behavior, as was done in Maryland's recent comprehensive privacy law.[5] Similar legislation was recently signed into law in Oregon.[6]

Some examples of harmful uses of consumers' sensitive data include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use sensitive data to target vulnerable individuals for scams, or otherwise use personal information to cause

[4] Connecticut Office of the Attorney General, Updated Enforcement Report Pursuant To Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515, Et Seq, (April 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf

[5] Maryland Online Data Privacy Act of 2024, Section 14–4607(A)(2), https://mgaleg.maryland.gov/2024RS/bills/sb/sb0541E.pdf

[6] Oregon HB 2008, https://olis.oregonlegislature.gov/liz/2025R1/Downloads/MeasureDocument/HB2008/Enrolled

harm. For example, scammers can use commercially available location data to increase the specificity of their phishing or social engineering scams, such as by including location-specific details, like mentioning a nearby business or the individual's recent activity.[7] Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.[8]

- *Predatory use of consumer data.* The sale of consumer data can result in financially disastrous consequences for consumers. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products. And a recent case brought by the Texas Attorney General alleged that the insurance company Allstate secretly purchased information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.[9] They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

- *Data breaches.* Data brokers sit on trillions of data points, many of them sensitive and purchased from other businesses. Unsurprisingly, this makes them a top target for hackers and cyber criminals. For example, the data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones every day,[10] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[11] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[12]

---

[7] Phishing Box, Tracking Data: Identifying the Anonymized, https://www.phishingbox.com/news/post/tracking-data-identifying-anonymized

[8] Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs

[9] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

[10] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf

[11] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

[12] Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S.Military Personnel, (November 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf

Civil Rights Protections

A key harm observed in the digital marketplace today is the disparate impact that can occur through processing of personal data for the purpose of creating granularized profiles of individuals based off of data both collected and inferred about them. Therefore a crucial piece of strong privacy legislation is ensuring that a business' processing of personal data does not discriminate against or otherwise makes opportunity or public accommodation unavailable on the basis of protected classes. We appreciate that S. 2619 contains specific language prohibiting the use of personal information to discriminate against consumers.

At the same time, we do recommend certain improvements to ensure that the legislation appropriately protects consumers:

Restore Strong Enforcement Provisions

Currently, the bill does not include a private right of action. We urge you to restore a private right of action that applies to covered businesses other than small businesses—and does not include a so-called "right to cure" in the administrative enforcement section. "Right to cure" provisions could force law enforcement to waste precious time and money building cases that go nowhere. In general, laws do not and should not contain provisions that wrongdoers can simply stop illegal behavior once they are caught and avoid any consequences entirely.

Further, consumers should be able to hold companies accountable in some way for violating their rights. Unfortunately, most state Attorney General offices are under-resourced and do not have the capacity to bring enough actions to meaningfully deter illegal behavior, meaning consumers may have no recourse in the event of a violation that harms them. Despite ample evidence suggesting widespread non-compliance with existing privacy laws,[13] there have not been commensurate enforcement efforts to-date. Consumer Reports has put out a number of reports demonstrating noncompliance with state privacy laws, including a recent report showing that many companies were showing targeted ads despite receiving legally binding universal opt-out signals.[14] Yet, to our knowledge, there are more states with active comprehensive privacy laws

[13] See, e.g. two separate studies indicating that less than 30 percent of top websites comply with universal opt-out requests: Privado, State of Website Privacy Report 2024, (December 2024), https://www.privado.ai/state-of-website-privacy-report-2024; Data Grail, Data Privacy Trends Report, https://www.datagrail.io/resources/interactive/data-privacy-trends/, (December 2024)

[14] Matt Schwartz *et al.*, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports, (Apr. 1, 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf

(13) than there have been public enforcement actions. It is therefore unsurprising that market behavior has yet to improve.

That said, while we think that an allowance for both public and private enforcement mechanisms makes sense—dozens of other consumer protection laws do the same—and are generally skeptical of claims that such an approach would open the floodgates to frivolous litigation, we are open to discussing guardrails to prevent that outcome if raised in good-faith.

Protections for Data Collected Through Loyalty Programs

Section 5(b) of the bill no longer includes common-sense protections that prevent controllers from ignoring consumers' privacy rights requests when they relate to data collected through loyalty programs. The language of the bill should be amended to prevent controllers from selling consumer data collected through loyalty programs for purposes unrelated to providing the benefits of the program.

To be clear, we understand why privacy laws may need to include some exceptions to allow loyalty programs to function properly. For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing that is *functionally necessary* to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. However, controllers do not need to sell data to others or to engage in cross-context behavior advertising in order to operate a bona fide loyalty program – such behaviors have nothing to do with the tracking of purchases to offer discounts or the ability to offer first-party advertising.

This matches with consumer expectations around loyalty program data. In November 2024, Consumer Reports conducted a nationally representative survey of 2,108 adult American consumers and found that 70 percent of consumers who belong to loyalty programs would be at least somewhat concerned if a company sold information about them obtained through their loyalty program to other companies for unrelated purposes.[15] Moreover, 79 percent of Americans said they would support a law limiting companies to collecting only the data they need to provide customers with loyalty program benefits.[16]

While consumers typically view loyalty programs as a way to get rewards or save money based on their repeated patronage of a business, they do not expect all the secondary use and sharing of

[15] Consumer Reports, November 2024 American Experiences Survey Omnibus Results, (November 2024), https://article.images.consumerreports.org/image/upload/v1734120809/prod/content/dam/surveys/Consumer_Reports_AES_November_2024.pdf
[16] *Id.*

data that companies can engage in.[17] For example, many grocery store loyalty programs collect information that go far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store.[18] This information is used to create detailed user profiles and is regularly sold to other retailers, social media companies, and data brokers, among others. Data sales are extremely profitable for such entities — Kroger estimates that its "alternative profit" business streams, including data sales, could earn it $1 billion annually.[19] At a minimum, businesses should be required to give consumers control over how their information is collected and processed pursuant to loyalty programs, including the ability to participate in the program without allowing the business to sell their personal information to third-parties.

******

We look forward to working with you to ensure that Massachusetts consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst

[17] Joe Keegan, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, The Markup, (February 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you
[18] *Id.*
[19] *Id*.