TO: Senate President Karen Spilka
Speaker of the House Ronald Mariano
Sen. Cindy Creem, *Senate Majority Leader*
Sen. Barry Finegold, *Chair, Joint Committee on Economic Development and Emerging Technologies*
Sen. Patrick O'Connor, *Assistant Minority Leader*
Rep. Michael Moran, *House Majority Leader*
Rep. Tricia Farley-Bouvier, *Chair, Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity*
Rep. David Vieira, *Third Assistant Minority Leader*

Dear Senate President Spilka, Speaker Mariano, and Honorable Members of the Conference Committee:

EPIC and Consumer Reports write to thank you for enacting strong data privacy legislation to protect the privacy of Massachusetts consumers. We appreciate the leadership both chambers have displayed in advancing a comprehensive data privacy law that contains meaningful protections and is backed up by robust enforcement.

Our organizations have been heavily involved in the debate on similar bills across the country over many years. The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization, established in 1994 to secure the fundamental right to privacy in the digital age for all people. Founded in 1936, Consumer Reports Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace.

A strong privacy bill must limit the amount of personal data that is collected about us and place meaningful limits on how it can be used. It must provide heightened protections for our most sensitive data, including precise geolocation data and data about kids and teens. And, critically, it must provide mechanisms for effective enforcement of the law to ensure compliance. We commend both chambers for including some combination of these priorities in S.2619 and H.5479.

The thoughtful work that both chambers has already invested in these bills gives the Legislature the opportunity to enact a law that provides Massachusetts residents with the protections they need to stay safe online and in their communities. Because our organizations have been involved in privacy advocacy at the state level for many years, we are familiar with recurring patterns of contention and compromise between businesses and consumer privacy advocates and we are happy to be a resource to the conference committee as it negotiates a compromise between the two bills.

We respectfully request the conference committee prioritize the following protections, and we go into more detail on each below:

1. The strict data minimization rules for the collection and processing of sensitive data from S. 2619;
2. The private right of action (incl. class actions under c.93A §§9/11) against large data holders in H. 5479;
3. The data minimization rules for non-sensitive data from S. 2619;
4. The ban on the sale of sensitive data from S. 2619;
5. The broader definition of sensitive data and narrower definition of publicly available data from H. 5479;
6. The loyalty program restrictions from H. 5479;
7. A combination of the permissible purposes in Sec. 9 of S. 2619 and Sec. 12 of H. 5479 to ensure the exceptions to the law do not swallow the rule.

1. Retain Senate data minimization rules for sensitive data.

Privacy laws must require businesses to minimize the amount of personal data they collect and limit secondary uses of that data. This is especially true for sensitive data such as precise geolocation data, minors' data, and health data. We respectfully ask the conferees to include the sensitive data protections in Sec. 5(a)(iii) of S. 2619 in the final bill.

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose and duration necessary to provide the goods or services that they requested. For example, a consumer looking up health symptoms on a website would not reasonably expect that their search terms or page they were viewing would be disclosed to third parties and combined with other data to profile them. And indeed, providing this service does not *require* selling, sharing, processing, or storing consumer data for unrelated secondary purposes. Yet these business practices are widespread. Nearly every online interaction is tracked and cataloged to build and enhance detailed profiles and retarget consumers with ads.

Sec. 5(a)(iii) of S. 2619 sets a baseline requirement that entities only collect, process, or transfer sensitive data that is "*strictly necessary*" to provide or maintain a product or service requested by the consumer. This standard allows companies to use sensitive data for legitimate business purposes while eliminating harmful practices that serve only to increase profits rather than benefiting consumers.

The Maryland Online Data Privacy Act includes the same rule as Sec. 5(a)(iii) of S. 2619, so many companies are already familiar with and complying with this rule.

Opt-in consent alone would not adequately protect Massachusetts residents from the abuse of their sensitive data. While many other states currently use an "opt-in" standard for sensitive data, this has not stemmed the tide of data abuses. In those states, many businesses simply *require* you to consent to the sale of your sensitive data as a condition of using the app or website, often through confusing pop-up notices or in long boilerplate privacy policies. This type of structure fails to meaningfully protect consumers. And ultimately, forcing consumers to make constant consent choices is not the solution to this problem. Instead of playing the cat-and-mouse consent game, privacy laws should simply prohibit unnecessary uses of sensitive data.

We respectfully ask the conferees to include the sensitive data protections in Sec. 5(a)(iii) of S. 2619 in the final bill.

2. Retain private right of action from the House bill

Sec. 14(a) of H. 5479 provides consumers with a private right of action under Chapter 93A when the entity violating the law is a "large data holder." Robust enforcement is the backbone of meaningful privacy protection. Without a real threat of enforcement, entities can simply ignore the law, particularly multi-billion dollar tech firms that can simply bake the risk of government enforcement into their budget as a cost of doing business. In order to encourage compliance with the law, we respectfully ask the conference committee to retain the private right of action against large data holders from the House bill.

While the Massachusetts Attorney General's office has a strong history of protecting data privacy, the scope of online data collection is simply too vast for one entity to regulate. Just one case against a Big Tech company would take the entire Privacy & Responsible Technology Division's staff time for years on end. A private right of action ensures controllers have strong financial incentives to comply with privacy laws. We have seen evidence of this in Illinois,[1] 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.[2] In contrast, in states where

[1] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the U.S.?*, AI Now Institute (2020), https://scholarship.law.bu.edu/faculty_scholarship/3086/.
[2] 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.

Attorneys General have sole enforcement authority, we have seen little enforcement of (and compliance with) privacy laws.[3]

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.[4] 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 or for Big Tech companies to not face the same penalties for violating Massachusetts law than other consumer-facing companies have done for decades.** We encourage the Conference Committee to retain Sec. 14(a) of H. 5479.

3. Retain data minimization rules for *non*-sensitive data from the Senate bill.

As discussed in section 1 above, privacy laws should set strong default limits on the data that companies can collect and use so that consumers can use online services or apps safely. This is true for all personal data, not just sensitive data.

While both the House and Senate bills include limits on the collection of personal data generally, we believe the rule in the Senate bill is clearer and will provide stronger consumer protections while also easing compliance for companies who are already complying with Maryland's law. Sec. 5(a)(i) of S. 2619 sets a baseline requirement that entities only collect personal data that is "*reasonably necessary*" to provide or maintain a specific product or service requested by the consumer. This standard aligns business practices with what consumers expect. We respectfully request that the Conference Committee retain the language from Sec. 5(a)(i) of Sec. 2619 in the final bill.

Data minimization is essential for both consumers and businesses. Data minimization principles provide much-needed standards for data security, access, and accountability, assign responsibilities with respect to user data, and restrict data collection and use. Indeed, a data minimization rule can provide clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. Data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

---

[3] *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.
[4] *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.

4. Retain the ban on the sale of sensitive data from the Senate bill.

S. 2619 bans the sale of all sensitive data, while H. 5479 bans the sale of precise geolocation data but allows for the sale of other sensitive data with consumer consent. Companies should not be allowed to *sell* our most sensitive personal data for profit. We respectfully request that the Conference Committee retain the Senate's ban on the sale of all sensitive data.

Unnecessary data sales of sensitive data 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. People often do not even know that data brokers sell extensive profiles about them. Criminals then use personal information obtained from data brokers to legitimize their attempts to scam and defraud consumers. Someone is more likely to fall for a phishing scam when the message includes accurate information about their location, employment, or bank accounts. Further, fraudsters target certain groups, including retirees and veterans, using information from data brokers. Data brokers also enable harm against domestic violence survivors by providing a tool for abusers to locate and track victims.[5] Even when survivors are able to escape their abuser, survivors may continue to live in fear that their abusers may be able to find them again by purchasing data about their new home or job. Similarly, data brokers fuel violence against public officials.[6] People who wish to harm public officials can often purchase personal information such as home addresses, names of close relatives, and location data, from data brokers, enabling them to use it to find and harm public officials and their families.

The move towards more protective standards for sensitive data that do not rely solely on consent is a clear trend among states. Maryland, Oregon, Virginia, Connecticut, and New Jersey have banned the sale of some – or, in Maryland and New Jersey's cases, all – categories of sensitive information. Massachusetts should extend similar protections to its residents.

---

[5] *Data Broker Harms: Domestic Violence Survivors*, EPIC & NNEDV (Nov. 2024), https://epic.org/documents/data-broker-harms-domestic-violence-survivors/.

[6] *See, e.g.* Justin Sherman, *Disrupting the Data-to-Violence Pipeline: How Existing State Consumer Privacy Laws Fail America's Public Servants, Public Service Alliance* (Feb. 2026), https://thepublicservicealliance.com/psa-security-project/privacy-laws-report/.

5. Retain the broader definition of sensitive data and narrower definition of publicly available data from the House bill.

The House bill includes a broader definition of sensitive data that we respectfully request the Conference Committee maintain.

The House definition of sensitive data includes personal data *revealing* (A) racial or ethnic origin, color, national origin or citizenship or immigration status, or (B) religious beliefs. The Senate covers those data points themselves, but not data revealing it. The House language is consistent with many other state laws.

The House bill also includes a few additional categories of personal data including union membership, status as a military servicemember or veteran, and consumer health and wellness data which we feel are critical. Consumer health and wellness data, such as fitness data collected from a smartwatch, is in particular a form of personal data that most consumers consider sensitive (and often erroneously believe is covered by HIPAA, when indeed it is not.)

One area in this definition we feel is stronger in the Senate bill is the knowledge standard to determine who is a minor. The House bill covers situations where a company "knows, or willfully disregards" a consumer is a minor, while the Senate has a "knew or should have known" standard. A "knew or should have known" standard requires less of a burden for parents to prove that the company should have protected their child's data and will better protect minors online. It also aligns with the standard in Maryland's law, easing compliance for businesses. We ask that the Conference Committee retain the Senate's "knew or should have known" standard.

We also request that the Conference Committee retain the definition of "publicly available data" from the House bill. "Publicly available data" is carved out of the definition of personal data and therefore receives no protection under the law. It is therefore critical to ensure that it is drafted as narrowly as possible.

6. Retain the protections from abusive loyalty program practices from the House bill.

Loyalty programs take advantage of the exact type of informational asymmetry that privacy laws should strive to eliminate. While consumers typically view loyalty programs as a way to save money or get rewards based on their repeated patronage of a business, they rarely understand the amount of data tracking that can occur through

such programs.[7] For example, many grocery store loyalty programs collect information that extends far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store. 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 — grocery giant Kroger estimates that its "alternative profit" business streams, including data sales, could earn it $1 billion annually.[8] 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.

Sec. 7(b) of the House bill says that sales of personal data may not be a condition of participation in a loyalty program. This allows consumers to opt out of the sale of their personal information collected through the program without forfeiting their access to the loyalty program as a whole. It still allows the retailer to use the data for internal use, but they may not sell that data to third parties if the consumer opts out. The House bill also adopts language from California's law that says that loyalty programs may not use practices that are "unjust, unreasonable, coercive, or usurious in nature." We have seen in other states that broad exceptions for loyalty programs are often abused. The rules in Sec. 7(b) of the House bill are critical consumer protections and we urge the Conference Committee to retain them in the final bill.

7. Combine the permissible purposes in Sec. 9 of S. 2619 and Sec. 12 of H. 5479 to ensure the exceptions to the law do not swallow the rule.

Sec. 9 of the Senate bill and Sec. 12 of the House bill contain exemptions from the law for certain permissible purposes, such as complying with federal law and defending legal claims. But it is critical to draft these exemptions narrowly as any purpose listed here can be used as a loophole to circumvent the data minimization and sale restrictions in the bill.

Companies should not be able to ignore data minimization rules simply by claiming that a consumer's personal data is being used to "improve their product" or "perform internal operations" and then interpreting such language extremely broadly. The Senate and House bills both contain language in this section that, when combined, would avoid such loopholes. We outline our recommendations here.

---

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

We ask the Conference Committee to retain Sec. 9(a)(v) of S.2619. That subsection says that nothing in the Act restricts a controller or processor's ability to "provide a product or service specifically requested by the consumer." This mirrors language in over a dozen existing state privacy laws.

The version of this exemption in Sec. 12(a)(5) of H.5479 says that nothing in the Act restricts their ability to "provide, *maintain, improve or update* a product or service specifically requested by the consumer," which means a company could avoid the rules in the bill by claiming they need the personal data to "maintain, improve, or update" their product, which could be anything from training AI systems to selling location data in order to "improve" their product. *No state includes such a broad exemption.* We ask the Conference Committee to retain Sec. 9(a)(v) of S.2619.

We also ask that Sec. 12(a)(16) of H.5479 be retained, which requires that controllers or processors using the "internal operations" exemption only use personal data they have already collected in accordance with the Act. This should be adopted instead of the broader "internal operations" exemption in S.2619 §9(xvi), because "internal operations" should not be a standalone permissible purpose for collecting and using data. Companies should not be allowed to get around the limitations on data collection, use, and sales in the bill simply by claiming they need the data for "internal operations." We ask the Conference Committee to retain Sec. 12(a)(16) of H.5479.

* * *

Thank you again for your leadership on data privacy this session, and we are happy to be a resource to the Conference Committee throughout this process.

Sincerely,

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)
fitzgerald@epic.org

Justin Brookman
Director, Digital Marketplace Policy
Consumer Reports
justin.brookman@consumer.org