epic.org

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

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

October 19, 2023

The Honorable Tricia Farley-Bouvier, Chair
The Honorable Michael O. Moore, Chair
General Court of the Commonwealth of Massachusetts
Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
24 Beacon St. Room 109-B
Boston, MA 02133

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

EPIC writes regarding S.25/H.83, An Act establishing the Massachusetts Data Privacy Protection Act. For more than two decades, powerful tech companies have been allowed to set the terms of our online interactions. Without any meaningful restrictions on their business practices, they have built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit. But it does not have to be this way – we can have a strong technology sector while protecting personal 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 both the state and federal level.[2]

Last year in Congress, bipartisan leaders in Congress proposed the American Data Privacy and Protection Act ("ADPPA"). The bill went through extensive negotiations between members of Congress of both parties, industry, civil rights groups, and privacy groups. The ADPPA received overwhelming bipartisan support in the House Energy & Commerce Committee, where it was favorably approved on a 53-2 vote. Unfortunately, Congress failed to enact ADPPA, but state legislators can now take advantage of the outcome of those negotiations by modeling a state bill on its bipartisan consensus language – S.25/H.83 provides the Massachusetts Legislature with that opportunity.

Key provisions of the Massachusetts Data Privacy and Protection Act include:

[1] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[2] See e.g. Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf.

- **Data minimization:** Establishes 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 (or pursuant to certain enumerated purposes.)

- **Strict restrictions on sensitive data collection and use:** Sets heightened protections for collection and use of sensitive data (i.e., biometrics, geolocation, health data), which is only permitted when strictly necessary and not permitted for advertising purposes.

- **Civil Rights:** Extends 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.

- **Cross-context behavioral advertising prohibited:** The collection, use, and transfer of information identifying an individual's online activities over time and across third party websites and services is strictly limited and cannot be used for advertising.

- **Protections for children and teens:** Prohibits targeted advertising to minors under age 17. Personal data of minors is considered "sensitive data." These additional protections would only apply when the covered entity *knows* the individual in question is under age 17, though the standard for certain high-impact social media companies is "known or should have known," and for large data holders is "knew or acted in willful disregard of the fact that the individual was a minor."

- **Algorithmic fairness and transparency:** Requires large data holders to conduct algorithmic impact assessments, which include mitigation measures to avoid potential harms from the algorithms. Entities must also conduct algorithm design evaluations prior to deployment in some instances. The assessments and evaluations must be submitted to the Attorney General. A summary must be posted publicly.

- **Manipulative design restrictions:** Prohibits obtaining consent in ways that are misleading or manipulative (e.g., dark patterns). Prohibits deceptive advertising.

- **Individual Rights:** Gives consumers the rights to access, correct, and delete personal information about them. Consumers also have the right to opt out of both data transfers to third parties and targeted advertising. Also requires the Attorney General to recognize, and entities to honor, global opt-out mechanisms.

- **Service Providers:** Establishes requirements for service providers handling personal data, including a prohibition on commingling data from multiple covered entities. Service providers can only collect, process, and transfer data to the extent necessary and proportionate to provide service requested by covered entity.

- **Data Brokers:** Data Brokers must register with the Office of Consumer Affairs and Business Regulation. The OCABR will create a public registry of data brokers.

- **Small business protections:** Small businesses (as defined) are exempt from compliance with many provisions of the Act.

- **Executive responsibility:** An executive must personally certify each entity's compliance with the Act.

- **Enforcement:** The Attorney General may bring cases in court to remedy violations of this chapter and for other relief that may be appropriate.

- **Private Right of Action:** Individuals may enforce their rights under the Act by bringing a case against a covered entity seeking liquidated damages, punitive damages, injunctive relief, reasonable attorney's fees and litigation costs, and any other appropriate relief. Small businesses are exempt from this provision.

- **Rulemaking:** The Attorney General is empowered to issue regulations for purposes of carrying out the Act.

- **Adds workplace surveillance protections**: Though not originally addressed in ADPPA, the Massachusetts Data Privacy and Protection Act adds section 204 to the labor code, establishing protections for workers against electronic monitoring.

In my testimony I will discuss why it is so critical that Massachusetts pass a privacy law, what has been happening recently in Congress and state legislatures on privacy and go into detail on a couple of key concepts that are crucial in any strong privacy bill.

A. A Data Privacy Crisis: Surveillance Capitalism Run Wild

The notice-and-choice approach to privacy regulation that dominated the United States' response to uncontrolled data collection over the last three decades simply does not work. The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did. Technologies' prevalence in our work, social, and family lives leaves us with no "choice" but to accept. And modern surveillance systems, including the schemes used to track our digital and physical activities across the web and across devices, are too complex and opaque for the vast majority of internet users to understand or control.

A recent study from the Irish Council for Civil Liberties (ICCL) found that the Real-Time Bidding (RTB) market, which is the engine that tracks and shares what people view online and their location in order to drive targeted advertising, alone exposes the average American's data 747 times

per day.[3] This means U.S. Internet users' online activity and location is being tracked and disclosed 107 trillion times per year.[4] ICCL cited some dangerous examples of the use of this data:

> There is no way to restrict the use of RTB data after it is broadcast. Data brokers used it to profile Black Lives Matter protestors. The US Department of Homeland Security and other agencies used it for warrant-less phone tracking. It was implicated in the outing of a gay Catholic priest through his use of Grindr. ICCL uncovered the sale of RTB data revealing likely survivors of sexual abuse.[5]

BuzzFeed reported last year that religious social networking service and app Pray.com was collecting detailed information about its users, including the texts of their posts, and linking it with information obtained from third-parties and data brokers.[6] Pray.com was also releasing detailed data about its users with third-parties, including Facebook, meaning "users could be targeted with ads on Facebook based on the content they engage with on Pray.com — including content modules with titles like 'Better Marriage,' 'Abundant Finance,' and 'Releasing Anger.'"[7] Users called these practices "exploitative," "manipulative," and said they went against the private nature of prayer.[8]

In 2020, the investigative journalists at The Markup found that one-third of websites surveyed contained Facebook's tracking pixel, which allows Facebook to identify users (regardless of whether they are logged into Facebook) and connect those website visits to their Facebook profiles.[9] They scanned hundreds of websites, discovering alarming instances of tracking, including:

- A state agency page on how to report child abuse sending data about its visitors to six ad tech companies;
- WebMD and Everyday Health sending visitor data to dozens of marketing companies;
- The Mayo Clinic using key logging to capture health information individuals typed into web forms for appointments and clinical trials, regardless of whether the individual even submitted the form or not—information which was saved to a folder titled "web forms for marketers/tracking."[10]

---

[3] Irish Council for Civil Liberties, *The Biggest Data Breach ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe* (May 2022), https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf.
[4] *Id.* at 2.
[5] *Id.*
[6] Emily Baker-White, *Nothing Sacred: These Apps Reserve The Right To Sell Your Prayers*, BuzzFeed (Jan. 25, 2022), https://www.buzzfeednews.com/article/emilybakerwhite/apps-selling-your-prayers.
[7] *Id.*
[8] *Id.*
[9] Julia Angwin, *What They Know… Now,* The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/what-they-know-now.
[10] Aaron Sankin & Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.

These trackers collect millions of data points each day that are sold or transferred to data brokers, who then combine them with other personal data sources to build invasive profiles. Often these profiles are used to target people with "personalized" advertisements that stalk them across the web. In other cases these profiles are fed into secret algorithms used to determine the interest rates on mortgages and credit cards, to raise consumers' interest rates, or to deny people jobs, depriving people of opportunities and perpetuating structural inequalities.[11]

And now, after the *Dobbs* decision, this data can be used to target women seeking reproductive care. Shortly after the Supreme Court's decision, a reporter at Vice Motherboard purchased a week's worth of location data showing where people who visited Planned Parenthood clinics came from, how long they stayed, and where they went afterwards – for only $160.[12] This means that even though women in Massachusetts still have the right to obtain an abortion, a resident of a state where is abortion is illegal who travels to Massachusetts for abortion care is at risk of prosecution, partly due to the easy availability of her location data on the open market.

These are just a few of the myriad ways our privacy is invaded every minute of every day. The harms from these privacy violations are real[13] and it is past time to correct the course.

B. Data Privacy in Congress and in the States

Last year in Congress, bipartisan leaders in both the House and Senate proposed the American Data Privacy and Protection Act ("ADPPA"). The bill went through lengthy negotiations between members of Congress of both parties, industry, civil rights groups, and consumer protection and privacy groups. The ADPPA received overwhelming bipartisan support in the House Energy & Commerce Committee, where it was favorably approved on a 53-2 vote, including support from Congresswoman Lori Trahan.

Unfortunately, Congress failed to enact ADPPA due to concerns about state preemption, but state legislators can now take advantage of those negotiations by using the bipartisan consensus language from ADPPA in state legislation. S.25/H.83 is based on that model.

In the states, twelve states have passed their own data privacy laws in recent years, at varying levels of effectiveness: California, Virginia, Connecticut, Colorado, Utah, Iowa, Indiana, Tennessee, Oregon, Montana, Texas, and Delaware.

---

[11] *See Protecting Consumer Privacy in the Age of Big Data*, 116th Cong. (2019), H. Comm. on the Energy & Comm., Subcomm. on Consumer Protection and Comm. (Feb. 26, 2019) (testimony of Brandi Collins-Dexter, Color of Change), https://tinyurl.com/53kr6at6.

[12] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Vice Motherboard (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[13] Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

I want to flag for the Committee that you should be skeptical of industry lobbyists urging you to mimic current state privacy laws. Many of the "privacy" laws enacted in recent years were drafted by and passed with the support of Amazon and industry trade groups, with little to no involvement of consumer and privacy advocates. Reuters found that "[i]n recent years, Amazon.com Inc has killed or undermined privacy protections in more than three dozen bills across 25 states, as the e-commerce giant amassed a lucrative trove of personal data on millions of American consumers."[14] They did this not only by opposing strong privacy bills, but by pushing weak ones. As Reuters reported in 2021:

> In Virginia, the company boosted political donations tenfold over four years before persuading lawmakers this year to pass an industry-friendly privacy bill that Amazon itself drafted.[15]

Industry lobbyists and trade groups are now shopping the Virginia model around in other states in the name of "consistent rules," but really their goal is to get enough states to pass a weak privacy law so it lowers the bar for the standard in a federal privacy bill.[16] Similarly, the "Connecticut model" was significantly weakened by industry after introduction and contains no rulemaking to keep the law current. Originally enacted in 2022, the Connecticut Legislature already had to pass amendments to the law in the summer of 2023. The sponsor of Connecticut's Data Privacy Law, Senate Majority Leader Bob Duff, told the Markup in 2021 as the bill moved through Committee:

> It's an uphill battle because you're fighting a lot of forces on many fronts. They're well funded, they're well heeled, and they just hire a lot of lobbyists to defeat legislation for the simple reason that there's a lot of money in online data.[17]

In the same article, Leader Duff's co-sponsor, Senator James Moroney, said "Our legislative commissioner took the Virginia language and applied Connecticut terminology."[18]

Connecticut's law is essentially an "opt-out" law, meaning that generally entities are allowed to collect and process consumers' personal data so long as they tell you what they're collecting in their privacy policy and you have not yet opted out. Massachusetts can and should do better.

---

[14] Jeffrey Dastin et al., *Amazon wages secret war on Americans' privacy, documents show*, Reuters (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/.
[15] *Id.*
[16] *See* Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, The Markup, (Apr. 15, 2021), https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious.
[17] *Id.*
[18] *Id.*

C. Data Minimization and Strong Enforcement: Two Keys to a Strong Privacy Law

a. Data Minimization

The ADPPA proposed in Congress last session raised the bar and relied on a concept that has long been a pillar of privacy protection in order to force changes to harmful commercial surveillance business practices: data minimization.

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 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. And indeed, providing this service does not require selling, sharing, processing, or strong consumer data for an unrelated secondary purpose. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers. 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.

The ADPPA 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 individual (or pursuant to certain enumerated purposes).[19] For sensitive data (as defined), it must be "*strictly necessary*," and may not be used for targeted advertising. This standard better aligns business practices with what consumers expect.

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. And data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

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. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[20]

[19] H.R. 8152 at §101 (2022), *available at* https://www.congress.gov/bill/117th-congress/house-bill/8152/text.
[20] 5 U.S.C. § 552a (e)(1).

The recently passed update to the California Consumer Privacy Act also includes provisions requiring a form of data minimization.[21] 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 their privacy policy.

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data. The ADPPA set out a model for data minimization that was subject to intense scrutiny by many parties as it moved through Congress. Massachusetts can now take advantage of that bipartisan consensus language.

b. Enforcement

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority or the creation of a state privacy agency is a very important piece to include in a strong privacy law.

But while government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate. Individuals and groups of individuals who use these online services are in a good position to identify privacy issues and bring actions to vindicate their interests. These cases preserve the state's resources, and statutory damages ensure that companies will face real consequences if they violate the law.

The inclusion of a private right of action is the most important tool the Legislature can give to their constituents to protect their privacy. A private right of action would impose enforceable legal obligations on companies. As Northeastern University School of Law Professor Woody Hartzog recently wrote with regard to a private right of action in the Illinois biometric privacy law:

> So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook's share price actually rose 2 percent after the FTC announced its historic $5 billion fine for the social

[21] Cal. Civ. Code § 1798.100(c) (regulations issued pursuant to this section provide two basic avenues for data collection, retention, and use. The first considers whether the data collection is reasonably necessary and proportionate to achieve the original purpose for which the information was collected or processed, provided that this purpose is "consistent with the reasonable expectations of the consumer." To determine the reasonable expectation of the consumer, the regulations set out five factors: (1) The relationship between the consumer and the business, (2) the nature of the personal information that a business seeks to collect or process, (3) the source of the personal information and method for collection or processing, (4) the "specificity, explicitness, prominence, and clarify of disclosures to the consumer," and (5) the degree to which the involvement of contractors, service providers or third parties are apparent to the consumer. The second avenue for data processing is whether the processing is reasonably necessary and proportionate to achieve a secondary purpose that is both disclosed to the individual and compatible with the context in which the personal data was originally collected. *See* 11 Cal. Code Regs tit. 11 § 7002.)

> media company's privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. […] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.[22]

The ACLU's suit against facial recognition company Clearview AI recently settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.[23] Private rights of action are extremely effective in ensuring that the rights in privacy laws are meaningful.

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. In crafting liability provisions in privacy statutes, legislatures have frequently included a liquidated damages provision to avoid protracted disputes over quantifying privacy damages. This is necessary because it is often difficult to assign a specific economic value to the harm caused by a privacy violation.

For example, when federal legislators passed the Cable Communications Policy Act in 1984, they established privacy rights for cable subscribers and created a private right of action for recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher.[24] The Video Privacy Protection Act specifies liquidated damages of $2,500.[25] The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state court against credit reporting agencies, users of credit reports, and furnishers.[26] In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The Drivers Privacy Protection Act similarly includes a private right of action.[27] The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss or up to $500 in damages per violation.[28]

The statutory damages set in privacy laws are not large in an individual case, but they can provide a powerful incentive in large cases and are necessary to ensure that privacy rights will be taken seriously and violations not tolerated. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they

---

[22] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf
[23] Ryan Mac and 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.
[24] 47 USC § 551(f).
[25] 18 USC § 2710(c)(2).
[26] 15 U.S.C. §§ 1681n-1681o.
[27] 18 U.S.C. § 2724.
[28] 47 USC § 227(c)(5).

would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations.

Conclusion

Privacy is a fundamental right, and it is time for business practices to reflect that reality. Self-regulation is clearly not working, and since Congress has still been unable to enact comprehensive privacy protections despite years of discussion on the topic, state legislatures must act. The Massachusetts Legislature has an opportunity this session to provide real privacy protections for the citizens of the Commonwealth.

Thank you for the opportunity to speak today. 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
EPIC Deputy Director