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

December 4, 2024

Chair Mary Cavanaugh
Senate Committee on Finance, Insurance, and Consumer Protection
Room 1200
Binsfeld Office Building
Lansing, MI 48933

Dear Chair Cavanagh and Members of the Committee:

EPIC writes in support of SB 659, the Michigan Personal Data Privacy Act. We commend Senator Bayer for crafting a bill that provides meaningful privacy protections for Michiganders. 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 – Michigan 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]

In my testimony I will discuss why it is so critical that Michigan pass a privacy law this session, the current state of state privacy laws, and how SB 659 would provide Michiganders with privacy protections that residents of other states already enjoy.

A. A Data Privacy Crisis: Surveillance Capitalism Run Wild

The notice-and-choice approach to privacy regulation that has 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

[1] EPIC, *About EPIC*, https://epic.org/about/.
[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.

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.

In 2022, BuzzFeed reported 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.[3] 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.'"[4]

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.[5] They scanned hundreds of websites, discovering alarming instances of tracking, including:

- 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 submitted the form or not—and saving it to a folder titled "web forms for marketers/tracking."[6]

These trackers collect millions of data points each day that are sold to data brokers, who then combine them with other data sources to build invasive profiles. Often these profiles are used to target people with ads that stalk them across the web. In other cases, they are fed into 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.[7]

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,[8] and it is past time to correct the course.

---

[3] 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.
[4] *Id.*
[5] Julia Angwin, *What They Know… Now,* The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/what-they-know-now.
[6] 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.
[7] *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.
[8] 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.

B. The State of State Privacy Law

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 14 laws enacted at the time of publication, nearly half received an F on our scorecard, and none received an A. They provide few meaningful privacy rights for consumers and do little to limit mass data collection and abuse.

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 industry lobbyists 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.

---

[9] Caitriona Fitzgerald, Kara Williams & R.J. Cross, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC and U.S. PIRG (February 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf.

[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/.

This simply requires that businesses only collect what is reasonably necessary for the purposes they disclose to consumers in their privacy policy. This does little to change the status quo, as businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. And even on the off-chance that consumers do read a privacy policy, they have no power to change the terms of these agreements, so their only "choice" is not to use the service. The clearer limits on data collection and use in SB659 are critical because they require companies to better align their data practices with what consumers expect.

Thankfully, states such as Maryland and California have established clearer rules that meaningfully limit data collection to better align with consumers' expectations.

C. SB 959 Provides Strong Privacy Protections by Limiting Data Collection and Establishing Strong Civil Rights Protections

Data Minimization

The excessive data collection and processing that fuel commercial surveillance systems are inconsistent with the expectations of consumers, who reasonably believe that the companies they interact with will safeguard their personal information. These exploitative practices don't have to continue. SB 659 rightfully integrates 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 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 storing 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. Just yesterday, the Federal Trade Commission

SB 659 relies on provisions already enacted in Maryland and California to set a baseline requirement that entities only collect data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the consumer. For sensitive data, the collection and processing of such data must be "*strictly necessary*." 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.

The Federal Trade Commission has recognized that the overcollection and misuse of personal information is a widespread problem that harms millions of consumers every day and has identified that data minimization is the key to addressing these unfair business practices. As it stated in a recent report:

> Data minimization measures should be inherent in any business plan—this makes sense not only from a consumer privacy perspective, but also from a business perspective because it reduces the risk of liability due to potential data exposure. Businesses should collect the data necessary to provide the service the consumer requested, and nothing more.[12]

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

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."[13]

States including Maryland and California have also embraced data minimization principles to protect the privacy of their residents. California regulations establish restrictions on the collection and use of personal information. The California Privacy Protection Agency explained that this "means businesses must limit the collection, use, and retention of your personal information to only those purposes that: (1) a consumer would reasonably expect, or (2) are compatible with the consumer's expectations and disclosed to the consumer, or (3) purposes that the consumer consented to, as long as consent wasn't obtained through dark patterns. For all of these purposes, the business' collection, use, and retention of the consumer's information must be reasonably necessary and proportionate to serve those purposes."[14] Similarly, Maryland's recently passed comprehensive privacy law, the Maryland Online Data Privacy Act, limits companies to collecting only the data that is reasonably necessary for the product or service a consumer requests. Maryland also banned the sale of sensitive data, an important protection also included in SB 659.

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

[12] FTC, *Bringing Dark Patterns to Light* 17–18 (2022), https://www.ftc.gov/reports/bringing-dark-patterns-light.
[13] 5 U.S.C. § 552a (e)(1).
[14] Cal. Priv. Protection Agency, *Frequently Asked Questions*, Question 1, https://cppa.ca.gov/faq.html.

wants to collect data for and discloses in their privacy policy (as is the case in the Connecticut Data Privacy Act). This framework better aligns with consumers expectations when they use a website or app. SB 659 accomplishes this goal and provides Michiganders with comparable protections to Maryland and California. It allows businesses to continue to advertise to potential customers but encourages Big Tech to innovate more privacy-protective forms of advertising.

EPIC does advocate that the rule in Sec. 19(e) be broadened to limit both the collection *and processing* of personal data to purposes that are reasonably necessary to provide or maintain a specific product or service requested by the consumer to whom the data pertains. The biggest impact of adding processing to the rule is that the entities that use our personal information in out-of-context ways, such as data brokers, will be unable to profile consumers in ways unrelated to why a consumer used an online service. The rule will limit the harmful practice of brokering, selling, or sharing personal data. We recommend that the Committee consider broadening that rule, but even a limitation on collection is a step in the right direction.

Civil Rights Protections

Importantly, SB 659 also 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 identity, or disability. Most state privacy laws attempt to prevent discrimination online by prohibiting the processing of personal data in ways that violate state and federal anti-discrimination laws. However, existing civil rights laws contain significant gaps in coverage and often do not apply to disparate impact.[15] These issues make existing laws insufficient to ensure all people are protected from discrimination online. The language in Sec. 21(1)(d) better protects individuals from discrimination online.

D. Enforcement is Critical

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority, with adequate resources, 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 the best 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. This is why privacy laws would ideally include a

[15] *See* 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 David Brody, Lawyer's Comm. for Civil Rights Under Law), https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-BrodyD-20220614.pdf.

private right of action,[16] just as the Michigan Consumer Protection Act allows consumers to protect their rights in Court. However, I acknowledge that this provision was cut in the interest of compromise, and EPIC supports SB 659 regardless, as it includes important privacy protections. We urge the Legislature to appropriate adequate resources to ensure effective enforcement of the law.

* * *

Privacy is a fundamental right, and it is time for business practices to reflect that reality. Big Tech does not need to track and monetize our every click online in order for businesses to advertise effectively. Better models are possible. By passing SB 659, the Michigan Legislature can encourage privacy-protective innovation and protect Michiganders online.

Thank you for the opportunity to speak today. EPIC is happy to be a resource to the Committee on these issues.

Sincerely,

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Deputy Director

/s/ *Kara Williams*
Kara Williams
EPIC Law Fellow

[16] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf