

February 13, 2024

The Honorable Pamela Beidle
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chair Beidle and Members of the Committee:

EPIC writes in support of SB 541, the Maryland Online Data Privacy Act of 2024. We commend the sponsors for crafting a bill that provides meaningful privacy protections for Marylanders. 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 – Maryland 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 Maryland pass a privacy law, the current state of state privacy laws, and how SB 541 rightfully includes stronger protections than existing state laws.

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, 14 states have passed comprehensive privacy laws. EPIC, in partnership with U.S. PIRG, released a report this month grading these state laws.⁹ Of the 14 laws, nearly half received an F on our scorecard, and none received an A. Most provide few meaningful privacy rights for consumers and do little to limit mass data collection and abuse.

With the exception of California, all 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 the Virginia and Connecticut models provide very few protections for consumers. These models 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 SB 541 are critical because they require companies to better align their data practices with what consumers expect.

C. SB 541 Provides Stronger 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 541 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.

SB 541 sets 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 individual. 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

The recently passed update to the California Consumer Privacy Act also includes provisions requiring a form of data minimization.¹⁴ 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.”¹⁵

The EU’s General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is “[a]dequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.”¹⁶ This is layered on top of restrictions on the legal bases under which companies can process personal data. The GDPR was groundbreaking in establishing broad data protection rights online, but Maryland should consider adopting a more concrete set of regulations now that difficulties with interpreting and enforcing

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. Civ. Code § 1798.100(c).

¹⁵ Cal. Priv. Protection Agency, *Frequently Asked Questions*, Question 1, <https://cppa.ca.gov/faq.html>.

¹⁶ Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

GDPR have been revealed. Luckily, a significant amount of the compliance work businesses are already doing to comply with GDPR would be applicable to the data minimization rules included in SB 541.

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 (as is the case in the Connecticut Data Privacy Act). This stricter framework better aligns with consumers expectations when they use a website or app. SB 541 accomplishes this goal.

EPIC does advocate that the rule in § 14-4607(B)(1)(I) 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 information unrelated to the primary collection purpose and accordingly limit harmful surveillance advertising. 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 541 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 do not apply to disparate impact.¹⁷ These issues make existing laws insufficient to ensure all people are protected from discrimination online. The language in § 14-4607(A)(7) 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 or the creation of a state privacy agency is a very important piece to include in a strong privacy law.

¹⁷ 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>.

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.

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 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.¹⁸

The ACLU's suit against facial recognition company Clearview AI settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.¹⁹ Private rights of action are extremely effective in ensuring that the rights in privacy laws are meaningful.

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 would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations. We would encourage the Committee to strike the text in § 14-4613(2) that states "except for § 13-408 of this Article," which would allow Marylanders to use their existing right to bring suit under the Unfair, Abusive, or Deceptive Trade Practices Act for violations of this bill.

¹⁸ Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>

¹⁹ 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>.

E. Additional Proposed Amendments

EPIC agrees with Consumer Reports' recommended amendments to broaden opt-out rights to include all data sharing and ensure that targeted advertising is adequately covered, eliminate the GLBA carveout, narrow the loyalty program exemption, remove ambiguities around universal opt-out requirements, and amend the prohibitions on default opt-outs.

F. 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 Maryland General Assembly has an opportunity this session to provide real privacy protections for Marylanders.

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