

HB567_EPIC_Davisson_FAV.pdf

Uploaded by: Caitriona Fitzgerald

Position: FAV

February 9, 2024

The Honorable C.T. Wilson
House Economic Matters Committee
Room 231
House Office Building
Annapolis, MD 21401

Dear Chair Wilson and Members of the Committee:

EPIC writes in support of HB 567, 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 HB 567 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 last week grading these state laws.⁹ Of the 14 laws, 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.

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 HB 567 are critical because they require companies to better align their data practices with what consumers expect.

C. HB 567 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. HB 567 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.

HB 567 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 GDPR have been revealed. Luckily, a significant amount of the compliance work businesses are

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).

already doing to comply with GDPR would be applicable to the data minimization rules included in HB 567.

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. HB 567 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, HB 567 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>.

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/ John Davisson

John Davisson
EPIC Senior Counsel

/s/ Kara Williams

Kara Williams
EPIC Law Fellow

von Lehmen__Staff_Maryland Cybersecurity Council__

Uploaded by: Greg Lehmen

Position: FAV

TESTIMONY PRESENTED TO THE
HOUSE COMMITTEE ON ECONOMIC MATTERS

HB 567 (MARYLAND ONLINE DATA PRIVACY ACT OF 2024)

DR. GREG VON LEHMEN
STAFF, MARYLAND CYBERSECURITY COUNCIL

POSITION: SUPPORT

February 13, 2024

Mr. Chairman, Vice Chairman, and members of the committee, thank you for the opportunity to testify. I am Dr. Greg von Lehmen, staff to the Maryland Cybersecurity Council, a statutory body chaired by Attorney General Brown. I am here to support HB 567 as consistent with Council recommendations.

I urge favorable consideration for three reasons.

First, when it comes to their sensitive data, consumers are vulnerable, and they suffer the consequences. As this committee knows, data about every aspect of our lives is collected at scale, attached to our personal identities, bought, sold, and diffused across many companies. Much of this activity is without our informed consent or knowledge. A published report by the Maryland Attorney General’s Office indicates that in FY 2022 there were almost a million reported Maryland residents whose personal identifying data was impacted by breaches.¹ When this happens, the costs are sometimes at the low end, like waiting for a new credit card. But there are high end costs too: ID theft, financial account takeovers, extortion, and on and on.

Second, this policy idea—codifying basic consumer privacy rights—has been kicked around for a while. There are now 13 states that have comprehensive consumer privacy rights legislation.² This is a bipartisan effort. California was the first. But in

¹ Office of the Attorney General Identity Theft Program. (2023). *Data Breaches FY 2022 Snapshot*. <https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/data-breaches-fy-2020-snapshot-pdf.pdf> Note: There were more than 1,300 reported breaches impacting Maryland residents in FY 2022. The number of residents affected likely overstates the number of unique residents impacted. This is because breaches are reported independently by each entity, making it probable that some residents were affected by more than one breach. This is particularly true when viewed longitudinally. The cumulative number of separately reported Maryland residents affected for the four snapshot reports to date comes to more than 6.2 million. The four reports are for 2016, 2018, 2020, and 2022.

² *US State Privacy Legislation Tracker*. (2024, February 2). IAPP. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

the mix is Texas, Tennessee, Virginia, Delaware, and a number of other red and blue states. There is some variation among their statutes reflecting different equilibria of interests. An example is whether to include the right of private action. But at their core, these statutes are very similar. House Bill 567 is informed by this experience. It is a good bill for Maryland.

Finally, the question is: if not now, when? The 13 states that I mentioned represent 35% of the American population. In my count, this is the fourth session of the General Assembly that a comprehensive consumer privacy bill has been proposed.³ Given the risks, Maryland residents deserve to be allowed a greater role in reducing their exposure to breaches and the consequences. House Bill 567 would do this. The time is now.

I urge favorable consideration of the bill.

Thank you.

³ The others are HB 807/SB 698 (2023), SB 11 (2022), and SB 930 (2021).

HB0567_Common Sense Media_Grosshans_FAV.pdf

Uploaded by: Holly Grosshans

Position: FAV



Written Testimony of Holly Grosshans

Senior Counsel, Tech Policy; Common Sense Media

Before the Maryland House Economic Matters Committee

regarding

“Maryland Online Data Privacy Act of 2024”

Bill No: HB0567

Position: Favorable

February 13, 2024

My name is Holly Grosshans. I am the Senior Counsel for tech policy at Common Sense Media, the nation’s largest organization dedicated to ensuring that children and families thrive—and remain safe—in the rapidly-changing digital age. In Maryland alone, more than 2,000 teachers have registered to teach Common Sense Media’s digital citizenship and literacy materials to their students in nearly 800 Common Sense recognized schools. But perhaps most importantly, I am the mother of two elementary school-age children and I care deeply about the privacy and well-being of my kids, and the millions of children like them, who are depending on this committee and this legislature to establish desperately-needed protections for their online safety, privacy, and overall well-being.

My testimony will focus on the consumer risks associated with unregulated online data privacy, the potential harms of personal data processing and targeted advertising to kids and teens, and how the Maryland Online Data Privacy Act will be an effective tool to protect Marylanders’ online privacy.

I. Introduction: Internet privacy is a pressing issue; states are beginning to regulate

Common Sense Media strongly supports the proposed Maryland Online Data Privacy Act of 2024 (HB0567). Recent research makes it clear that concerns about internet privacy are growing—as many as 71% of Americans are worried about how companies are using their personal data, while 89% are somewhat or very concerned about social media companies collecting data about kids.¹ As of this writing, 13 states² have passed comprehensive data privacy bills while at least 20 more³ have proposed bills that would particularly strengthen kids’

¹ Colleen McClain et al., *How Americans View Data Privacy*, Pew Research (Oct. 18, 2023).

² F. Paul Pittman, *US Data Privacy Guide*, White & Case (Feb. 5, 2024).

³ Kirk J. Nahra, *State Child Privacy Law Update*, WilmerHale (Feb. 28, 2023).

data privacy protections. Common Sense believes that Maryland’s kids and families also deserve strong data privacy protections and so supports the Maryland Online Data Privacy Act.

Among the provisions of this bill that we particularly support, this bill offers strong protections against the sale of user data and targeted advertising, will prevent companies from pretending they don’t have kids on their sites, and will protect teenagers’ privacy and create additional benefits for safety. While we recommend that the bill could be further strengthened by clarifying the ban on targeted advertising to children under 13 by changing 14-4607(A)(5) to remove “at least 13 years old and” so that it applies to all consumers under 18, Common Sense Media offers our unambiguous support for your bill.

II. Background: Marylanders, and especially kids, suffer from a lack of data privacy

There is no comprehensive federal data privacy law, and the only federal children’s data privacy law is 25 years old. Maryland does not have its own online data privacy law for adults or for minors. This leaves Marylanders in significant need of this legislation.

The vast majority of Americans believe that they have little or no control over their personal data.⁴ Many report that companies are too opaque about what they do with user data for individuals to even have a say, and the majority of surveyed Americans who report taking their data privacy seriously think that even their making good privacy decisions would have little or no impact on whether companies actually collect their data. Recent consumer research suggests Americans are troubled by this state of affairs—74% of whom rate their data privacy as highly important to them.⁵ But there are also practical concerns: lack of robust data privacy increases the risk of abuse, fraud, and identity theft, and may dissuade users from visiting certain sites or taking advantage of certain internet resources.

Data privacy concerns are particularly acute for kids. Recent research suggests that kids’ internet usage is at an all-time high.⁶ Teens are spending an average of 4.5 hours per day on their phones, with about a quarter of them spending as much as 5 to 8 hours in front of their screens every day. Nearly half of teens report that they feel addicted to their phones.⁷ Teens connect with each other through these platforms at higher rates than any other group, report that these platforms form a larger part of their social life than any other group, and have outsized levels of difficulty stopping technology use once they’ve started.⁸ And kids and teens must use technology for educational purposes, meaning that K–12 students in Maryland and elsewhere don’t have the option to avoid tech and the data privacy concerns it raises. As a result, teens and kids are being surveilled by platforms and having their behavior tracked, packaged, and sold to third-parties at an alarming rate.

⁴ McClain et al., *supra*.

⁵ *What Is Data Privacy & Why Is It Important?*, Dashlane (Apr. 18, 2023).

⁶ Jenny S. Radesky et al., *Constant Companion: A Week in the Life of a Young Person’s Smartphone Use*, Common Sense (2023).

⁷ Kim Chronister, *Teen Phone Addiction*, Key Healthcare (May 4, 2022).

⁸ *Id.*

Worse still, teens are more susceptible than older users to targeted ads and to data mining. Teens are far more likely to overshare information about themselves online thanks in part to their unique social relationship with media platforms, and in part to the underdevelopment of the parts of their brain responsible for dealing with judgment and long-term consequences.⁹ Research suggests teens are less able to identify targeted advertising and, in many cases, don't fully understand that features like algorithmic personalization both require large amounts of their data to function properly and make it harder for teens to stop or decrease screen time.¹⁰

Data privacy regulation is sorely needed. As Americans seek greater protection for their online data and wish for greater control over how their data is used, trust in online companies and their ability to self-regulate is at an all-time low. Decisive regulatory action is the only option and Common Sense supports the Online Data Privacy Act as exactly this kind of action.

III. Common Sense Media Supports the Maryland Online Data Privacy Act of 2024

The Online Data Privacy Act is essential legislation to protect online privacy for kids and their families. We point to three provisions that, as we understand the legislation, provide robust protections.

Strong Protections Against Sale of User Data and Targeted Advertising — Section 14-4607(A) broadly prohibits and limits the collection of personal data “for the sole purpose of content personalization or marketing” without consent from the user. It further bans outright the sale of “sensitive data” which includes data of children under 13. Common Sense believes that these provisions are essential to protecting privacy online. They protect children, teens, and everyone from having their behavior tracked, processed, and monetized. The provisions enable adult users to have control over how their data is used by requiring their consent to process their data. And they allow consumers autonomy in what they choose to reveal to companies; permitting users to make case-by-case judgment calls about the value of the personalization service relative to their data privacy.

The bill also safeguards teens. It only permits sale of teen data with user consent, and creates a blanket ban on the processing for purposes of targeted advertising of teens' (aged 13-18) user data. That there is no consent provision for teens to opt-in to processing and sale of their data is an important safeguard for teens. Otherwise, teens who are primed to engage in risky behavior for short-term rewards may be tempted to give up privacy in order to maximize the personalization of their user experience but, as mentioned, may not fully be able to grasp the consequences of doing so.

As noted above, while we support this section of the bill we believe it could be strengthened. The bill could be clarified with respect to targeted advertising and children under 13; it is not clear that targeted advertising is outright prohibited with respect to such users as it is with

⁹ Devorah Heitner, *Here's why your teen overshares online, and why that could be good*, Washington Post (Sept. 15, 2023).

¹⁰ Samuel Levine, *Protecting Kids from Stealth Advertising in Digital Media*, FTC (Sept. 2023).

teenagers. Specifically, we recommend changing 14-4607(A)(5) to remove “at least 13 years old and” so that it applies to all consumers under 18. This would maximize the Bills’ protection of the most vulnerable users.

Prevent Companies From Pretending They Don’t Have Kids On their Sites — Throughout the bill, heightened protections apply when platforms “know or should have known” that a user was either a child (under 13) or a teen (13-18). Common Sense emphasizes its support for this ‘knew or should have known’ language throughout the bill. The ‘should have known’ portion powerfully holds companies to account by preventing them from pleading ignorance of violations. Without such language, platforms are incentivized to purposefully turn a blind-eye to user age so as to claim they ‘didn’t know’ that their data collection activity swept in children or teens. The ‘should have known’ language creates a statutory safeguard against that ignorance defense by holding companies to what they could reasonably know, not just what they choose to note in their records.

Protect Teenagers’ Privacy and Create Knock-on Benefits for Safety — The bill gives heightened protections not just to children 12 and under, but also to teenagers. This fills an important gap in the federal Children’s Online Privacy Protection Act (COPPA), which currently applies only to children under 13 years of age. In particular, several aspects of the Online Data Privacy Act balance the interests of protecting teens’ data privacy while also encouraging them to develop autonomy concerning their own user data.

As referenced above, teens in particular are spending more and more time on their phones and report skyrocketing rates of digital addiction. This state of affairs is no idle coincidence; social media companies’ business model—based on targeted advertising and data collection—encourages the production of addictive design features such as endless scrolling pages and notification nudging. Common Sense additionally supports this bill to help change those incentives. A general prohibition on the use and sale of consumer data, and children’s data in particular, would curtail the incentive to create features that encourage users to spend more time on their phones.

IV. Conclusion

Marylanders’ online data privacy is currently underprotected and susceptible to use or abuse by companies and others. This presents a particular threat for Maryland’s kids and teens, who are the most vulnerable with respect to data breaches and targeted advertising. The Maryland Online Data Privacy Act creates a stalwart framework for protecting adults’ and childrens’ data privacy, while balancing consumers’ interests in personalized user experiences and parents’ interests in their kids’ online development. Common Sense applauds the bill sponsors for bringing forward this important legislation at a critical time for children and teens online and we urge the committee and the House of Delegates to approve this important measure.

HB 567_MNADV_FAV.pdf

Uploaded by: Melanie Shapiro

Position: FAV



BILL NO: House Bill 567
TITLE: Maryland Online Data Privacy Act of 2024
COMMITTEE: Economic Matters
HEARING DATE: February 13, 2024
POSITION: **SUPPORT**

The Maryland Network Against Domestic Violence (MNADV) is the state domestic violence coalition that brings together victim service providers, allied professionals, and concerned individuals for the common purpose of reducing intimate partner and family violence and its harmful effects on our citizens. **MNADV urges the House Economic Matters Committee to issue a favorable report on HB 567.**

House Bill 567 is an important example of policy and laws that are needed to keep up with rapidly evolving technology. This bill provides protections to consumer information collected online. Most people do not understand the laws governing information shared online and may think that information is in fact protected when it is not protected. For victims of domestic violence, privacy is of the utmost importance and can be critical for their safety.

MNADV supports this legislation because it would allow Maryland to protect the privacy of consumer information. Online vendors would be restricted, except in limited circumstances, from sharing or redisclosing sensitive consumer data without the express consent of the consumer. The legislation also provides additional protection for consumers seeking reproductive and behavioral health services by prohibiting the use of geofencing data to track those consumers.

For the above stated reasons, the **Maryland Network Against Domestic Violence urges a favorable report on HB 567.**

Maryland PIRG HB0567 Testimony.pdf

Uploaded by: RJ Cross

Position: FAV

HB0567: Maryland Online Data Privacy Act of 2024

February 9, 2024

R.J. Cross, Maryland PIRG

Favorable

Maryland PIRG is a state based, small donor funded public interest advocacy organization with grassroots members across the state. We work to find common ground around common sense solutions that will help ensure a healthier, safer, more secure future.

When we use our favorite apps, websites and smart devices, the companies on the other side are often gathering information about us. Sometimes it's data that makes sense; Amazon needs your shipping address to send you a package. Often, however, the data companies collect [far exceeds](#) what's necessary for delivering the service consumer's are expecting to get, and they often use it for irrelevant purposes. These practices are incredibly common - and dangerous for consumers' personal security.

The more data that companies collect about you, and the more companies they sell it to or share it with, the more likely it is your information will be exposed in a breach or a hack. This makes it more likely your information will end up in the wrong hands like with identity thieves or scammers.

The Online Data Privacy Act of 2024, as currently drafted, will protect Maryland residents against threats to their personal security. It is imperative that this legislation does not get watered down.

The heart of the Online Data Privacy Act that will most benefit consumers is its data minimization provisions. These are common sense protections that will make sense to everyone. Namely:

- Limiting the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer. This would solve the problem of, for example, the fast food chain Tim Hortons allegedly using its [mobile ordering app](#) to harvest the location data of users 24/7, even when the app was closed. Tim Hortons doesn't need to collect my location every day in order for me to place an order at the nearest restaurant once.
- Prohibiting companies from processing, sharing or selling sensitive data - such as health, religious beliefs, or geolocation - in ways that have nothing to do with delivering the service a consumer is expecting to get. This would stop educational apps used by schools, for example, from [selling schoolchildren's data](#) to data brokers and advertising companies. This protection is crucial for minors, but it makes sense for everyone.

The Maryland Online Data Privacy Act of 2024 should strengthen this latter provision to prohibit the secondary uses of **all** consumer data, not just sensitive information. This would be a clear cut solution that is intuitive to people: only gather my data when it's necessary, and use it for what I'm expecting. It makes sense, and it's the single best thing we can do to protect people's personal security.

A word of warning: Across the country, states are trying to pass data privacy laws that protect people. However, many of them end up facing [massive efforts](#) by [corporate trade](#) groups and [Big Tech](#) lobbyists [that have](#) developed [a playbook](#) used nearly everywhere. Many of the bills have become so industry-friendly, they do virtually nothing for the people they're supposed to protect.

Maryland has the opportunity to take a different path.

We respectfully request a favorable report.

02.09 - HB 567 - Maryland Online Data Privacy Act

Uploaded by: Robin McKinney

Position: FAV



HB 567 - Maryland Online Data Privacy Act of 2024

Economic Matters Committee

February 13, 2024

SUPPORT

Chair Wilson, Vice-Chair Crosby and members of the committee, thank you for the opportunity to submit testimony in support of House Bill 567. This bill will increase data rights protections for Marylanders.

The CASH Campaign of Maryland promotes economic advancement for low-to-moderate income individuals and families in Baltimore and across Maryland. CASH accomplishes its mission through operating a portfolio of direct service programs, building organizational and field capacity, and leading policy and advocacy initiatives to strengthen family economic stability. CASH and its partners across the state achieve this by providing free tax preparation services through the IRS program 'VITA', offering free financial education and coaching, and engaging in policy research and advocacy. **Almost 4,000 of CASH's tax preparation clients earn less than \$10,000 annually. More than half earn less than \$20,000.**

The ability for consumers to regulate how businesses collect and store their personal data and use their personal data is a right that all Marylanders should have. Consumer data is not only an issue of privacy but also an issue of security. Data breaches are disturbingly common incidents that impact consumers across Maryland. **In 2023, Maryland had over 500 instances of data breaches.**¹ There are already several large data brokers who collect volumes of information on consumers and sell the information for a fee.

HB 567 includes provisions on protecting an individual's private data, including biometric data. Biometric data consists of a person's unique physical characteristics like fingerprints, palmprints, voiceprints, facial, or retinal measurements. It is increasingly becoming more popular to use biometrics in law enforcement, healthcare, and commercial industries. As the use of this data becomes more popular, the risk to consumers of having their personal biometric data breached is also increased. Unfortunately, this can result in consumers becoming victims of identity fraud.

Low-income consumers are at even greater risk of harmful data breaches, as they are more likely to use older devices that aren't equipped for newer security updates.² HB 567 would establish greater data privacy protections for all Marylanders, which would be especially beneficial to low-income residents. Consumers must be very careful about who has access to their personal information. CASH supports legislation that will ensure Maryland remains a national leader in consumer protection policy.

Thus, we encourage you to return a favorable report for HB 567.

¹ <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx>

² <https://carnegieendowment.org/2023/03/13/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions-pub-89254#>

2024 ACNM HB 567 House Side.pdf

Uploaded by: Robyn Elliott

Position: FAV



Committee: House Economic Committee

Bill Number: HB 567 – Maryland Online Data Privacy Act of 2024

Hearing Date: February 13, 2024

Position: Support

The Maryland Affiliate of the American College of Nurse Midwives (ACNM) strongly supports *House Bill 567 – Maryland Online Data Privacy Act of 2024*. The bill would safeguard personal information collected online and provide consumers more control over the use and redisclosure of the data.

ACNM supports this legislation because not all health data is protected by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA only protects the information collected by providers in electronic health records. State confidentiality laws extend similar protections to any paper health records. However, HIPAA and state laws do *not* protect health data that consumers provide to entities who are not connected to health care providers. For example, there are a proliferation of apps that help consumers track their menstrual cycles, health indicators such as heart rate, and sleep patterns.

This legislation is essential to providing safeguards, so that consumers may determine how their personal data is used and shared. It also provides essential protections to consumers seeking reproductive or behavioral health, as it prohibits the use of geofencing data that could later be used to penalize or intimidate consumers.

We urge a favorable report. If we can provide any further information, please contact Robyn Elliott at relliott@policypartners.net.

2024 LCPCM HB 567 House Side.pdf

Uploaded by: Robyn Elliott

Position: FAV



Committee: House Economic Committee

Bill Number: HB 567 – Maryland Online Data Privacy Act of 2024

Hearing Date: February 13, 2024

Position: Support

The Licensed Clinical Professional Counselors of Maryland supports *House Bill 567 – Maryland Online Data Privacy Act of 2024*. The bill provides protection of consumer information collected online. LCPCM supports this bill because there are a growing number of online vendors, including apps, that collect mental health information that is not protected by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA only protects the information in health provider records. When there is a platform offered by entity not affiliated with a health care provider, there are few, if any, privacy protections in state or federal law. There are a growing number of platforms that advertise being able to help consumers improve their mental health and wellbeing. Consumers may be providing sensitive person information without understanding that there are virtually no legal barriers to the platform selling or redisclosing that data. The sharing of this data may be detrimental to consumers' health. Therefore, LCPCM supports this legislation which will begin to provide some safeguards to this data. We ask for a favorable report. If we can provide any further information, please contact Robyn Elliott at relliott@policypartners.net.

HIPAA only protections the information collected by providers in electronic health records. State confidentiality laws extend similar protections to any paper health records. However, HIPAA and state laws do *not* protect health data that consumers provide to entities who are not connected to health care providers. For example, there are a proliferation of apps that help consumers track their menstrual cycles, health indicators such as heart rate, and sleep patterns.

This legislation is essential to providing safeguards, so that consumers may disclose how their personal data is used and shared. It also provides essential protections to consumers seeking

reproductive or behavioral health, as it prohibits the use of geofencing data that could later be used to penalize or intimidate consumers.

We urge a favorable report. If we can provide any further information, please contact Robyn Elliott at relliott@policypartners.net.

2024 WLCM HB 567 House Side.pdf

Uploaded by: Robyn Elliott

Position: FAV

Committee:	House Economic Committee
Bill Number:	HB 567 – Maryland Online Data Privacy Act of 2024
Hearing Date:	February 13, 2024
Position:	Support

The Women's Law Center of Maryland (WLC) strongly supports *House Bill 567 – Maryland Online Data Privacy Act of 2024*. The bill provides privacy protections for consumer information collected online. The bill generally prohibits the disclosure of consumer information collected by online vendors, unless the disclosure is essential to provide the service offered by the vendor.

In recent years, there has been a proliferation of online platforms, including apps, that collect health and other sensitive personal information. Consumers may have an expectation of privacy, as the public generally thinks that health information is protected by the Health Insurance Portability and Accountability Act (HIPAA). However, many online platforms are not subject to HIPAA, as HIPAA only protects the electronic health records of health care providers and related business entities, such as health insurers.

Online platforms generally may set their own privacy policies. These policies, even when disclosed, may be challenging for consumers to navigate and fully understand their implications. WLC believes that the lack of privacy standards may compromise consumers' safety and wellbeing; and in some cases, redisclosure of information may create legal peril for consumers.

There has been an increase in the popularity and use of health and wellbeing apps. Consumers can use apps to track their menstrual periods, sleep cycles, and mental health. However, most of these apps are not subject to HIPAA, leaving consumers at the mercy of the privacy policies set by the vendors. This problem has gained more attention in the wake of the *Dobbs* decision, as information from period tracking apps and geofencing data could be used by prosecute people leaving states that ban abortion to seek care elsewhere. The Federal Trade Commission has fined some period tracking apps for redisclosure of health information.^{i ii} However, an individual state has no authority to protect its own residents unless the state adopts specific statutory protections.

WLC supports this legislation because it would allow Maryland to protect the privacy of consumer information. Online vendors would be restricted, except in limited circumstances, from sharing or redisclosing sensitive consumer data without the express consent of the consumer. The legislation also provides additional protection for consumers seeking reproductive and behavioral health services by prohibiting the use of geofencing data to track those consumers.

We ask for a favorable report. If there is additional information that we can provide, please contact Robyn Elliott at relliott@policypartners.net.

The Women’s Law Center of Maryland is a private, non-profit, legal services organization that serves as a leading voice for justice and fairness for women. It advocates for the rights of women through legal assistance to individuals and strategic initiatives to achieve systemic change, working to ensure physical safety, economic security, and bodily autonomy for women in Maryland.

ⁱ <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

ⁱⁱ <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>

HB 567 - Delegate Love Privacy Written (1).pdf

Uploaded by: Sara Love

Position: FAV



THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

HB 567 – Maryland Online Data Privacy Act of 2024

Chair Wilson, Vice Chair Crosby, Members of Economic Matters –

Right now, in Maryland, we have no comprehensive online privacy law. And this is a problem. Companies are collecting and selling personal and sensitive data about our lives without our knowledge or consent. When you download that ‘free’ app, it isn’t really free. We get that app in exchange for our personal data that it collects, usually unbeknownst to us. We are both the consumer and the product. At least 70% of mobile apps share data with third parties, and one study found that 15% of those reviewed were connected to five or more trackers. This data could be our mental health data.¹ It could be our reproductive data. It could be our location data. That data is collected, aggregated, and sold. All without our knowledge or consent.

HB 567 includes:

- Data minimization – making sure companies are only collecting and processing the data needed for the transaction at hand.
- Data protection – ensuring companies keep the data they do collect safe
- Consumer control over personal data – giving consumers the right to know what is collected and who it is shared with, along with the right to correct the data, delete the data, and opt out of targeted ads, sale of data and profiling.
- Extra layers of protection for sensitive data. Sensitive data includes:
 - Biometrics
 - Geolocation
 - Reproductive, mental health, and gender affirming care
 - Racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status
 - Personal data that a controller knows or has reason to know is that of a child

Because this is a large bill, I am submitting with this testimony an overview of the bill for the Committee’s convenience.

I respectfully request a favorable report on HB 567.

¹ “One company advertised the names and home addresses of people with depression, anxiety, post-traumatic stress or bipolar disorder. Another sold a database featuring thousands of aggregated mental health records, starting at \$275 per 1,000 ‘ailment contacts.’ For years, data brokers have operated in a controversial corner of the internet economy, collecting and reselling Americans’ personal information for government or commercial use, such as targeted ads. But the pandemic-era rise of telehealth and therapy apps has fueled an even more contentious product line: Americans’ mental health data. And the sale of it is perfectly legal in the United States, even without the person’s knowledge or consent.” [Washington Post](#) 2/13/23

HB 567 Attachment Delegate Love MD OPA 2024 Overvi

Uploaded by: Sara Love

Position: FAV

HB 567 Overview

Application

Bill covers personal data, defined as “data that can be reasonably linked to an identified or identifiable consumer.”

- It also addresses sensitive data (biometrics, child data, consumer health data, data revealing race, gender identity, etc.)

The bill applies to a person that:

- Conducts business in the state; or
- Produces services or products that are targeted to residents of the state; and
 - Controlled or processed the personal data of at least 35,000 consumers (excluding solely for a payment transaction); or
 - Controlled or processed the persona data of at least 10,000 consumers and derived 20% of gross revenue from the sale of personal data.

Bill exempts several entities, as well as a number of specific types of data.

Consumer Rights

Bill grants consumers certain rights:

1. Right to confirm a controller is processing their personal data
2. Access that data
3. Correct the data
4. Require the controller to delete the data
5. Obtain a copy of the data
6. Obtain a list of categories of 3d parties to whom the controller has disclosed the personal data
7. Opt-out of the processing for:
 - a. Targeted advertising
 - b. The sale of personal data
 - c. Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.
8. Designate an authorized agent to opt-out of the processing in #7.

Exercising those rights

A controller:

1. Must establish a secure way for consumers to exercise their rights.
2. Shall respond to the request w/in 45 days. Can extend
3. Must notify the consumer w/in 15 days that they complied.
4. May decline. If they do, they shall inform the consumer and provide an appeal process.

Controllers

Controllers are the one who “determines the purpose and means of processing personal data.” The bill puts guardrails on controllers’ activities: data minimization, restrictions on collection and use of sensitive data, protecting data confidentiality, limits on the use of personal data

Details:

A. If a controller processes data

- They shall protect the confidentiality and security of the data
- Reduce risks of harm to the consumers relating to the collection, use or retention of the data
- Process the data to the extent it is reasonably necessary and proportionate to the purposes in the bill & is adequate, relevant & limited to what is necessary.

B. Responsibilities

A controller may not:

1. Collect personal data for the sole purpose of content personalization or marketing, unless they have the consumer’s consent.
2. Collect, process, or share sensitive data concerning a consumer (except where strictly necessary to provide or maintain a specific product or service requested by the consumer, and only with the consumer’s consent).
3. Sell sensitive data
4. Process personal data in violation of anti-discrimination laws
5. Process personal data for purposes of targeted advertising or sell the consumer’s personal data, if controller knows or has reason to know the consumer is between 13-18.
6. Discriminate against a consumer for exercising their rights under this title.
7. Collect, process, or transfer personal data in a way that discriminates or makes unavailable the equal enjoyment of goods (Civil Rights lang. from bi-partisan federal bill)
8. Process personal data for a purpose that is not reasonably necessary to or compatible with the disclosed purposes for which the data is processed (unless consumer consents).

A controller shall:

1. Limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a service requested by a consumer.
2. Establish reasonable security practices to protect the data
3. Provide a reasonable mechanism for a consumer to revoke consent.
4. Stop processing data within 15 days of a consent revocation.
5. Provide a clear privacy notice that includes:
 - a. Categories of personal data processed, including sensitive data
 - b. Purpose for processing the data
 - c. How a consumer may exercise their rights
 - d. Categories of 3d parties with which the controller shares data, with sufficient detail so the consumer understands what they are and how they may process the data
 - e. Categories of data shared with 3d parties
 - f. Active email address to contact the controller

C. Other

Nothing in this bill:

1. Requires a controller to provide a product or service that requires data they don't collect
2. Prohibits a controller from offering different levels of service if the offering is in connection with a loyalty program.

Processors

A processor is “a person that processes personal data on behalf of a controller.”

Processors & controllers must enter a contract that includes:

- Instructions for processing the data
- Nature and purpose of processing
- Type of data subject to processing
- Duration of processing
- Duty of confidentiality
- Issues of retention/return/deletion of data

Processors:

1. Help controllers comply with the Act
2. May engage subcontractors with controller's consent

Controller v. processor? A processor

- is limited in processing of specific data per controller's instruction
- can be deemed a controller if they
 - fail to adhere to instructions
 - determine purposes and means of processing data

“Processing Activities that Present a Heightened Risk of Harm” & Data Assessments

This section sets out requirements for processing activities that ‘present a heightened risk of harm.’ Those are defined as:

1. the processing of personal data for targeted advertising
2. the sale of personal data
3. the processing of sensitive data
4. processing of personal data for the purposes of profiling, which risks
 - a. unfair, abusive or deceptive treatment
 - b. having an unlawful disparate impact
 - c. financial, physical, or reputational injury
 - d. physical or other intrusion into private affairs
 - e. other substantial injury

For each activity in #4, a controller must conduct a data protection assessment. This assessment shall:

1. identify and weigh the benefits to the controller, the consumer, & the public against the risks to the consumer (as mitigated by any safeguards the controller employs) and the necessity of processing in relation to the stated purpose of the processing.

2. Include various factors, such as
 - a. The use of de-identified data
 - b. Consumer expectations
 - c. Context
 - d. Relationship between controller and consumer
3. Be made available to the OAG Div. of Consumer Protection where relevant to an investigation.

Misc.

These pages lay out a series of things the tech industry negotiated for in other states' bills. For example, they do not have to:

- Maintain data in an identifiable form
- Collect any data to authenticate a consumer request
- Comply with a request if they can't associate the request with the data

The bill doesn't restrict controllers or processors from a litany of actions, including complying with laws, subpoenas, cooperate with law enforcement, establish a defense to a claim, provide a product specifically requested, perform under a contract, protect life or physical safety, prevent/detect fraud, assist another with obligations under this bill, effectuate a recall, identify & repair technical errors, perform internal operations.

Enforcement

By the Office of the Attorney General

No Private Right of Action

Violation is an unfair, abusive or deceptive trade practice

Other remedies at law available to consumers

HB567 Written Testimony .pdf

Uploaded by: Zoe Gallagher

Position: FAV



HB567 Maryland Online Data Privacy Act of 2024

Position: Favorable

2/13/2024

The Honorable C.T. Wilson, Chair
Economic Matters Committee
Room 231
House Office Building
Annapolis, MD 21401

CC: Members of the House Economic Matters Committee

Economic Action Maryland (formerly the Maryland Consumer Rights Coalition) is a people-centered movement to expand economic rights, housing justice, and community reinvestment for working families, low-income communities, and communities of color. Economic Action Maryland provides direct assistance today while passing legislation and regulations to create systemic change in the future.

As an organization with a long history of advocating for consumer protection, I am writing today to urge your favorable report on HB567, the Maryland Online Data Privacy Act of 2024. This bill would limit the consumer data that companies collect online to only what is necessary for business operations.

Every day, companies are collecting and selling consumer data for an enormous profit, while many consumers remain unaware that their personal information is being traded and sold. In 2019, an estimated \$33 billion of revenue was collected from data sales alone just in the United States.¹ The unclear relationship between data collection and company profit has led to a significant amount of distrust from consumers. According to our published [report on digital equity](#), reluctance to use and distrust of the internet is one of the most significant factors challenging digital equity in Maryland. Reforms that seek to mitigate distrust from users is key to closing digital equity gaps.

The harmful effects of nonconsensual data collection can manifest in a myriad of ways. For example, tenant screening agencies scrape the internet for information on previous evictions and court cases and then sell their services to landlords so they can make “more informed decisions” on approving housing applicants without that prospective tenant even knowing the landlord had access to that data.² Data collection is also increasingly being utilized in the job market, where hiring agencies use data to determine characteristics of the “ideal applicant³.” This can create the major risk of discrimination against vulnerable populations, and prevent skilled applicants from finding employment.

This bill empowers consumers by providing them with new rights, including the ability to view, correct, delete, and opt out of data collection. Allowing consumers to choose what data is collected is beneficial in

¹ https://econaction.org/wp-content/uploads/2023/11/rhinesmith_2023_digital_equity_justice_maryland.pdf

² *ibid.*

³ *ibid.*



many contexts, from This increased control over their personal information gives consumers a say in how their data is used, promoting digital equity.

Additionally, requiring large companies to limit the collection of consumer data to what is necessary for legitimate business needs promotes data minimization practices. This helps prevent the unnecessary collection of sensitive information, reducing the potential for misuse or data breaches, further protecting consumers from harm.⁴

Maryland lacks a comprehensive data privacy law and this bill seeks to close this regulatory gap by introducing measures that address the challenges posed by rapid technological advancements, demonstrating a commitment to keeping consumer protections up to date and responding to emerging technologies. Our state has a long history of standing up for consumers, and we should continue to lead the nation in innovative policy that puts consumer protection and privacy at the forefront.

For these reasons we urge a favorable report on HB567.

Sincerely,
Zoe Gallagher, Policy Associate

⁴<https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=1fffbab51da4>

HB 567 Testimony - FWA - LexisNexis.pdf

Uploaded by: Caitlin McDonough

Position: FWA

February 9, 2024

The Honorable C.T. Wilson
Chair, House Economics Matters Committee
House Office Building, Room 231
6 Bladen Street
Annapolis, MD 21401

Re: HOUSE BILL 567 – THE MARYLAND ONLINE DATA PRIVACY ACT (Favor with amendment)

Dear Chair Wilson and Members of the House Economics Matters Committee:

I am writing on behalf of LexisNexis Risk Solutions (“LexisNexis”), a leading provider of credential verification and identification services for government agencies, Fortune 1000 businesses, and the property and casualty industry, to express concerns with House Bill 567, as introduced. While LexisNexis appreciates and supports Maryland’s efforts to provide practical and effective consumer protections for personal information and data, we join with industry in seeking clarifications in the proposed law to ensure the inclusion of the most up to date definitions and provisions and preserve our ability to provide quality services to our customers, particularly in the area of supporting fraud detection and identity theft.

Specifically, LexisNexis respectfully requests that the Committee consider amending the proposed legislation to (1) include “data subject to” in the Gramm-Leach-Bliley Act exemption to ensure that data subjected to the GLBA are properly regulated, (2) conform the definition of “publicly available information” with the majority of states who have privacy statutes, and (3) conform the provision to assist controllers who obtain data about a consumer from a source other than the consumer with the majority of states who have privacy statutes. We stand willing to work with the Sponsor and the Committee to develop language that achieves the intended privacy protections for consumers, while allowing industry participants to effectively comply and continue to provide valuable services.

LexisNexis takes this opportunity to thank Delegate Love for her hard work in this space and we remain committed to further collaboration in the development and implementation of best practices for data privacy, based on our expertise and experience. Thank you for your consideration of LexisNexis’ feedback on the proposed legislation.

Please let us know if we can answer any questions or provide any additional information.

Respectfully submitted,

Jeffrey Shaffer
Manager, Government Affairs, Mid-Atlantic
RELX (parent company of LexisNexis Risk Solutions)
1150 18th Street, NW, Suite 600
Washington DC, 20036
Mobile: 202-286-4894
Email: Jeffrey.shaffer@relx.com

HB567 - FWA - CSPRA.pdf

Uploaded by: Caitlin McDonough

Position: FWA



COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

Date: February 9, 2024
To: Members of the Maryland Legislature
Re: **Comments on HB 567 and SB 541 (the Bills)**

Who We Are

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit organization dedicated to promoting the principle of open public records access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, governmental, commercial, and societal benefit. Members of CSPRA are just a few of the many entities that comprise a vital link in the flow of information for these purposes and provide services that are widely used by constituents in your state. Collectively, CSPRA members alone employ over 75,000 persons across the U.S. The economic and societal activity that relies on entities such as CSPRA members is valued in the trillions of dollars and employs millions of people. Our economy and society depend on value-added information and services that includes public record data for many important aspects of our daily lives and work, and we work to protect those sensible uses of public records.

Ask: Replace Current Language with a Clean, Clear, Complete, and More Uniform Exemption for Publicly Available Information/Public Records

The current Bills have non-standard and limited Publicly Available Information (PAI) exemption. California, Utah, Virginia (and other states), and the model Uniform Personal Data Protection Act (UPDPA) proposed by the Uniform Law Commission (ULC) all have clean, clear, and complete publicly available information/public records exemptions. We support changing the bills to incorporate such an exemption that applies to all aspects of the bills.

The current Bills state:

PUBLICLY AVAILABLE INFORMATION MEANS INFORMATION THAT:

- (I) **IS LAWFULLY MADE READILY AVAILABLE TO THE GENERAL PUBLIC THROUGH FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS; OR**
- (II) **A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE THAT A CONSUMER HAS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC THROUGH WIDELY DISTRIBUTED MEDIA.**

We Recommend the UPDPA Language or Language Similar to other States as a Clean Public Records Exemption.

The UPDPA language mimics the state statutory exemptions for ALL public records and other PAI by exempting the following from the act:

- “(15) “Publicly available information” means information:
- (A) lawfully made available from a federal, state, or local government record;
 - (B) available to the general public in widely distributed media, including:
 - (i) a publicly accessible website;
 - (ii) a website or other forum with restricted access if the information is available to a broad audience;
 - (iii) a telephone book or online directory;
 - (iv) a television, Internet, or radio program; and
 - (v) news media;
 - (C) observable from a publicly accessible location; or
 - (D) that a person reasonably believes is made available lawfully to the general public if:
 - (i) the information is of a type generally available to the public; and
 - (ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed.”

Notice it covers more information that is clearly within 1st Amendment Rights by including widely distributed media and publicly observable facts and addresses all public records. Here are three other state definitions:

Iowa:

Publicly available information - means information that is lawfully made available through federal, state, or local government records, or information that a business has reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

Virginia:

“Publicly available information’ means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.”

Utah:

(29) "Publicly available information" means information that a person:
(a) lawfully obtains from a record of a governmental entity;

- (b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or
(c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

The Public Records Exemption Must Be Consistent with Maryland Public Records Law

Not all public records are made widely available “to the general public.” We recommend that this added “to the general public” language be removed from the exemption and that it read instead as noted above in the ULC UPDBA model act in section A. It states: “Publicly available information means information: (A) lawfully made available from a federal, state, or local government record.” Therefore, public records as a class and other publicly available information would not be personal information under any section of the act if it is properly placed in a definition section that covers the entire act.

Maryland’s existing public records law regulates access to certain public records to certain persons and for certain purposes. Adding the unnecessary and problematic qualifier “to the general public” would weaken existing privacy protections under the Maryland public records law which restricts access to certain public records to certain persons and for certain purposes (also note our discussion below on vendors to government and their use of public records on government’s behalf).

There Will Be Unintended Consequences from Including Opt-out and Secondary Use Restrictions Without Exemptions for all Public Records

The interaction of the opt-out and secondary use clauses with the lack of an adequate and clear public records exemption that applies to all sections of the Bill would be fatal to many essential uses of public records for law enforcement, child support recovery, lien enforcement, debt collection, underwriting, tax enforcement, witness location, judicial and legal processes, loans, auto safety recalls, and numerous other uses. We know that it is not author’s intent to let bad actors remove their public records from databases to commit more bad acts or escape responsibility for those they have already committed. A clean public records exception and authorized government vendor exemption (see below) solves these problems.

There Is a Need for A Clear Government and Government Vendor Exemption

Generally, government itself should not be governed by new public access to public records laws, and rules as the specific role of government, the enabling statutes, the rights involved, and privacy rules vary widely from government program to government program. Therefore, any proposed general privacy laws or rules should not apply to and hence shackle the government itself. It is therefore important to make it clear that vendors, parties, and subcontractors who carry out activities for and at the behest of government are also exempt from any general statute such as the ones proposed.

There are several ways that private entities use public and private data to support government administration, investigation, and enforcement of several laws. For example, vendors help with

finding missing and exploited children and trafficked persons, child support collection, tax lien collection, witness location, criminal investigations, and finding potential claimants or injured parties as part of a civil enforcement action by government. The Bills need to clearly exempt government **and** its selected vendors from the law for the lawful purposes for which the government uses those vendors.

Public Records Help Provide Essential and Valuable Services to State Residents, Businesses, and Government

Many persons and entities access and add value to the records they receive from public sources. They use these public records for a variety of personal, socially desirable, and essential civic and governmental purposes. We have attached an infographic that summarizes the benefits and uses of public information in the everyday lives of state residents and businesses. You will see that the information in the public record is foundational to many important life events and transactions of your state's residents.

Value-added services such as risk management, property title protection, news, protection of vulnerable populations, the administration of justice, law enforcement, monitoring government spending and corruption, enforcement of court orders and child support collection, and economic forecasting are just a few of the uses of public data. Consumers depend on the services that access, combine, and add value to public and private data almost every day and in ways that benefit all residents in every state whether they are aware of it or not.

Many institutions like the free press as well as businesses and service providers greatly rely on combinations of public and private records to function, and we all benefit in ways including, but not limited to, the following.

- Public and private data is used to monitor government for waste, fraud, and corruption.
- Data is used to find parents delinquent on child support.
- Combined public and private mapping data are used for locations, safety, consumer protection, and ratings of restaurants and retail stores.
- Real estate facts like square footage derived from public databases are key to buying and selling houses and provide consumers with accurate information.
- Vehicle registration data is used for safety recalls and helping forecast car sales data on which stock markets and manufacturing suppliers rely.
- Public information is used to find missing persons, witnesses, and suspects.

Protect Legal and Beneficial Uses of Public Records

Information in public records from local, state, and federal government sources are **owned by the People of Maryland**, not the person who is the subject of the record. Public records already **do not** include selected personally identifiable information and **do** include limits on its availability to selected parties for selected purposes in law, in rules, and by contract.

Information is so intricately embedded in so many aspects of life and commerce that it is difficult to predict all the ways a change in information policy will affect various people, products, services, uses, and government functions. CSPRA has tracked such policies over the last three decades and we often see many unintended consequences of limits on access and use of public records. This often results in a long list of frequently revised exceptions. The root cause of such unintended consequences is the attempt to limit access to public records and public information rather than focusing on bad actors and acts that the society wants to regulate.

Thank you for your consideration of our input. We strongly request that proposed privacy legislation include a clean PAI/public records exemption.

Richard J. Varn
Executive Director
Coalition for Sensible Public Records Access

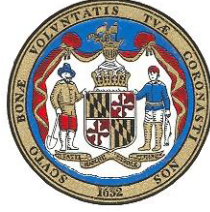
San Antonio, TX
Email: cspra@cspra.org
Cell : (515) 229-8984
(210) 236-1282

A non-profit organization dedicated to promoting the principle of open public records access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, commercial, and societal benefit.

HB 567 - STO Testimony.pdf

Uploaded by: Dereck Davis

Position: FWA



MARYLAND STATE TREASURER
Dereck E. Davis

Testimony of the Maryland State Treasurer’s Office

House Bill 567: Maryland Online Data Privacy Act of 2024

Position: Favorable with Amendments

House Economic Matters Committee

February 13, 2024

Since assuming responsibility of the Maryland 529 Program on June 1, 2023, the State Treasurer’s Office (STO) has become more familiar with privacy-related issues that arise in the savings program space. Proper data privacy protections are especially important when individuals’ personal savings are involved.

House Bill 567 specifies that the new requirements do not apply to “a regulatory, administrative, advisory, executive, appointive, legislative, or judicial body of the State, including a board, bureau, commission, or unit of the State or a political subdivision of the State.”¹ While this language clearly demonstrates an intent to exempt State entities, scenarios could arise where the program managers who administer the Maryland College Investment Plan, the Maryland Prepaid College Trust, and the Maryland Achieving A Better Life Experience (ABLE) Program would not be covered by the exemption. For this reason, STO respectfully requests an amendment to clarify that the new subtitle does not apply to instrumentalities of the State.

With the addition of the clarifying amendment, STO requests that the Committee give House Bill 567 a favorable with amendments report. Please contact Laura Atas, Deputy Treasurer for Public Policy (latas@treasurer.state.md.us), with any questions.

¹ Commercial Law, § 14-4603(a)(1).

HB 567_NICB_De Campos_FWA.pdf

Uploaded by: Eric De Campos

Position: FWA



February 9, 2024

The Honorable C. T. Wilson and Members of the Committee
House Economic Matters Committee
Maryland General Assembly

RE: House Bill 567 - Maryland Online Data Privacy of 2024

Dear Chair Wilson and Members of the Committee:

I am writing on behalf of the National Insurance Crime Bureau (“NICB”) to address concerns with House Bill 567 regarding consumer data privacy. As written, the bill would pose serious hardships on the ability of NICB – along with that of the Maryland Insurance Administration, our Maryland state and local law enforcement partners, and our member insurance companies – to combat insurance fraud.

Organization and Purpose

Headquartered in Des Plaines, Illinois, and with a 110-year history, the National Insurance Crime Bureau is the nation’s premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance fraud through intelligence-driven operations.

NICB sits at the intersection between the insurance industry and law enforcement, helping to identify, prevent, and deter fraudulent insurance claims. NICB’s approximately 400 employees work with law enforcement entities, government agencies, prosecutors, and international crime-fighting organizations in pursuit of its mission. NICB is primarily funded by assessments on our nearly 1,200-member property-casualty insurance companies, car rental companies, and other strategic partners. While NICB provides value to our member companies, we also serve a significant public benefit by helping to stem the estimated billions of dollars in economic harm that insurance crime causes to individual policy holders across the country every year.

NICB maintains operations in every state around the country, including in Maryland where NICB works together with law enforcement, state agencies, and prosecutors in a joint effort to protect Maryland consumers. NICB is an unmatched and trusted partner in the fight against insurance fraud.

Maryland’s Fraud Mandate and Specific References to NICB in Statute

The Maryland General Assembly acknowledged the public policy benefits of enabling the flow of insurance fraud reporting by enacting a requirement that insurers report suspected fraud to the Insurance Fraud Division. Md. Insurance Code § 27-802; *see also* COMAR 31.04.15.05. The Insurance Fraud Division receives this information from most insurers through NICB’s Fraud Bureau Reporting System (FBRP). That same statute provides NICB immunity from civil liability by facilitating insurance fraud reporting information through the FBRP. *Id.* § 27-802(c)(1)(iii).

The General Assembly also recognized the importance of NICB’s mission by specifically naming NICB in statute as a mandatory member of the Maryland Vehicle Theft Prevention Council within the Department of State Police. Md. Public Safety Code § 2-702.

Applicability of House Bill 567 and News Sections of Articles 13 and 14 of the Annotated Code of Maryland

House Bill 567 establishes various consumer rights relating to their personal data. The bill applies to any “person” conducting business in Maryland. Unlike laws enacted in California, Utah, Virginia, and Connecticut, the bill does not provide any exemption for non-profit organizations.

Section (A) of 14-4612 of the bill does provide certain limitations on the reach of the statute in order for entities to cooperate with law enforcement agencies concerning conduct or activity that may violate federal, state or local laws and regulations. Although our Charter aligns with this provision, and NICB would benefit from this section, our understanding is that the language of Section 14-4612 (A) is not meant to provide a wholesale exemption for such activities – meaning that, notwithstanding our ability to continue fighting fraud and other insurance crimes consistent with our Charter, NICB would still be subject to consumer requests to, for example, delete their data. Even for non-viable requests under this bill, NICB would nevertheless bear the burden of proving to each consumer directly, or in litigation, that NICB’s activities fall within the exception. The obligation to do so would strain our organization’s resources to such a degree that our operations, and ability to protect Maryland policyholders, would be drastically encumbered and diminished.

Although all entities within the scope of H.B. 567 would incur some level of compliance costs, the policy reasons for excluding NICB from these burdens are several-fold. First, NICB provides significant benefits to the general public and to the millions of consumers who are victims of insurance fraud. Second, as a non-profit organization that serves a public interest, NICB is not equally situated with private entities that typically establish more complex compliance infrastructure for private-sector-related obligations. For a public-service non-profit operating on an extremely lean budget, the potential cost of complying with H.B. 567 would drastically reduce the benefits NICB provides to the overall public good – without any associated benefit to consumers. Third, NICB’s required responses to individual consumer requests, or involvement in civil litigation, would likely expose otherwise covert criminal investigations. For example, if an illicit actor who is involved in multiple criminal conspiracies demands that NICB confirm that we are processing that individual’s data and requests access to that data, a mere response from NICB tying that information to a fraud-related purpose would provide a clear signal to that individual, thereby exposing any criminal investigation. Lastly, imposing what is essentially a “compliance, response, reporting and litigation” obligation – without any benefit to consumers – is wholly inconsistent with current insurance fraud reporting statutes and civil immunity provisions referenced above, which were enacted to facilitate the mandatory flow of insurance fraud information to Maryland state authorities. *See* Md. Insurance Code § 27-802; COMAR 31.04.15.05.

In addition to the constraints that the fraud limitation would provide as set forth above, that section would not provide NICB any protection for our operations relating to catastrophic events. For example, NICB provides invaluable assistance to federal, state, and local emergency response agencies and law enforcement entities in response to hurricanes, tornados, floods and other natural disasters. NICB partners with these entities in the lead up to and immediate aftermath of these events. NICB often deploys agents to assist with emergency responders and law enforcement in many different ways. The Geospatial Insurance Consortium (GIC), which is an initiative developed by NICB, has become an integral part of public agencies’ overall response plans to significant catastrophic events. GIC is an information sharing partnership designed to provide aerial maps and other information to help response agencies efficiently allocate their resources to the most heavily impacted areas. NICB provides sensitive information for purposes of taking aerial images and facilitating the flow of imagery information to emergency responders and law enforcement. This service is available as a result of partnerships with several public and private organizations and is provided at no cost to the public.

If the bill were enacted as is, the GIC program would be substantially impacted and could ultimately be shut down because not all critical information obtained and provided through the program would neatly apply within the limitation of Section 14-4612 (A). As a consequence, the service would be unavailable to public agencies and their overall response management plan. Without access to that information, the ability for first responders and law enforcement to successfully deploy resources in the most efficient way possible would be severely reduced. Moreover, information that NICB provides on an as-needed basis could be eliminated, further reducing the effectiveness of the public response to catastrophic events.

Proposed Changes and Policy Rationale

Consistent with longstanding public policy determinations already enshrined in Maryland law referenced above, NICB respectfully requests a narrow exemption to H.B. 567 by amending the following language into Section 14-4603 (A):

- (4) a not-for-profit entity that collects, processes, uses, or shares data solely in relation to identifying, investigating, or assisting:*
- (I) Law enforcement agencies in connection with suspected insurance-related criminal or fraudulent acts; or*
 - (II) First responders in connection with catastrophic events*

The policy reasons for such an exclusion are several-fold. First, NICB provides significant benefits to the general public, and to the millions of consumers who are victims of insurance fraud, in particular. Our law enforcement partners will bear testament to the enormous value NICB delivers. Second, NICB's mission is to lead a united effort to combat and prevent insurance crime. Subjecting NICB to data subject demands and potential litigation costs would be inconsistent with the plain language, intent, and spirit of the insurance fraud immunity statutes and the wholesale immunity provisions outlined above that are specifically designed to protect the sharing of information for insurance fraud reporting purposes. Even with the limitations described above, the bill would be at odds with that grant of immunity. Finally, the bill would not only impose significant compliance costs but could also substantially impact or eliminate NICB's catastrophic event response programs, thereby potentially diminishing and drastically reducing the benefits that NICB provides to the overall public good.

Conclusion

We appreciate your consideration of our concerns. I welcome the opportunity to follow up directly with your staff to discuss these issues in more detail. In the meantime, if you have any questions or need additional information, please contact me at edecampos@nicb.org or 847.989.7104.

Respectfully,



Eric M. De Campos
Senior Director
Strategy, Policy and Government Affairs
National Insurance Crime Bureau

OAG CPD Written Testimony HB 567.pdf

Uploaded by: Hanna Abrams

Position: FWA

CANDACE McLAREN LANHAM
Chief Deputy Attorney General

CAROLYN A. QUATTROCKI
Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CHRISTIAN E. BARRERA
Chief Operating Officer

ZENITA WICKHAM HURLEY
Chief, Equity, Policy, and Engagement

PETER V. BERNS
General Counsel



WILLIAM D. GRUHN
Chief
Consumer Protection Division

ANTHONY G. BROWN
Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

Writer's Direct Dial No.
(410) 576-7296

February 13, 2024

TO: The Honorable C.T. Wilson, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: House Bill 567 – Consumer Protection – Maryland Online Data Privacy
Act of 2024 (SUPPORT WITH AMENDMENT)

The Consumer Protection Division of the Office of the Attorney General supports House Bill 567 (“HB 567”), sponsored by Delegates Love, Valderrama, Boaf, Charkoudian, Feldmark, Fraser-Hidalgo, Hill, Kaiser, Kaufman, Lehman, Palakovich Carr, Pena-Melnyk, Shetty, Solomon, Stewart, Taveras, Watson, and Ziegler. House Bill 567 provides Marylanders with much needed control over who can collect, share, use, and sell their personal information.

Today, companies collect vast amounts of consumer data without consumer knowledge or consent. This data is sometimes used to serve consumer needs, but it can also be used to target, exploit, and expose consumers in harmful and sometimes dangerous ways.¹ Consumer data is often combined to provide detailed insights into very personal issues including mental health, gender, racial identity, religious beliefs, sexual preferences, and even our precise locations.² Indeed, data brokers compile data into lists of specific individuals with highly personal characteristics³ and sell it to third parties to be used to deliver everything from targeted

¹ See Technology Safety, Data Privacy Day 2019: Location Data & Survivor Safety (Jan. 28, 2019), <https://www.techsafety.org/blog/2019/1/30/data-privacy-day-2019-location-data-amp-survivor-safety>.

² Lee Matthews, *70% Of Mobile Apps Share Your Data with Third Parties*, Forbes, (June 13, 2017), <https://www.forbes.com/sites/leemathews/2017/06/13/70-percent-of-mobile-apps-share-your-data-with-third-parties/#562270ce1569> (finding that at least 70% of mobile apps share data with third parties, and 15% of the apps reviewed were connected to five or more trackers).

³ Drew Harwell, *Now For Sale: Data on Your Mental Health*, Washington Post (Feb.14, 2023), <https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/> (citing a Duke University study that found that based on data amassed online data brokers marketed lists of individuals suffering from anxiety and a spreadsheet entitled “Consumers with Clinical Depression in the United States”).

advertising,⁴ to differential pricing, to enable algorithmic scoring⁵ which can have discriminatory outcomes.⁶ Unlike consumers in thirteen other states, Maryland consumers have no knowledge or control over what is collected about them or what is done with that personal information.

House Bill 567 provides individuals with some transparency into and control over how their data is used. This transparency, coupled with giving users the right to access, correct, or delete their data, empowers individuals to protect themselves. They can reduce their data footprint, or remove their data from insecure third parties, minimizing the risk of fraud, identify theft, and exploitation.

Consumer Rights Provided by House Bill 567

House Bill 567 will provide Marylanders with important rights over their personal information, and impose specific obligations on businesses who handle consumers' personal data, including:

- *Right to Know*: consumers will have the right to know whether controllers are processing their data, as well as the categories of data being processed and the third parties the data has been disclosed to. Consumers will also have a right to obtain a copy of the consumer's personal data that a controller has or is processing;
- *Right to Correct*: Consumers will have the right to correct inaccuracies in their data;
- *Right to Delete*: Consumers will have the right to require a controller to delete their personal data;
- *Right to Opt-out of Sale*: Consumers will have the right to opt out of processing of the personal data for targeted advertising, sale, or profiling of the consumer in a way that produces legal effects.

In addition, HB 567 provides heightened protections for “sensitive data” – including, genetic, biometric, and geolocation data – which by its nature is especially revealing. House Bill 567 provides specific limitations on data that “presents a heightened risk of harm to a consumer” by limiting entities' ability to sell, monetize, or exploit this data.

⁴ *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>.

⁵ A Berkeley study found that biases in “algorithmic strategic pricing” have resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans as compared to White and Asian borrowers. This difference costs them \$250 million to \$500 million every year. Laura Counts, *Minority homebuyers face widespread statistical lending discrimination, study finds*, Haas School of Business at the University of California, Berkeley, (Nov. 13, 2018), <http://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/>; Upturn, *Led Astray: Online Lead Generation and Payday Loans*, (Oct. 2015), <https://www.upturn.org/reports/2015/led-astray/>. See also Yeshimabeit Millner and Amy Traub, *Data Capitalism and Algorithmic Racism, Data for Black Lives and Demos* (2021), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf

⁶ Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, ProPublica (Nov. 21, 2017), <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>.

Importantly, HB 567 sets an important baseline requirement that entities only collect data that “is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains.” This limits the misuse and accidental leakage of data by restricting what is collected at the outset.

Proposed Amendments

We do, however, have some recommendations in connection with HB 567:

Definitions:

Affiliate: In SB 567, “affiliate” is defined as a person that “shares common branding with another person” (page 2, lines 20-23) with no other limitations. We have concerns that this definition is overly broad and captures more than what would be traditionally considered an “affiliate.” We recommend amending the definition of affiliate to:

a person that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person such that: (a) The person owns or has the power to vote more than 50 percent of the outstanding shares of any voting class of the other person’s securities; (b) The person has the power to elect or influence the election of a majority of the directors, members or managers of the other person; (c) The person has the power to direct the management of another person; or (d) The person is subject to another person’s exercise of the powers described in paragraph (a), (b) or (c) of this subsection.⁷

Deidentified Data: Page 6, line 5, replace the word “if” with “and” to conform to the definition found in the Maryland Genetic Information Privacy Act.

Personal Data: On page 7, we recommend adding to the end of line 20 “consumer *or to a device identified by a unique identifier*” in order to be consistent with the definition of targeted advertising.

Exemptions:

We have concerns about the breadth of the exemptions in HB 567 that could serve to dilute the effect of the law, which we have shared with the sponsor. For example, page 12 lines 28-30, exempts *all* financial institutions and *all* affiliates of financial institutions subject to the federal Gramm-Leach-Bliley Act (GLBA) regardless of whether the personal data is governed by the GLBA. Advocates for financial institutions will claim that the industry is highly regulated and therefore they do not need additional privacy regulations, but financial institutions and their affiliates regularly collect information that is not governed by the GLBA. For example, when a financial institution collects information from non-customers or obtains information from a third-party or an affiliate outside of the context of providing a joint product or service, that personal information is not governed by federal privacy regulations.⁸ Given the breadth of the affiliate

⁷ Oregon Consumer Privacy Act, definition of “affiliate.”

⁸ 16 CFR § 313.1(b).

relationship, the Division recommends that page 12, lines 28-30 be replaced with the following language:

(3)(i) A financial institution, as defined by Md. Code, Fin. Inst. § 1-101, or a financial institution’s affiliate or subsidiary that is only and directly engaged in financial activities, as described in 12 U.S.C. 1843(k);

(ii) An insurer, as defined by Md. Code, Ins. §§ 1-101(v), other than a person that, alone or in combination with another person, establishes and maintains a self-insurance program and that does not otherwise engage in the business of entering into policies of insurance;

(iii) An insurance producer, as defined by Md. Code, Ins. § 1-101(u); and

(iv) A person that holds a license issued under Md. Code, Ins. § 10-103.

Similarly, we recommend clarifying that the exemption found on page 13, line 3, applies to protected health information that is regulated by the Health Insurance Portability and Accountability Act of 1996 by replacing it with the following language:

Protected health information that a covered entity or business associate processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, and regulations promulgated under the Act, as in effect on the effective date of this 2023 Act.

Controller Obligations:

We recommend clarifying, on page 22, line 21, that the disclosure applies to “sale” as well as processing (conspicuously disclose the *sale or processing...*”). This resolves an internal inconsistency because according to lines 17-18, the paragraph applies if a controller “sells personal data . . . or processes personal data,” but the term sale is absent from the controller disclosure obligations on line 21.

Finally, we note that HB 567 does not include a private right of action. Without a private right of action, as the lone entity able to take action against violators, the Consumer Protection Division will need significantly more resources to enforce this bill. To that end, the Office of the Attorney General believes that a Privacy Enforcement and Protection Unit with sufficient resources should be established within the Consumer Protection Division.

We urge the Economic Matters Committee to issue a favorable report on HB 567 with the amendments discussed.

cc: Members, Economic Matters Committee
The Honorable Sara Love
The Honorable Kriselda Valderrama
The Honorable Adrian Boafo
The Honorable Lorig Charkoudian
The Honorable Jessica Feldmark

The Honorable David Fraser-Hidalgo
The Honorable Terri L. Hill
The Honorable Anne R. Kaiser
The Honorable Aaron M. Kaufman
The Honorable Mary A. Lehman
The Honorable Julie Palakovich Carr
The Honorable Joseline A. Pena-Melnyk
The Honorable Emily Shetty
The Honorable Jared Solomon
The Honorable Vaughn Stewart
The Honorable Deni Taveras
The Honorable Courtney Watson
The Honorable Natalie Ziegler

FavWAmEd AHA Data Privacy HB 567.pdf

Uploaded by: Laura Hale

Position: FWA



February 9, 2024

Testimony of Laura Hale
American Heart Association

Favorable W/ Amendment HB 567 Maryland Online Data Privacy Act of 2024

Dear Chair Wilson, Vice Chair Crosby and Honorable Members of the Economic Matters Committee,

Thank you for the opportunity to speak before the committee today. My name is Laura Hale, and I am the Director of Government Relations for the American Heart Association. The American Heart Association expresses its support for HB 567 with one amendment.

We appreciate your leadership on the important issue of consumer data privacy and support the Legislature's desire to establish important consumer protections. The AHA shares this goal and, as such, uses industry standard security protocols to protect our donors' and volunteers' information, and readily make our privacy policy available to the public. We do, however, have some concerns that the current version of House Bill 567 will create unintended consequences for non-profit organizations.

The cost of proving our compliance with the policy is high and is burdensome for nonprofit organizations. Every dollar that a public charity must devote to data privacy compliance is a dollar that we cannot use to further our missions. For AHA, this means less going toward funding cardiovascular research, setting clinical guidelines for cardiac and stroke care, and providing CPR training materials and courses that are used throughout the US. Moreover, when a public charity like AHA does not commercialize that data (i.e., sell it), the costs are even more painful. Donors expect their funds to support the mission, not for handling consumer data questions and portability support requests, and they can easily read the privacy policies and charity watchdog ratings to see how their data is used.

With that in mind, we recommend connecting 501(c)3 nonprofit compliance with this legislation to the Better Business Bureau Standards for Charity Accountability¹. By being registered and in compliance with these standards, we are following the spirit and intent of the Data Privacy Law. By being able to demonstrate that we are registered and in compliance (by the rating provided by the BBB Standards for Charity Accountability) nonprofits would both demonstrate that we are complying with data privacy, but also remove the more burdensome process of demonstrating this compliance. Below I have copied the standards outlined by the BBB Standards for Charity Accountability:

¹ [Implementation Guide to the BBB Standards for Charity Accountability \(give.org\)](https://www.give.org/standards)

“Address privacy concerns of donors by

- a. providing in written appeals, at least annually, a means (e.g., such as a check off box) for both new and continuing donors to inform the charity if they do not want their name and address shared outside the organization, and
- b. providing a clear, prominent and easily accessible privacy policy on any of its websites that tells visitors (i) what information, if any, is being collected about them by the charity and how this information will be used, (ii) how to contact the charity to review personal information collected and request corrections, (iii) how to inform the charity (e.g., a check off box) that the visitor does not wish his/her personal information to be shared outside the organization, and (iv) what security measures the charity has in place to protect personal information. “

Bearing this in mind, we ask for the amendment outline below, we are very open to conversations on how best to work towards this amendment (or similar language) and look forward to continued discussion with the sponsors.

Amendment Language:

14-4603

A. THIS SUBTITLE DOES NOT APPLY TO:

.....

(4) A 501(c)3 NONPROFIT CHARITY THAT IS REGISTERED AND COMPLIANT WITH THE BETTER BUSINESS BUREAU WISE GIVING ALLIANCE STANDARDS FOR CHARITY ACCOUNTABILITY

The American Heart Association urges amending this legislation to lessen the burden on nonprofits for compliance with this legislation.

2024 NAMIC letter HB567 Consumer data privacy (2).

Uploaded by: Matt Overturf

Position: FWA

House Economic Matters Committee
MARYLAND HB 567: Consumer Data Privacy
Favorable w/Amendment | February 13, 2024

Chair Wilson and Members of the House Economic Matters Committee:

On behalf of the National Association of Mutual Insurance Companies¹ (NAMIC) thank you for the opportunity to submit this statement of Favorable with Amendment (FWA) to House Bill 567.

NAMIC consists of nearly 1,500 member companies, including seven of the top 10 property/casualty insurers in the United States. The association supports local and regional mutual insurance companies on main streets across America as well as many of the country's largest national insurers.

The insurance industry takes consumer privacy very seriously and have been subject to numerous laws and regulations for years for the protection of consumer data. Our industry's commitment to appropriate use and safeguarding of consumer information has helped establish what has become a comprehensive federal and state regulatory framework governing the use and disclosure of personal information for the insurance industry.

Exceptions for GLBA-Subject Financial Institutions

NAMIC is very appreciative of the inclusion of GLBA exemption language in House Bill 567 and would respectfully request the exemption be amended slightly to include 'data' as well as citing the implementing regulations of Title V of the Gramm-Leach Bliley Act of 199 in the Maryland Insurance Code Sec. 2-109.

When considering the broad privacy landscape, NAMIC encourages legislators to fully understand all the existing frameworks of laws and regulations currently in place, which can vary significantly from industry to industry. New provisions would not be enacted in a vacuum. This is especially true for insurance -- each state and the federal government already has robust laws/regulations to address data privacy, security, and other requirements. By recognizing that this is not a blank slate and to forestall confusion and conflicts, NAMIC advocates that new provisions are not a disconnected additional layer of obligations. To avoid unintended consequences, NAMIC encourages policy makers to recognize existing laws and regulations.

Given the vital business purposes for data in the insurance transaction, historically policy makers have recognized the important role information plays in insurance and, with certain protections in place, they have allowed collection, use, and disclose for operational and other reasons.

Title V of the Gramm-Leach-Bliley Act (GLBA)² provides a landmark privacy framework for financial services, including insurance. It sets forth notice requirements and standards for the disclosure of nonpublic personal

¹ NAMIC member companies write \$357 billion in annual premiums and represent 69 percent of homeowners, 56 percent of automobile, and 31 percent of the business insurance markets. Through its advocacy programs NAMIC promotes public policy solutions that benefit member companies and the policyholders they serve and fosters greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

² See 15 U.S.C. Sec. 6801 et. seq.



financial information – it specifically requires giving customers the opportunity to opt-out of certain disclosures. Under GLBA, functional financial institution regulators implemented the privacy standards. Given concerns with consistency, the National Association of Insurance Commissioners (NAIC) has adopted multiple model laws with regard to data privacy and cybersecurity³. And states have moved forward with adopting those models. For insurers, the Maryland Insurance Administration (MIA) regulates privacy matters (including consistent with Md. Code regs. 31.16.08.01 to 31.16.08.24) and provides robust oversight.

When it comes to retaining information, insurers are already subject to specific record retention requirements. This information is important for several reasons. Insurers need to have information available for claims and litigation and insurance regulators rely on data for market conduct purposes. Again, insurance-related data is subject to numerous existing laws and regulations.

While NAMIC is pleased to see the inclusion of a GLBA exemption in HB 567, the exception should apply to both the data and entity subject to the GLBA as follows:

(3) A Financial Institution or affiliate of a financial institute or *data* that is subject to Title V of the Federal Gramm-Leach-Bliley Act and regulations adopted under the act and the rules and implementing regulations promulgated thereunder or to Maryland Insurance Code Ann. Sec. 2-109 and the rules and implementing regulations promulgated thereunder.

Thank you for taking the time to consider our position on House Bill 567.

Sincerely,

Matt Overturf
Regional Vice President
Ohio Valley/Mid-Atlantic Region

³See NAIC Model Laws [668](#), [670](#), [672](#), [673](#)

HB 567 Support with Amendments.pdf

Uploaded by: Matt Power

Position: FWA



140 South Street,
Annapolis, MD 21401
410-269-0306
www.micua.org



Support with Amendments

House Economic Matters Committee *House Bill 567 (Love) Maryland Online Data Privacy Act of 2024*



Matt Power, President
mpower@micua.org
February 14, 2024



On behalf of the member institutions of the Maryland Independent College and University Association (MICUA) and the nearly 55,000 students we serve, I thank you for the opportunity to provide this written testimony support with amendments [HB 567 \(Love\) Maryland Online Data Privacy Act of 2024](#). This bill establishes a new standard for data privacy in Maryland both for consumers as well as controllers of data.



The bill is similar to legislation passed in other states across the country to provide consumers a greater say in the use and sale of their data. MICUA members take data privacy extremely seriously and spend a tremendous amount of time and resources to keep student data protected. Unfortunately, the bill seems to inadvertently single out non-profit institutions of higher education for inclusion while exempting public institutions of higher education. Similar bills in other states like Utah, Colorado and Connecticut have exempted both public and non-profit institutions of higher education.



MICUA requests that the sponsors consider a friendly amendment to Sec. 14-4603(3) that would include an exemption for non-profit institutions of higher education.



If you have any questions or would like additional information, please contact Irnande Altema, Associate Vice President for Government and Business Affairs, ialtema@micua.org.



For all of these reasons, MICUA requests a favorable Committee report, with amendments, for House Bill 567.



Re_ H.B. 567 Maryland Online Data Privacy Act - SU

Uploaded by: Matt Schwartz

Position: FWA



February 9, 2024

Chair C.T. Wilson
Vice Chair Brian M. Crosby
Economic Matters Committee
Maryland House of Delegates
Room 231
House Office Building
Annapolis, Maryland 21401

Re: H.B. 567 Maryland Online Data Privacy Act - SUPPORT WITH AMENDMENTS

Dear Chair Wilson, Vice Chair Crosby, and Members of the Economic Matters Committee,

Consumer Reports¹ sincerely thanks you for your work to advance consumer privacy in Maryland. H.B. 567 would extend to Maryland consumers important new protections, including meaningful data minimization restrictions, heightened standards for the processing of sensitive data, and strong civil rights protections. The bill also creates baseline consumer privacy rights, including the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the ability to require businesses to honor universal opt-out signals and authorized agent requests to opt out of sales, targeted advertising, and profiling.

Consumers currently 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 process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers are constantly tracked online and their behaviors are often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which erode individuals' basic expectation of privacy and can lead to disparate outcomes along racial and ethnic lines.

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.

This bill's data minimization provision (Section 14-4607 (B)(1)(I)) surpasses many other states' and would go a long way toward mitigating many of these types of harms. While we prefer privacy legislation that limits companies' collection, use, *and* disclosure of data to what is reasonably necessary to provide the service requested by the consumer (the bill only currently applies this standard to data collection, while allowing a much looser standard for processing activities)², simply reigning in systemic over-collection of consumers' personal information alone would help eliminate common practices that have contributed to, among other things, the persistent drip of massive data breaches.

Suitably, H.B. 567 also seeks to reduce unwanted secondary processing of data by creating a framework for universal opt-out through universal controls. Privacy legislation with universal opt-outs empowers consumers by making it easier to set their preferences relating to secondary processing, like sales or targeted advertising, eliminating the need for them to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.³ The goal of universal opt-out is to create an environment where consumers can set their preference once and feel confident that businesses will honor their choices as if they contacted each business individually.

Aside from this bill's thoughtful approach to minimization and opt-outs, we also appreciate that it includes the following elements:

- *Special Protections for Sensitive Data.* The bill builds on the underlying data minimization standard by requiring that the collection, processing, or sharing of any *sensitive* information be "strictly necessary" to provide the service requested by the consumer and that the controller obtain consent prior to undertaking any of these activities. These restrictions would effectively ban third-party targeted advertising and data sales based on our most personal characteristics, including data about our race, religious beliefs, health data, and data about children (targeted advertising to teens is also separately banned), which would represent a major change to the digital ecosystem, appropriately shifting the burden of privacy protection away from consumers themselves to companies that otherwise have every incentive to exploit consumer data for their own benefit. While we have concerns that this section's opt-in consent provisions may introduce unnecessary consent fatigue (if data processing is truly limited to providing what the consumer asked for, why should they need to consent on top of that), we support the intent of this provision wholeheartedly.

² Section 14-4607(9) of the bill ostensibly includes data minimization language restricting processing activities; however, because data processing is limited to any purpose listed by a company in its privacy policy — instead of to what is reasonably necessary to fulfill a transaction — that language will in practice have little effect for secondary purposes after data is collected.

³ Aleecia M. McDonanld and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, no. 3 (2008), 543-568.
https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y

We also note that Section 14-4604 (4) should be eliminated, since consumer health data is included as a category of sensitive data, and sales of sensitive data would never be “strictly necessary” to provide or maintain a service.

- *Strong civil rights protections.* This bill appropriately addresses a key harm observed in the digital marketplace today: 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. The bill ensures that a business’ processing of personal data cannot lead to discrimination against individuals or otherwise make opportunity or public accommodation unavailable on the basis of protected classes. A number of privacy bills introduced federally in recent years have included similar civil rights protections, including the American Data Privacy and Protection Act which overwhelmingly passed the House Energy and Commerce Committee on a 53-2 bipartisan vote.⁴ Consumer Reports’ Model State Privacy Legislation also contains similar language prohibiting the use of personal information to discriminate against consumers.⁵

At the same time, the legislation still contains several loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Maryland consumers deserve:

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* H.B. 567’s opt-out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions). In California, many companies have sought to avoid the CCPA’s opt-out requirements by claiming that much online data sharing is not technically a “sale” (appropriately, CPRA expands the scope of California’s opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).⁶ We recommend including “sharing” in H.B. 567’s opt-out right and using the following definition:

“Share” [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

We also recommend refining the definition of “targeted advertising” to better match consumer expectations of the term. The drafted definition opens a loophole for data

⁴ See Section 2076, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act,

<https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf>

⁵ See Sections 125 and 126, Consumer Reports, Model State Privacy Act, (Feb. 2021)

https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf

⁶ Id.

collected on a single site; it only includes ads based on a “consumer’s activities over time and across nonaffiliated **websites**” (plural, emphasis ours). This would exempt “retargeted” ads from the scope of the bill’s protections — ads based on one particular product you may have considered purchasing on another site. Such advertising — such as a pair of shoes that follows you all over the internet after you had left a merchant’s site — are the stereotypical example of targeted advertising; the law’s opt-out provisions should certainly apply to it. We suggest a shift toward the following definition:

“Targeted advertising” means the targeting of advertisements to a consumer based on the consumer’s activities with one or more businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller’s own commonly-branded websites or online applications; (b) based on the context of a consumer’s current search query or visit to a website or online application; or (c) to a consumer in response to the consumer’s request for information or feedback.

- *Add a private right of action.* Given the AG’s limited resources, a private right of action is key to incentivizing companies to comply. Under an AG-only enforcement framework, businesses that recognize that the AG is only capable of bringing a handful of enforcement actions each year might simply ignore the law and take their chances in evading detection. Further, it’s appropriate that consumers are able to hold companies accountable in some way for violating their rights. We strongly encourage legislators to include a private right of action in future drafts of the legislation.
- *Eliminate the GLBA carveout.* The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act. This carveout makes it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business crosses the threshold into providing traditional financial services, a line many of them are already skirting, if not already well past.⁷ The bill should instead simply provide an exemption for *information* that is collected pursuant to GLBA, as was done with HIPAA covered data.
- *Narrow the loyalty program exemption.* We are concerned that the exception to the anti-discrimination provision when a consumer voluntarily participates in a “bona fide loyalty, rewards, premium features, discounts, or club card program” (Section 14-4607(c)(2)) is too vague and could offer companies wide loopholes to deny or discourage consumer rights by simply labeling any data sale or targeted advertising practice as part of the “bona fide loyalty program.” We urge the sponsors to adopt a more precise definition and provide clearer examples of prohibited discrimination that

⁷ See e.g., The Economist, “Big Tech Pushes Further into Finance,” (Dec. 15, 2022), <https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance>; Richard Waters,

does not fall under this exception. 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, generally 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 first-party advertising.

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.⁸ 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.⁹ 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.¹⁰ 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.¹¹

- *Remove ambiguities around requirements that the universal opt out mechanism not “unfairly disadvantage” other controllers.* The bill requires controllers to allow consumers to opt out of sales and targeted advertising through an opt-out preference signal (OOPS). However, the bill would also confusingly prohibit OOPSs from “unfairly disadvantage[ing]” other controllers in exercising consumers’ opt-out rights. It is unclear what “unfairly disadvantage” might mean in this context, as by their definition mechanisms that facilitate global opt-outs “disadvantage” some segment of controllers by limiting their ability to monetize data. Consumers should be free to utilize OOPSs to opt out from whatever controllers they want. For example, a consumer may want to use a certain OOPS that specifically opts them out from data brokers (or may configure a general purpose mechanism to only target data brokers); in that case, a consumer (and the OOPS) should be empowered to only send opt-out requests to data brokers. The

⁸ 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>

⁹ *ibid.*

¹⁰ *ibid.*

¹¹ See Consumer Reports’ model State Privacy Act, Section 125(a)(5) for an example of a concise, narrowly-scoped exemption for loyalty programs. <https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/>

term “unfairly” introduces unnecessary ambiguity and the subsection should be eliminated.

- *Amend prohibitions on default opt-outs.* Currently, the bill states that OOPSs cannot send opt-out requests or signals by default. The bill should be amended to clarify that the selection of a privacy-focused user agent or control should be sufficient to overcome the prohibition on defaults; an OOPS should not be required to specifically invoke Maryland law when exercising opt-out rights. OOPSs are generally not jurisdiction-specific — they are designed to operate (and exercise relevant legal rights) in hundreds of different jurisdictions. If a consumer selects a privacy-focused browser such as Duck Duck Go or Brave — or a tracker blocker such as Privacy Badger or Disconnect.me — it should be assumed that they do not want to be tracked across the web, and they should not have to take additional steps to enable the agent to send a Maryland-specific opt-out signal. Such a clarification would make the Maryland law consistent with other jurisdictions such as California and Colorado that allow privacy-focused agents to exercise opt-out rights without presenting to users a boilerplate list of all possible legal rights that could be implicated around the world.

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Maryland residents have the strongest possible privacy protections.

Sincerely,
Matt Schwartz
Policy Analyst

HB 567_Maryland Online Data Privacy Act of 2024_MD

Uploaded by: Andrew Griffin

Position: UNF



LEGISLATIVE POSITION:

Unfavorable

House Bill 564

Maryland Online Data Privacy Act of 2024

House Economic Matters Committee

Tuesday, February 13, 2024

Dear Chairman Wilson and members of the committee:

Founded in 1968, the Maryland Chamber of Commerce is the leading voice for business in Maryland. We are a statewide coalition of more than 6,800 members and federated partners working to develop and promote strong public policy that ensures sustained economic health and growth for Maryland businesses, employees, and families.

House Bill 564 would establish a framework for regulating how consumer's personal data is controlled and processed. The bill would also grant certain rights to consumers regarding their personal data and establish methods for consumers to exercise those rights. The Maryland Chamber of Commerce and its members place a high priority on consumer privacy and believe that privacy laws should provide strong safeguards for consumers but also balance the need for industry to innovate.

The Chamber recognizes the work and collaboration that have gone into writing HB 564 compared to iterations of past years. To that end, it is imperative from the Chamber perspective, that members of the General Assembly and stakeholders continue working toward a data privacy law that mirrors the budding regional approach, providing a clear set of rules for businesses and consumers, no matter their location. Areas of outstanding concern with HB 564 include:

- 1. Aligning definitions and requirements with those in other states.**
 - a. The definition of biometric information, consumer health data, and sensitive data is of most concern.
- 2. Ensuring the Attorney General retains sole responsibility of enforcement.**
- 3. Remove the requirement for permission to use personalized marketing techniques.**

The Maryland Chamber of Commerce represents businesses of all sizes and industries, many of which would be impacted in some way by HB 564. We look forward to continuing the conversation on behalf of our diverse membership to produce legislation that is effective, consistent, and avoids unnecessary burdens.

SPSC - MD HB 567 (Omnibus) - Unfavorable Testimony

Uploaded by: Andrew Kingman

Position: UNF

STATE PRIVACY & SECURITY COALITION

February 09, 2024

Chair C.T. Wilson
Vice Chair Brian M. Crosby
House Economic Matters Committee
Room 231
House Office Building
Annapolis, MD 21401

Re: Comprehensive Privacy (HB 567) - Unfavorable

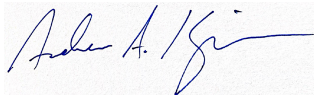
Dear Chair Wilson, Vice Chair Crosby, and Members of the Committee,

The State Privacy and Security Coalition (SPSC), a coalition of over 30 companies and six trade associations the retail, telecom, tech, automotive, and payment card sectors respectfully opposes HB 567 in its current form, but writes with general recommendations to HB 567 and the hope that this bill can be improved and in a place to be enacted in 2024. We appreciate that Maryland is taking a comprehensive approach to privacy legislation and respectfully request amendments that effectively balance consumer protections in Maryland with implementation and compliance by the business community in a way that aligns with the protections provided and obligations imposed by other states that have adopted similar frameworks.

We appreciate the diligence from and consideration by the sponsors regarding the concerns that we have communicated to them, and look forward to continuing our conversations. Our primary concerns stem around provisions that are either unique to this bill (they do not appear in any other US privacy law) or provisions that are in all other laws which do not currently appear in HB 567.

We believe that working from a comprehensive, interoperable framework that provides strong privacy protections for consumers, clear and robust obligations for businesses, while still maintaining interoperability with other states, will provide the most seamless and modern approach to privacy for Maryland consumers. After a number of years of consideration by this legislature, we are hopeful that HB 567 represents a path forward that will put Maryland with the growing number of states with a comprehensive privacy framework.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

HB0567_UNF_MTC_Maryland Online Data Privacy Act of

Uploaded by: Drew Vetter

Position: UNF



MARYLAND TECH COUNCIL

TO: The Honorable C.T. Wilson, Chair
Members, House Economic Matters Committee
The Honorable Sara Love

FROM: Andrew G. Vetter
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
Christine K. Krone
410-244-7000

DATE: February 13, 2024

RE: **OPPOSE UNLESS AMENDED** – House Bill 567 – *Maryland Online Data Privacy Act of 2024*

The Maryland Tech Council (MTC) writes in **opposition unless amended** to *House Bill 567: Maryland Online Data Privacy Act of 2024*. We are a community of nearly 800 Maryland member companies that span the full range of the technology sector. Our vision is to propel Maryland to become the number one innovation economy for life sciences and technology in the nation. We bring our members together and build Maryland’s innovation economy through advocacy, networking, and education.

Consumer privacy is of the utmost importance to members of the MTC, so we are supportive of the concept of protecting the private data of Maryland residents. We appreciate the efforts of the bill sponsors to model this bill on laws in other states and the attempt to craft a law that works for Maryland consumers and businesses. The most important issue for the MTC is to have a data privacy law where full compliance is not overly burdensome. In many respects, this bill is based on laws that have been passed in other states such as Connecticut, Delaware, Colorado, Virginia, and others. In fact, there have been 13 states to date that have passed “comprehensive” data privacy laws, such as the one proposed here. In that spirit, the MTC has remaining concerns about portions of the bill that make compliance more difficult or impractical.

First, the MTC encourages the committee to align defined terms and data processing provisions as closely as possible to those in already-enacted laws in other states. There are MTC member companies doing business in other states and have already adapted their business practices in those states to align with these definitions and provisions. Having different rules and misaligned definitions of the same terms from state to state makes compliance impractical. We are aware that trade groups like TechNet and SPSC have been working with the bill sponsors to highlight these differences. The MTC is strongly in support of aligning these definitions and provisions to consensus language in other states.

Second, the MTC strongly advocates for the inclusion of a right to cure provision in the bill. By nature, a comprehensive online data privacy bill is lengthy and complicated. Businesses, especially smaller businesses, will be challenged in digesting these complex new requirements and bringing their business processes and systems into compliance. Our members appreciate the need for a comprehensive

data privacy bill and want to be in compliance. Businesses should be given the opportunity under the bill to correct minor compliance issues or mistakes before they are subject to enforcement actions. An opportunity to correct errors, even for some reasonable period of time, is merited in this circumstance, given the complex nature of the bill and the extent of new requirements.

Third, and also in the vein of compliance, the MTC recommends pushing back the effective date of the bill. The proposed effective date in the bill is October 1, 2024. That leaves businesses only 6 months from the end of Session until the effective date to get into compliance with this new law. Again, the requirements contained within this bill are lengthy and complex. Many of the Maryland-based companies impacted by this bill are small and do not have compliance teams or in-house attorneys to quickly operationalize these new requirements. These companies should be given more time to make the changes necessary to comply with this law by pushing back the effective date.

In conclusion, the MTC's concerns with this legislation can be summarized into two main areas: consistency and compliance. We urge the committee to make this bill as consistent as possible with comprehensive data privacy laws already passed in other states. We also request that the committee amend the bill to make it more feasible for companies to comply, specifically by looking at provisions, such as a right to cure and a different effective date.

The MTC recommends an unfavorable report unless amended consistent with this testimony. Thank you for the consideration.

HB0567(MD) SIA Opposes - Final version.pdf

Uploaded by: George Sewell

Position: UNF



February 22, 2023

Chair C. T. Wilson
Economic Matters Committee
Maryland General Assembly

RE: Security Industry Association (SIA) Position on House Bill 567

Dear Chair Wilson, Vice-Chair Crosby and Members of the Economic Matters Committee:

On behalf of the Security Industry Association (SIA) and our members, I am writing to express our concerns with HB 567 as it currently stands under consideration by the committee.

SIA is a nonprofit trade association located in Silver Spring, MD that represents companies providing a broad range of safety and security-focused products and services in the U.S and throughout Maryland, including more than 40 companies headquartered in our state. Among other sectors, our members also include the leading providers of biometric technologies available in the U.S.

Privacy is important to the delivery and operation of security systems and services, and our members are committed to protecting personal data. Given the lack of congressional action on a nationwide data privacy framework, in 2024, more than a dozen U.S. states have enacted consumer data privacy laws and many more are considering similar measures during legislative sessions this year.

While we are pleased to see that the measure as introduced is similar to the emerging consumer data privacy standard common among the vast majority of states that have enacted such measures, we believe numerous changes are critical to bring it into full alignment that will support uniform and thorough compliance.

Of these, we have submitted several key proposed adjustments to the House and Senate sponsors of the measure, none of which alter its intended effect:

- Ensuring the definition of “biometric data” is consistent with the current standard across existing state data privacy laws.
- Ensuring similar definitional alignment for various security/anti-fraud exceptions.
- Addition of explicit language ensuring exclusive Attorney General enforcement, which is uniform across existing state data privacy laws.
- Addition of a local preemption provision, which is also standard across existing state data privacy laws.

These key changes would address our concerns with HB 567. We urge the committee not to approve the measure unless these changes are made.

Again, we support the overall goal of HB 567 in safeguarding personal data and information, and we stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully submitted,

George Sewell
Government Relations Coordinator
Security Industry Association
Silver Spring, MD
gsewell@securityindustry.org
www.securityindustry.org

CTIA Testimony in Opposition to Maryland HB 567 -

Uploaded by: Jake Lestock

Position: UNF



**Testimony of
JAKE LESTOCK
CTIA**

In Opposition to House Bill 567

Before the Maryland House Economic Matters Committee

February 13, 2024

Chair Wilson, Vice-Chair Crosby, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to House Bill 567. Our members support strong consumer privacy protections, including empowering consumers with the rights necessary to control their data. While consumer data is best addressed at the federal level, we look forward to working with the sponsor to ensure this legislation aligns with existing state frameworks on consumer protection.

Consumer privacy is an important issue and the stakes involved in consumer privacy legislation are high. State-by-state regulation of consumer privacy is creating an unworkable patchwork that will lead to consumer confusion. That is why CTIA strongly supports ongoing efforts within the federal government to develop a uniform national approach to consumer privacy. Deviating from clearly defined definitions, obligations, and privacy protections could have serious consequences for consumers, innovation, and competition in Maryland. A



patchwork quilt of state regulations would only complicate federal efforts and impose serious compliance challenges on businesses, ultimately confusing consumers.

The Maryland legislature is considering a privacy law that would generally apply to all industries. While a national standard is our preferred approach, we understand the concerns driving state action on these issues in the absence of a federal privacy law. The comprehensive approach in HB 567 is the right approach for state regulation. Importantly, it largely aligns with the comprehensive frameworks enacted in fifteen other states to date. This alignment is critical to ensure consistently strong consumer protections for consumers and to drive interoperable compliance processes for businesses with customers in many states.

We encourage the Maryland legislature to continue with this approach, and to make some amendments to ensure the bill is interoperable with the laws that have already passed in other states. For example, we urge the legislature to further conform definitions like “targeted advertising” and “consumer health data” to match other state laws. General data collection and use restrictions also need to be further aligned with existing state laws. Ensuring conformity in definitions will ensure strong consumer privacy rights and protections and impose robust but clear obligations on businesses.

Additionally, HB 567 does not include a provision for a right to cure, which is found in the Virginia, Connecticut, Colorado, and Utah data privacy frameworks. This is a significant tool that allows a state enforcement authority to seek speedy resolution to good faith



compliance issues, and to focus their resources for enforcement actions on those businesses that either will not or cannot come into compliance within the statutory cure period.

In closing, we reiterate our concern about the enactment of state laws that create further fragmentation at the state level and recommend Maryland looks to further conform definitions and data collection restrictions with existing state laws and include a right to cure provision. For these reasons, CTIA respectfully opposes HB 567. We look forward to working with the sponsor to address some ways the bill can be amended to better align with existing state laws.

CHPA Amendment Request MD HB 567.pdf

Uploaded by: John McLuckie

Position: UNF



CONSUMER
HEALTHCARE
PRODUCTS
ASSOCIATION

Taking healthcare personally.

February 6, 2024

Delegate C.T. Wilson
Chair, House Economic Matters Committee
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

Re: H.B. 567 - Maryland Online Data Privacy Act of 2024

Dear Chairman Wilson,

On behalf of the Consumer Healthcare Products Association (CHPA), the Washington, D.C. based national trade organization representing the leading manufacturers of over-the-counter (OTC) medicines, dietary supplements, and consumer medical devices, thank you for the opportunity to comment on H.B. 567. Unfortunately, I'm writing to express opposition to this bill as currently drafted. Although we do not object to the overall goal of the bill, which aims to empower consumers to have greater authority over their personal data, we do hold reservations about its compatibility with current federal regulations pertaining to controlled substances. Given the potential clash between these laws, we are against HB 567 unless it undergoes amendments to accommodate the existing federal obligations regarding data collection.

Controlled Substances Act

The Controlled Substances Act (CSA), also referred to as the Comprehensive Drug Abuse Prevention and Control Act, was enacted by Congress in 1970 with the aim of regulating the production, distribution, and utilization of controlled substances. As per 21 U.S.C. Section 830 of this Act, individuals or entities involved in transactions concerning listed chemicals (such as pharmacies selling allergy medications containing ephedrine or pseudoephedrine) are obligated to gather and retain identifiable personal records pertaining to these transactions and to share the data with law enforcement as required. Unfortunately, this bill does not provide an exemption for such transactions from its privacy provisions.

Amendment Recommendations

To avoid potential conflict with already existing federal law, CHPA recommends the following amendment to H.B. 567 on page 14, line 22 as item (13):

[\(13\) Personal data collected and used for purposes of the federal policy under the Controlled Substances Act Section on the Regulation of Listed Chemicals under 21 U.S.C. SEC. 830.](#)

Conclusion

CHPA and its members are committed to safeguarding the privacy of our customers' data. We commend the House Economic Matters Committee for taking on this important issue, but unfortunately, we cannot support this bill in its current form. We look forward to continued dialogue with the hope we can come to an equitable resolution.

Respectfully submitted,



Carlos I. Gutiérrez
Vice President, State & Local Government Affairs
Consumer Healthcare Products Association
Washington, D.C.
cgutierrez@chpa.org | 202-429-3521

Cc: Members of the House Economic Matters Committee

2024-2-9_CCIA Comments on MD HB 567.pdf

Uploaded by: Khara Boender

Position: UNF



February 9, 2024

House Economic Matters Committee
Room 231, House Office Building
6 Bladen Street
Annapolis, MD 21401-1912

RE: HB 567 - “Maryland Online Data Privacy Act of 2024” (Unfavorable)

Dear Chair Wilson and Members of the House Economic Matters Committee:

On behalf of the Computer & Communications Industry Association (CCIA)¹, I write to respectfully oppose HB 567, unless amended.

CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.²

CCIA strongly supports the protection of consumer data and understands that Maryland residents are rightfully concerned about the proper safeguarding of their data. CCIA also appreciates the significant effort that lawmakers have undertaken to strike the appropriate balance for meaningful protections while preserving benefits consumers receive and the ability for innovation to thrive. As you know, in the absence of a comprehensive law at the federal level, there is a growing number of states that have enacted their own laws. The majority of these laws harmonize a key set of definitions and concepts related to privacy. While we appreciate the sponsors’ work on this bill, as written, HB 567 still would diverge from existing frameworks in several key ways, as further detailed below.

Definitions and controller obligations should be clear and interoperable.

Existing broad-based privacy laws typically recognize a core set of rights and protections including individual control, transparency of processing activities, and limitations on third-party disclosures. However, even minor statutory divergences between frameworks for key definitions or the scope of privacy obligations can create onerous costs for covered organizations. Therefore, CCIA encourages that any consumer privacy legislation is reasonably aligned with existing definitions and rights in other jurisdictions’ privacy laws so as to avoid unnecessary costs to Maryland businesses. As drafted, key

¹ CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: <https://www.ccianet.org/about>.

² Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), <https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf>

definitions in HB 567 are likely to prompt significant statutory interpretation and compliance difficulties, even for businesses with existing familiarity with other US state laws. Specifically, CCIA recommends attention to the following terms to align definitions such as: “biometric data”, “consumer health data”, and “targeted advertising”. We also suggest aligning the definition of “geofence” based on existing state laws, such as in Washington and New York. As currently written, the bill’s definition of “geofence” is inconsistent and conflicts with the bill’s definition of “precise geolocation data”.

CCIA also suggests clarifying that the definition of “sensitive data” would encompass the personal data of a *known* child. This would be consistent with the *actual knowledge* standard under COPPA and remove ambiguity.

CCIA suggests slight amendments to the definition of “publicly available information” to align with definitions in Oregon or Virginia. Under the current definition, a Maryland “consumer” (resident) that is not acting in a commercial or employment context would be required to make data publicly available. By extension, this would mean that any public information about a Maryland resident made available by persons other than a “consumer” could be excluded from being considered “publicly available information” and it would be treated as “personal information”. This would be a significant departure from the understanding of what constitutes “personal information” and could create a broadly sweeping “right to be forgotten”, where a person could request for data generally accepted as “publicly available” to be deleted. These provisions could have broad implications for other uses of such data, including search indexing, and training of artificial intelligence models, creating potential quality and bias concerns.

Finally, HB 567 would require a controller to obtain consumer consent prior to collecting personal data for content personalization or marketing. CCIA recommends striking this language as it is a novel provision in the context of other state data privacy laws, hindering the development of new products and services. This provision would also limit businesses' ability to conduct ad measurement, which would limit digital advertising for businesses large and small and have significant impacts on the internet economy.

CCIA requests further clarification regarding the enforcement provisions.

CCIA appreciates Maryland lawmakers’ consideration of appropriate enforcement mechanisms for a comprehensive data privacy framework and requests further clarity that HB 567 would not permit consumers to bring legal action against businesses that have been accused of violating new regulations. Every state that has established a comprehensive consumer data privacy law to date has opted to invest enforcement authority with their respective state attorney general. Private rights of action on other issues in states, such as under the Illinois Biometric Information Privacy Act, have resulted in plaintiffs advancing frivolous claims with little evidence of actual injury. These lawsuits also prove extremely costly and time-intensive for all parties involved, including the state, and it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state. In other states, similar lawsuits have resulted in plaintiffs advancing frivolous claims with little evidence of actual injury. These lawsuits also prove extremely costly and time-intensive for all parties involved, including the state, and it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state. Further, every state



that has established a comprehensive consumer data privacy law to date has opted to invest enforcement authority with their respective state attorney general.

* * * * *

CCIA and our members are committed to providing consumers with protections and rights concerning their personal data, however, further harmonization with established frameworks is needed. We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

UNFAVORABLE.HB567.SB541.MDRTL. L.Bogley.PDF

Uploaded by: Laura Bogley

Position: UNF



Opposition Statement HB567/SB541
Maryland Online Data Privacy Act of 2024
Laura Bogley-Knickman, JD
Director of Legislation, Maryland Right to Life

We Oppose HB567/SB541

On behalf of our 200,000 followers across the state, we respectfully yet strongly object to HB567/SB541. This bill is unconstitutional, as it infringes on the First Amendment right to freedom of speech.

The bill infringes on First Amendment Free Speech

This bill, without due process of law, would deny free speech by prohibiting the use of geofencing within proximity of reproductive health clinics. Geofence marketing or “geofencing” is a commonly used location-based **marketing** and advertising strategy that allows you to send targeted ads to customers within a given geographical area. This marketing technology relies only on locating mobile signals within a triangulated area from a cell tower.

Geofencing technology locates cell phone signals but does not access data from cell phones or computers and therefore does not violate an individual’s right to privacy. This legal marketing method is a relatively less expensive way for a nonprofit or community-based organization to communicate with or educate potential customers. This bill would discriminately impose economic restrictions on the ability of Maryland nonprofits and other businesses to conduct business in the state. This violates the Equal Protection clause of the Constitution.

This bill discriminates on the content of speech by prohibiting geofence marketing only in proximity to “reproductive health” clinics and not other locations or business industries.

The offending section reads as follows and should be removed:

14–4604. A PERSON MAY NOT: (3) USE A GEOFENCE: (I) TO IDENTIFY, TRACK, COLLECT DATA FROM, OR SEND A NOTIFICATION TO A CONSUMER REGARDING THE CONSUMER’S CONSUMER HEALTH DATA; AND (II) WITHIN 1,750 FEET OF A MENTAL HEALTH FACILITY OR REPRODUCTIVE OR SEXUAL HEALTH FACILITY;

The bill denies women and girls Informed Consent

By limiting the use of geofencing in proximity to reproductive health clinics, the state would be denying women who seek reproductive health services, access to additional and/or alternative services related to reproductive health. In enacting this bill, the state would be denying Maryland women the right to informed consent by blocking access to educational and informational resources relevant to reproductive health. By denying women informed consent, the state subjects women to reproductive coercion and other forms of medical abuse.

Federal Precedent Prohibits Targeting Pro-life Speech

In conflict with federal court precedent, this bill attempts to **target and suppress pro-life speech** in Maryland. In [*Greater Baltimore Ctr. for Pregnancy Concerns, Inc. v. Mayor & City Council of Baltimore*, 879 F.3d 101 \(4th Cir. 2018\)](#), the City of Baltimore acting on behalf of abortion advocates, attempted unsuccessfully to put pro-life pregnancy centers out of business by enacting a targeted ordinance against commercial speech as "deceptive advertising".

The federal appeals court for the 4th Circuit affirmed the lower court's decision in favor of the pro-life pregnancy center, noting that ***"the City has considerable latitude in regulating public health and deceptive advertising. But Baltimore's chosen means here are too loose a fit with those ends, and in this case compel a politically and religiously motivated group to convey a message fundamentally at odds with its core beliefs and mission."*** The City also failed to establish that the pro-life pregnancy center was engaged in commercial or professional speech, which required the Court to apply higher scrutiny against the government action. Without proving the inefficacy of less restrictive alternatives, providing concrete evidence of deception, or more precisely targeting its regulation, the City did not prevail.

For these reasons we oppose this bill and request your unfavorable report.

[MD] HB 567 Privacy_TechNet_written_pdf.pdf

Uploaded by: margaret durkin

Position: UNF



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622
www.technet.org | @TechNetMidAtla1

February 9, 2024

The Honorable C.T. Wilson
Chair
House Economic Matters Committee
Maryland House of Delegates
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

RE: HB 567 (Love) - Maryland Online Data Privacy Act of 2024.

Dear Chair Wilson and Members of the Committee,

On behalf of TechNet, I'm writing to offer remarks on HB 567 related to omnibus data privacy.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.2 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, and Washington, D.C.

We appreciate your leadership and thoughtful approach to consumer data privacy. The technology industry is fully committed to securing privacy and security for consumers and engages in a wide range of practices to provide consumers with notice, choices about how their data is used, as well as control over their data. TechNet believes that any consumer privacy bill should be oriented around building consumers' trust and fostering innovation and competitiveness. New privacy laws should provide strong safeguards to consumers while also allowing the industry to continue to innovate. These new laws should be based upon a uniform set of standards to avoid imposing a patchwork of policies across jurisdictions.

Thank you to Delegate Love for including TechNet in the stakeholder process early on and for incorporating several of our suggested changes. As mentioned during discussions with the sponsors, interoperability among states is key in the absence of a federal privacy standard. As such, TechNet continues to seek changes to HB 567, which are outlined below.

Definitions

TechNet requests that definitions in the bill align with other states' models. Specifically, we request that the definition of "Biometric Data" include the language "are used", as opposed to "can be used", and "identify" instead of "authenticate". For "Consumer Health Data", we request this definition be aligned with Connecticut's definition to avoid a different set of data being covered by each state. We also request that "status" in the definition be struck and replaced with "condition or diagnosis". For "Sale" and "Targeted Advertising", we request those match other states. For "De-identified Data", we request that the requirement of publicly committing not be limited to a privacy policy or terms and conditions. On "Precise Geolocation", we request a comma after "contents of communication". This is a clarifying change, universal among states. For "Sensitive Data", we suggest using the language "known child" and "for the purpose of uniquely identifying an individual" after genetic data or biometric data. No other state uses a "knows or has reason to know" standard.

Enforcement

TechNet requests at least a one-year effective date, right to cure period, and clarifying language around prohibiting private rights of action. Companies, large and small, will need adequate time to come into compliance with this bill by implementing consent mechanisms, renegotiating all existing contracts with vendors, and establishing new teams for Data Protection Assessments, among several others. A right to cure period allows for injunctive relief for the consumer and allows time for businesses to right any perceived wrongs while coming into compliance with this bill. TechNet thanks the sponsor for their intention to not include a private right of action in this legislation; however, to avoid loopholes, TechNet requests the below language to take that intent a step further.

- THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE ENFORCEMENT AUTHORITY TO ENFORCE VIOLATIONS OF THIS ACT. NOTHING IN THIS ACT SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BE SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS OR ANY OTHER LAW.

14-4607 – Controller Responsibilities

On page 19 of the bill, please strike lines 27 through 29 dealing with content personalization. Content personalization is a major outlier and strays from other states' models. Regarding the standard of "knew or should have known", TechNet is requesting that phrase be struck and replaced with "has actual knowledge or willfully disregards...". To our knowledge, no other state has a "knew or should have known" standard, so we have aligned this to the standard in most other states.

Finally, as other state AGs develop their own lists of approved opt-out signals, we believe it makes sense to state that if a controller is working from a list of approved signals by another state AGO, it shall be deemed in compliance with this section.

Additional requests are appended in this document and have been shared with the sponsors ahead of this hearing.

TechNet joins industry partners and strongly encourages Maryland to look to the protections for consumers included in other states' omnibus privacy laws to avoid a patchwork of state laws that are difficult to comply with and confusing for consumers. Our members are committed to being collaborative in Maryland as the process moves forward. Please continue to consider TechNet's members a resource in this effort. Thank you for your time and we look forward to continuing these discussions with you.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

**MD COMPREHENSIVE PRIVACY BILL (HB 567 / SB 541)
TOP PRIORITIES**

1. Definitions:

a. Biometric Data

- i. "Are used" vs. "Can be used" (overinclusive)
- ii. "Identify" vs. Authenticate (underinclusive)

b. Consumer Health Data

- i. Match to CT (implementing language as well)
 - 1. Sale w/ consent permitted for all sensitive data

c. Sale

- i. Match exceptions to all other states

d. Targeted Advertising

- i. Match to all other states

e. Deidentified Data

- i. "publicly commits"

f. Precise Geolocation

- i. "Contents of communications, or"

g. Sensitive Data

- i. Biometric/genetic "for the purpose of uniquely identifying..."
- ii. "Known child" instead of "reason to know"

2. Enforcement

a. "Nothing in this act..." and "AG exclusive authority" language

- i. "This act does not prevent a consumer from pursuing any other remedy provided by law."

b. Right to Cure

c. Effective Date

d. Preemption

3. §14-4607

a. Delete Consent for use of marketing/personalization if sole use (not in any of the 13 states, can be deceiving).

b. Align Data minimization with all 13 other states

c. Prohibition on selling sensitive data without the consumer's consent

d. "Actual knowledge or willfully disregards..." instead of "known or should have known" phrasing

4. DPA Requirements

a. "For each algorithm used"

b. "On a regular basis"

c. DPA's not retroactive

5. Exemptions

a. Conduct solely internal research

- b.** No liability for misuse by other party if no actual knowledge
 - c.** Exemptions for current MD Medical Records/Information statutes
 - d.** GLB – add data
 - e.** HIPAA/Healthcare alignment with other states
- 6. Non-Conforming Provisions that Do Not Advance Privacy/Tweaks**
- a.** 14-4608(A)(3)(II) and (III) deletion
 - b.** 14-4608(B)(1) deletion
 - c.** 14-4607(D)(4) conformance with CT (Privacy Policy) or CO if needed (as outlined in redline)
 - d.** 14-4608(D)(4) – Delete third party reference
 - e.** 14-4605(E)(2)(III) deletion
 - f.** Delete 14-4612(B)(1) exception
 - g.** 14-4606(A) – clarify that opt-out mechanism applies only to sale/targeted advertising
 - h.** Replace all references to “Person” with “A controller or processor”
 - i.** Add consent requirement to (A)(9)

MDDC Oppose HB567.pdf

Uploaded by: Rebecca Snyder

Position: UNF



Maryland | Delaware | DC Press Association

P.O. Box 26214 | Baltimore, MD 21210

443-768-3281 | rsnyder@mddcpres.com

www.mddcpres.com

To: House Economic Matters Committee

From: Rebecca Snyder, Executive Director, MDDC Press Association

Date: February 9, 2024

Re: **HB567 - OPPOSE**

The Maryland-Delaware-District of Columbia Press Association represents a diverse membership of newspaper publications, from large metro dailies such as the Washington Post and the Baltimore Sun, to hometown newspapers such as the Star Democrat and Maryland Independent, to publications such as The Daily Record, Baltimore Jewish Times, and online-only publications such as the Baltimore Banner, MoCo 360, Maryland Matters and Baltimore Brew.

The Press Association cannot support HB 567 as written. Previous versions of the bill were more strictly tailored to biometric data and the Press Association chose not to weigh in. We have concerns with recent changes to the bill, now called the Maryland Online Data Privacy Act of 2024.

We believe some modifications in this year's version of the bill could impose unintended negative consequences on Maryland's news media entities, which in turn would curtail access to vital journalism resources for the state's residents.

Three top concerns are highlighted below, and we welcome the opportunity to provide further feedback and redlines as you consider the legislation.

- 1. Geofencing:** We recognize the Legislature's intent in including restrictions on the use of geofencing in sensitive health-related settings. However, we believe the new language may contain a drafting error that would create a technical violation for common advertising practices completely unrelated to the protected facility.

Connecticut's amended privacy legislation [Public Act No. 23-56](#) reads:

"No person shall:...(C) use a geofence to establish a virtual boundary that is within one thousand seven hundred fifty feet of any mental health facility or reproductive or sexual health facility *for the purpose of* identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data; or (D) sell, or offer to sell, consumer health data without first obtaining the consumer's consent."

In contrast, HB 0567 reads: "14-4604. A PERSON MAY NOT: (3) USE A GEOFENCE:

(I) TO IDENTIFY, TRACK, COLLECT DATA FROM, OR SEND A NOTIFICATION TO A CONSUMER REGARDING THE CONSUMER'S CONSUMER HEALTH DATA; AND

(II) WITHIN 1,750 FEET OF A MENTAL HEALTH FACILITY OR REPRODUCTIVE OR SEXUAL HEALTH FACILITY; OR

(4) SELL OR OFFER TO SELL CONSUMER HEALTH DATA WITHOUT THE CONSENT OF THE CONSUMER WHOSE



We believe a strong news media is central to a strong and open society.

Read local news from around the region at www.mddcnews.com

HEALTH DATA IS TO BE SOLD OR OFFERED TO BE SOLD. “

As drafted, the Maryland Online Data Privacy Act of 2024 could restrict the ability to use a geofence to send notifications to or communicate with consumers, even with their consent. The reordering of the section would also prohibit the use of a geofence within 1,750 of a facility regardless of purpose. Particularly in densely developed urban and suburban areas, there is a high likelihood of colocation of pharmacies and other medical practices with the protected facilities in question. The effect is highly likely to result in unintended technical violations of the bill.

Worse, the language could severely impact the ability of local merchants and businesses who happen to be within 1750 feet of a facility to engage in effective and compliant marketing and advertising practices to draw attention to and benefit businesses. Local news media entities often provide some services on behalf of these businesses. We urge adoption of the Connecticut language.

2. Controller Data Collection Limitations: We have two concerns with new bill language.

First, sections 14-4607. (A) (1), (3), (5) and (6) contain language that mirrors other legislation, most notably Connecticut, but with slight changes in sentence drafting. These changes could have the unintended consequence of banning any marketing, sale of sensitive data, or the processing of data that is consistent with COPPA. We welcome the opportunity to suggest technical redlines to restore the intent of the bill.

Second, the previous version, 2023’s HB 0807, contained controller duties that were largely similar to those with other states, such as Connecticut: “A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary to collect for the purposes for which the data is processed” which is consistent with well-understood principles of data minimization.

The exact section in HB 0567 has been modified as follows:

“14-4607. (B) (1) A CONTROLLER SHALL: (I) LIMIT THE COLLECTION OF PERSONAL DATA TO WHAT IS REASONABLY NECESSARY AND PROPORTIONATE TO PROVIDE OR MAINTAIN A SPECIFIC PRODUCT OR SERVICE REQUESTED BY THE CONSUMER TO WHOM THE DATA PERTAINS;

We are concerned the amended language would prohibit well-understood, expected data processing tasks done in service of common activities such as research and development, audience analysis, or marketing.

Most critically, as written, the language serves as a *de facto* opt-in for targeted advertising, which directly conflicts with the clearly outlined sections in the bill that outline opt-out requirements for targeted advertising.

3. Enforcement: Consistent with other states’ comprehensive consumer privacy legislation, we appreciate that the Maryland Online Data Privacy Act of 2024 does not include a private right of action. However, we note the addition of the following language:

“14-4613. (B) THIS SECTION DOES NOT PREVENT A CONSUMER FROM PURSUING ANY OTHER REMEDY PROVIDED BY LAW.”

As evidenced by discussions over the state’s anti-SLAPP legislation, news media entities are disproportionately vulnerable to baseless, frivolous lawsuits. Given Maryland’s robust ability to enforce unfair, abusive, or deceptive trade practices under Title 13, we recommend striking the language above from the bill, and/or adding the following:

“THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE AUTHORITY TO ENFORCE VIOLATIONS OF SECTIONS OF THIS ACT.”

We look forward to working with the sponsor on these technical amendments. Until these amendments are made, we urge an unfavorable report.

HB567_MRA_UNF.pdf

Uploaded by: Sarah Price

Position: UNF



HB567: Maryland Online Data Privacy Act of 2024
Economic Matters Committee
February 13, 2024

Position: Unfavorable as introduced, neutral with amendments

Background: HB567 establishes generally the manner in which a controller or a processor may process a consumer’s personal data; authorizing a consumer to exercise certain rights in regards to the consumer’s personal data; requiring a controller of personal data to establish a method for a consumer to exercise certain rights in regards to the consumer’s personal data; etc.

Comments: Based on feedback received from members, the Maryland Retailers Alliance respectfully proffers the following amendments to HB567:

1. Page 5, line 13: INSERT “intentionally” before “designed or manipulated.”
 - a. Dark pattern violations are like fraud and should be considered an intentional act of deceit.
2. Page 4, line 23, Strike lines 21-23 and INSERT in its place “(I)(1) “Consumer health data” means personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a regulated entity uses to identify the past, present or future physical or mental health status of the consumer.”
 - a. This change further clarifies the meaning of the term.
3. Page 6, line 1: STRIKE OR DEFINE “(8) access to essential goods or services”.
 - a. This is problematic without a precise definition of “essential goods and services”.
4. Page 8, line 13: AMEND the definition of “processor” to include that a processor “does not determine the purposes or means of processing the personal data”.
 - a. The current definition is missing this key limitation which was included in all other state privacy laws.
 - b. Did processors request that this limitation be left out of the Maryland draft?
5. Page 11, line 1: STRIKE line 1 “((VIII) Citizenship or immigration status)”, ADJUST remaining numbering.
 - a. This list of potentially sensitive data qualifiers should be struck as it broadens the defined term of “sensitive data” to potentially include “non-personal data”. This non-personal data may imply inaccurate information

about consumer (e.g., buying a cross might “reveal” one is Christian; buying cosmetics might “reveal” race). A law based on possible inferences drawn from retail purchases would be problematic.

6. Page 11, line 17: INSERT “unaffiliated” before “websites or online applications”.
 - a. The current definition of “target advertising” could include providing ads based on a consumer’s activities on a business’s first-party website or mobile app, which has no precedence of being considered targeted advertising in state privacy laws.
 - b. This issue could also be addressed by adding “advertisements based on a consumer’s activity displayed by a controller on any first-party website or mobile app owned or operated by that control” to the list of exemptions of “targeted advertising” beginning on page 10, line 20.
7. Page 11, after line 24: Recommend adding a second sentence that a third party must not determine the purposes or means of data processing, to reflect other recommendations regarding the definition of “processor” (page 8, line 5, mentioned above).
8. Page 12, line 8: REPLACE “produces” with “provides”.
 - a. “Provides” is a more standard term used for this policy in other states. “Produces” could have unclear meaning and unintended consequences.
9. Page 12, line 12: REPLACE “35,000 consumers” with “100,000 consumers”.
 - a. Setting the threshold at 35,000 is far too low to protect small businesses. Most states use 100,000.
10. Page 12, line 9: REPLACE “10,000 consumers” with “50,000 consumers” AND REPLACE “20%” with “50%”.
 - a. This should say at least 50,000 consumers and derived more than 50% of revenue from the sale to remain consistent with almost every other state.
11. Page 15, line 27: ADD “, unless retention of the personal data is required by law” after “consumer”.
 - a. Creates an exception that allows a controller to dismiss a consumer’s request to delete and retain information if it is required by another area of law.
12. Page 19, lines 5-11: STRIKE lines 27-29 in entirety, from “(1) collect personal data...” through “share sensitive data concerning a consumer;” ADJUST remaining numbering.
 - a. Section 14-4606(A)(1) and (2) are highly problematic. Like other consumer-facing businesses, retailers typically grow by attracting new customers. For example, retailers opening new store locations traditionally obtain lists of local households to send mailers announcing the new store opening. The law must preserve the same ability to collect data in the online environment for the purpose of marketing to prospective customers.

- b. Further, the law should not limit collection or processing to that “strictly necessary” to provide or maintain a “specific product or service requested by the consumer”. Retailers have always marketed products to inform the public of what is available for purchase. The inclusion of “strictly necessary” would limit the ability to provide this information to consumers.
- 13. Page 19, line 26: STRIKE “(1) Collect personal data for the sole purpose of content personalization or marketing without the consent of the consumer whose personal data is collected;”, ADJUST remaining line number.
 - a. Personalized marketing does not create a harm for a consumer and should not be treated like sensitive information.
- 14. Page 21, line 5: ADD “and processor” after “controller”.
 - a. Data minimization provisions should apply equally to both and not to controllers alone. There is no legitimate public policy justification for limiting this to controllers only; processors oppose data minimization requirements for their own benefit. The policy should establish an equal playing field.
- 15. Page 21, line 21: REPLACE “15” with “45”.
 - a. Extends the amount of time controllers have to respond to consumer requests to be in line response requirements on Page 17, lines 5 and 8 and consistent with requirements in other states’ consumer privacy laws.
- 16. Page 25, line 1-3: STRIKE “the controller shall comply with the consumer’s opt-out preference signal. (2)”
 - a. The indicated phrase would require the general opt-out preference (signaled by a browser) to override a consumer’s previous opt-in to voluntarily participate in a controller’s loyalty program. The recommended edit would clarify this for the customer and allow them to choose to continue participation in the loyalty program, rather than automatically overriding their original opt-in choice.
- 17. Page 27, line 16: INSERT “designed” before “to ensure”.
 - a. Controllers cannot guarantee that a processor will adhere to instructions. Including “designed” protects controllers when processors do not follow instructions that are intended to limit consumer data processing.
- 18. Page 28, line 15: STRIKE “(V) Other substantial injury to a customer”.
 - a. “Other substantial injury” is not defined, so this potential risk is unclear and should be removed.
- 19. Page 32 and 33, lines 29-2:
 - a. The protection provided to third party controllers or processors in 14-4610(D) needs to run both ways to protect controllers from the independent misconduct of third-party processors and controllers, as it

does in most state privacy laws. Controllers must similarly be protected from the violations of the law by processors and third parties and held harmless unless they have actual knowledge the processor or third party intends to violate the law with the consumer data they receive from the controller.

20. Page 33, lines 10-12: ADD “or processor” after “If a controller” and ADD “or processor” before “shall demonstrate that the processing:”
 - a. This obligation should apply equally to both controllers and processors.
21. Page 34, lines 11-12: STRIKE lines 11-12 in entirety, from “(B) This section” to “other remedy provided by law”.
 - a. We would ask that private right of action be prohibited.
 - b. Making clear AG enforcement via the following language:
“THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE ENFORCEMENT AUTHORITY TO ENFORCE VIOLATIONS OF THIS ACT. (D) NOTHING IN THIS ACT SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BE SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS OR ANY OTHER LAW.”
22. Page 34, line 18: REPLACE “2024” with “2025”.
 - a. Controllers need adequate time to prepare for compliance with these requirements.
23. Other States have a “right to cure” provision including California. We would respectfully ask for one with a sunset to ensure compliance.

Additionally, MRA has historically expressed concerns to the legislature regarding the impact that data privacy policies may have on the ability to offer retail loyalty rewards programs, which customers voluntarily choose to participate in for access to discounts and other rewards. Page 21 of the bill prohibits retailers from charging different prices for goods if a customer opts out of data sharing, which would restrict access to loyalty programs and which was not included in laws in the majority of other states.

The bill already has a disclosure requirement for data sales, and not all retailers engage in data sales with respect to their customer loyalty plan data, so it does not make sense to add a duplicative disclosure requirement or, worse, ban data sales from loyalty plans when their data sales are not banned outright in every other use case.

We suggest adding language clarifying that the disclosure requirements related to data sales also applies to loyalty plans, and that a retailer may not offer a loyalty program unless they are in compliance with those disclosure obligations in subsection (E) of the same section 14-4607 where the loyalty plan language is located. Suggested amendment in bold:

14-4607.

* * *

(C) NOTHING IN SUBSECTION (A) OR (B) OF THIS SECTION MAY BE CONSTRUED TO:

* * *

(2) PROHIBIT A CONTROLLER FROM OFFERING A DIFFERENT PRICE, RATE, LEVEL, QUALITY, OR SELECTION OF GOODS OR SERVICES TO A CONSUMER, INCLUDING OFFERING GOODS OR SERVICES FOR NO FEE, IF THE OFFERING IS IN CONNECTION WITH A CONSUMER'S VOLUNTARY PARTICIPATION IN A BONA FIDE LOYALTY, REWARDS, PREMIUM FEATURES, DISCOUNTS, OR CLUB CARD PROGRAM **THAT COMPLIES WITH SUBSECTION (E).**

Thank you for your consideration. We look forward to working with the sponsor and committee to resolve these issues.