

CPD Written Testimony HB 567 in Senate Finance.pdf

Uploaded by: Hanna Abrams

Position: FAV

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



ANTHONY G. BROWN
Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

WILLIAM D. GRUHN
Chief
Consumer Protection Division

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

March 21, 2024

TO: The Honorable Pamela Beidle, Chair
Senate Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

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

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 gives users the right to access, correct, or delete their data, allowing 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.

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.

Privacy Enforcement and Education Unit

House Bill 567 creates a comprehensive scheme of consumer rights and the Consumer Protection Division will require additional resources in order to implement and enforce this bill, especially because HB 567 excludes the private right of action under § 13-408 of the Consumer Protection Act. Accordingly, the Attorney General requested that the General Assembly create a Privacy Enforcement and Education Unit in the Consumer Protection Division, however it does not appear that the requested Unit will be funded this year.

Comparison to Senate Bill 541

We note that there are some differences between Senate Bill 541 and House Bill 567.

§ 14-4601 Definitions:

- *Biometric Data*: Unlike SB 541, HB 567 defines “biometric data” in a manner consistent with existing Maryland law. The definition found on page 3, line 25 of HB 567 conforms to the definition in the Maryland Personal Information Protection Act which defines “biometric data” to include “any other unique biological characteristics that *can be* used to uniquely authenticate a consumer’s

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>.

identity” (Md. Com. Law § 1-3501(e)(1)(i)(6)).⁷ The Division requests that the Senate Finance Committee keep the definition set forth in HB 567 since introducing a different definition for the same term in statutes governing related conduct as SB 541 does will lead to confusion.

- *Decisions that produce legal or similarly significant effects concerning the consumer:* We support the definition in HB 567 because it is consistent with *all other states* that define this term in their privacy law. Removing “insurance” from this definition, as SB 541 does, creates inconsistency between the States’ privacy laws and could lead to unnecessary confusion.⁸

§ 14-4603 Exemptions:

- We have concerns that SB 541 includes an exemption not found in HB 567 for a nonprofit controller that process or shares personal data for the purpose of assisting law enforcement agencies in investigating criminal or fraudulent acts relating to insurance; or first responders in responding to catastrophic events.” This exemption, which appears to exempt a single entity, is duplicative and unnecessary as this conduct is already permitted under § 14-4612(8)-(9) which ensure that controllers are allowed to take immediate steps to protect life or physical safety and to prevent harm or any other illegal activity.⁹
- The Division notes that there is a difference between the language excluding “medical records” found in HB 567 and SB 541.¹⁰ We recommend using the language found in SB 541 (page 14, line 30 through page 15, line 14) as it more accurately reflects the intent to exclude only records that are protected under the Maryland Medical Records Act, but not under the Health Insurance Portability and Accountability Act.
- The Division is concerned about the exemption found in SB 541, which is not in HB 567, for personal data that “is collected . . . in furtherance of the business of insurance.” (page 16, lines 11-14). The exemption could create a loophole for secondary uses as it is focused on the purpose of the *collection* and does not limit its use to purposes that are “in furtherance of the business of insurance.” We also note that there is already an exemption for both institutions *and data* that are subject to Title V of the Federal-Gramm-Leach Bliley Act (§ 14-4603(3)).

⁷ Page 3, line 22 of SB 541 defines biometric data to include “any other unique biological characteristics that *are* used to uniquely authenticate a consumer’s identity.”

⁸ See Colorado Data Privacy Act, 6-1-1303(10), C.R.S.; Connecticut Data Privacy Act, Section 1(12); Delaware Personal Data Privacy Act, Section 1(13); Indiana Consumer Data Protection Act, Section 11; Montana Consumer Data Privacy Act, Sec. 2, (10); New Jersey Act (S332), page 9, line 32; Oregon Consumer Privacy Act, Section 1(10); Tennessee Information Protection Act, 47-18-3201(10); Virginia Consumer Data Protection Act, Va. Code § 59.1-575.

⁹ House Bill 567 page 34, lines 3-10.

¹⁰ Compare HB 567, p.14, line 31 through page 15, line 12 with SB 541 page 14, line 30 through page 15, line 14.

§ 14-4605 Consumer Rights

- Page 19, lines 7-9: Both HB 567 and SB 541 provide consumers with appeal rights, but HB 567 clarifies that a controller must inform consumers whether their request has been complied with or denied, which allows consumers to determine whether they should invoke their appeal rights.

§ 14-4607

- Page 21, lines 18-20: This language ensures that consumers who would like content personalization have the opportunity to receive this feature, but that those who do not want content personalization do not have their data collected unnecessarily. It merely requires consumers to consent to content personalization. Senate Bill 541 removes individual choice by removing the consent requirement and permitting the collection of personal data for the sole purpose of content personalization.
- Page 22, lines 1-2: House Bill 567 provides more robust protections for children by prohibiting the sale of personal data of underage users.
- Page 23, line 19- page 24 line 4: House Bill 567 closes a loophole created in the loyalty program exemption.

§ 14-4612

- The Division is concerned that SB 541 adds a provision not found in HB 567 that disincentivizes controllers and processors from taking steps to ensure that third parties will not misuse the data. Senate Bill 541 (page 34, line 29 – page 35, line 4) protects controllers and processors from third-party violations unless the controller had “actual knowledge” at the time the data was disclosed that the recipient would violate SB 541. Given the use of companies overseas in countries that do not respect American law such a safe harbor poses a very real threat to both national security and individual privacy.

§ 14-4614

- The Division requests that the Finance Committee resist adding the right to cure found in Senate Bill 541, as the procedure unnecessarily codifies a process similar to the mediation process currently undertaken by the Consumer Protection Division when it receives a consumer complaint.

We respectfully ask the Senate Finance Committee give House Bill 567 a favorable report and not adopt the provisions from SB 541 about which the Division has expressed the concerns discussed above.

cc: Members, Finance Committee
The Honorable Sara Love

AdvaMed Written Testimony_MD HB 567_Senate Finance

Uploaded by: Roxy Kozyckyj

Position: FAV



March 20, 2024

Senator Pamela Beidle, Chair
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Senator Katherine Klausmeier, Vice-Chair
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

RE: HB 567, Maryland Online Data Privacy Act of 2024 – Adopt Senate Amendments on De-identified Data

Chair Beidle, Vice-Chair Klausmeier, and Members of the Committee,

AdvaMed appreciates the complex work before the committee and the overall effort of the sponsors to provide confidence to Maryland constituents that their data privacy is secured. HB 567 would provide the residents of Maryland with transparency and control over their personal data and provide new privacy protections. ***AdvaMed appreciates the opportunity to provide comments regarding HB 567 and respectfully requests that the committee adopt the language on de-identified data in the Senate companion bill.***

AdvaMed member companies produce the medical devices, diagnostic products, and digital health technologies (collectively, “Medical Technologies”) that are transforming health care through the potential for earlier disease detection, less invasive procedures, and more effective treatments. AdvaMed members range from the largest to the smallest medical technology innovators and companies. We are committed to ensuring patient access to lifesaving and life-enhancing devices and other advanced medical technologies in the most appropriate settings.

Adopt Senate Language on De-identified Data

AdvaMed recommends the committee adopt the Senate bill’s language on de-identified data or alternatively use the clarifying language also proposed below.

Senate amendment, SB 641:

(III) Information that is de-identified in accordance with the requirements for de-identification set forth in 45 C.F.R. 164.514 that is derived from individually identifiable health information as described in HIPAA or personal information consistent with the human subject protection requirements of the U.S. Food and Drug Administration.

OR



Supplement existing definition in HB 567:

§14-4601.

(A) In this subtitle the following words have the meanings indicated.

...

(P) “De-identified data” means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data does all of the following:

- (1) Takes reasonable measures to ensure that such data cannot be associated with an individual.
- (2) Commits in publicly available terms and conditions or in a publicly available privacy policy to maintain and use the information in de-identified form; and
- (3) Contractually obliges any recipients of the information to comply with all provisions of this subsection.

“De-identified data” also includes data de-identified in accordance with the requirements in 45 CFR 164 (HIPAA), where any recipients of such data are contractually prohibited from attempting to reidentify such data.

Why Unify De-identified Data Definition with HIPAA.

Data de-identified under HIPAA may not be considered “de-identified data” under this bill. Some patient data controlled or processed by medtech companies is de-identified under the HIPAA and transmitted for analysis, research, development, or some other essential health care purpose. AdvaMed recommends adding a clarifying provision so that data de-identified under HIPAA can continue to be used for analysis, private research, and development that can advance scientific understanding and lead to improvements in care and innovative solutions. This can be accomplished by incorporating the Senate’s language OR supplementing the definition of “de-identified data” with an additional sentence, as shown by the blue underlined text below.

Conclusion

AdvaMed appreciates this opportunity to offer comments. To date, fourteen states have passed their data privacy reform laws that include amendments similar to those requested above. Most recently, New Hampshire passed legislation inclusive of all key healthcare exemptions that allow healthcare delivery, research, and patient privacy to interact and proceed unimpeded. We encourage the committee to follow suit and ensure that there continues to be alignment across the country with respect to data privacy.



Thank you, Chair Beidle and Vice-Chair Klausmeier, for your consideration of our recommendations. We welcome any opportunity to serve as a resource, especially as it relates to medtech data privacy and security. If you have any questions or need additional information, please contact rkozyckyj@advamed.org.

Respectfully submitted,



Senior Director, State Government and Regional Affairs
AdvaMed



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

HB0567 (1).pdf

Uploaded by: Suzanne Price

Position: FAV

Maryland Online Data Privacy Act of 2024.

If HB0567 is truly going to protect the privacy of Maryland citizens then I am all for it, if it is a farce to push something else then I would not support it. So often these bills intentionally use titles to trick the public into believing they are supporting something good when in reality it is not.

Suzanne Price
Annapolis, MD

_HB567 Written Testimony Crossfile FAV 2024.pdf

Uploaded by: Zoe Gallagher

Position: FAV



HB567 Maryland Online Data Privacy Act of 2024

Position: Favorable

3/21/2024

The Honorable Senator Pamela Beidle, Chair
Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

CC: Members of the Senate Finance 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>

MSFT FWA HB576.pdf

Uploaded by: Keith Walmsley

Position: FWA

Testimony in Support of House Bill 576:
Maryland Online Data Privacy Act of 2024
Favorable With Amendments

March 21, 2024

Chair Beidle and distinguished members of the Finance Committee, it is my pleasure to offer testimony in favor with amendments for **House Bill 576: Maryland Online Data Privacy Act of 2024**. If enacted, this bill would provide the strongest consumer data privacy law in the country. Our amendments would maintain that standard.

We at Microsoft applaud you for advancing data privacy legislation. At Microsoft, we have long taken the privacy of our customers seriously, and we have a long track record of supporting responsible, thoughtful reform.

The data minimization provisions would hamstring research and innovation. They prohibit companies from collecting any personal data unless it “is reasonably necessary and proportionate to provide or maintain a specific product or service requested by [a] consumer”.

As drafted these sections would seriously hinder our ability to improve or create new, innovative technologies. People expect their technology to improve. They like to receive new products, features, and services. As terrific as Microsoft Word was in 1998, people like it much better with updated features like Track Changes, Sharing Documents, or the ability to insert links or photos. It would inhibit our ability to create services like Microsoft Reading Coach, which helps teachers accelerate students’ ability to learn,¹ or to build services like Seeing AI, which narrates the world for people with vision impairments.² All of that innovation relies upon data.

We also acknowledge that some have expressed concerns that the data minimization provisions in existing privacy laws, which mostly require companies to limit their data collection to the purposes outlined in their privacy policies, are not strong enough and that companies should face stricter guardrails about what they can and cannot collect.

We would ask the committee to consider, instead, tying companies’ data minimization obligations to **consumer’s reasonable expectations**. In other words, companies would be obligated to **“limit the collection of personal data to what is reasonably necessary and proportionate to:**

- (1) provide or maintain a product or service requested by the consumer to whom the data pertains; or;**
- (2) a consumer’s reasonable expectations considering the context in which the personal data is collected and the relationship between the consumer and the controller.**

This approach provides a sensible alternative. It would be **much stronger** than the minimization provisions in other laws because it would prevent companies from setting the terms of their own

¹ For more on Microsoft Reading Coach, see: <https://www.youtube.com/watch?v=fHZdcLxdzFQ>.

² For more on Seeing AI, see: <https://www.microsoft.com/en-us/garage/wall-of-fame/seeing-ai/>.

data collection and from hiding abusive data collection practices in lengthy privacy policies. It would also be more flexible than the bill's current language, addressing concerns that the current minimization provisions are too rigid and will hamper innovation, because it would tie companies' obligations to consumer expectations—expectations which will invariably differ in different contexts.

In addition, we recommend that the minimization provisions be applied not to processors, but to controllers, as originally drafted. By applying the minimization provisions to processors, the bill diverges from 30 years of privacy law and threatens to undermine the legal protections that have permitted all governments, organizations, and businesses large and small to use enterprise cloud services.

For several important reasons, privacy laws globally have long differentiated between the obligations that apply to “controllers” and those that apply to “processors.” Under that framework, the controller is the entity that “determines the purposes and means” of processing personal data. In other words, it is calling the shots about what's being collected, how it's being used or shared, and why. It is typically the entity that has a relationship with consumers, and it is directly responsible for satisfying consumers' requests to exercise their privacy rights

The processor is only permitted to process personal data pursuant to the instructions given it by the controller in a binding contract. The processor cannot call the shots about what is done with (or “determine the purposes and means” of processing) personal data. If it did so, it would not only violate the law and its contract with the controller, but it would itself become a controller (and therefore on the hook for complying with all of the obligations that apply to controllers). The processor's obligations are, among other things, to ensure that the controller can comply with its obligations under the law.

These roles are function- and context-specific, which means that the same corporate entity could be serving as a controller in one scenario but a processor in another.

This concept—the controller/processor distinction—has been critical to provide assurances to all customers, including governments, nonprofits, and businesses large and small, that if they decide to move their data to an enterprise cloud service, the data will remain the customer's, and the cloud service will not start rifling through it or using it for its own purposes. Without the concept, the entire system of enterprise cloud services could come crashing down.

For these reasons, we recommend:

Removing the “Or Processor” amendments attached by the House at various points throughout, conforming it in this instance to the Senate bill.

We ask you to humbly consider our suggested amendments and look forward to dully supporting the amended bill. We urge a report of Favorable With Amendment.

2024-3-20_CCIA Comments on MD HB 567.pdf

Uploaded by: Khara Boender

Position: FWA



March 20, 2024

Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

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

Dear Chair Beidle and Members of the Senate Finance Committee:

On behalf of the Computer & Communications Industry Association (CCIA)¹, I write to respectfully oppose HB 567, unless further 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 and continued 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’ extensive work on this bill, as written, HB 567 still would diverge from existing frameworks in several key ways, as further detailed below. We appreciate your consideration.

Definitions and controller obligations should be clear and interoperable.

CCIA appreciates the harmonization of the definitions for “targeted advertising” and “publicly available information”, however, further amendments would help to address persisting divergences.

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>

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 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", and "consumer health data". 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.

Finally, HB 567 would require a controller to obtain consumer consent prior to collecting personal data for content personalization or marketing. This provision would 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. Personalization is also essential to the core value of the internet, and without it, online services would be far less efficient, and possibly unusable. Further, personalization serves a very different purpose than marketing – personalization helps online businesses create a safer and more enjoyable online experience from their users. The frameworks established in other states, such as Connecticut and Virginia address such exemptions. For example, Virginia's law includes the following under § 59.1-582, and CCIA recommends considering similar language:

The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to:

- 1. Conduct internal research to develop, improve, or repair products, services, or technology;*
- 2. Effectuate a product recall;*
- 3. Identify and repair technical errors that impair existing or intended functionality; or*
- 4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.*



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.

* * * * *

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

Crossover FavWAmEd AHA Data Privacy HB 567.pdf

Uploaded by: Laura Hale

Position: FWA



March 30th, 2024

Testimony of Laura Hale
American Heart Association

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

Dear Chair Beidle, Vice Chair Klausmeier and Honorable Members of the Finance 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:

"Address privacy concerns of donors by

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

- 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.

MD HB 567 FWA 3-20.pdf

Uploaded by: Laura Srebnik

Position: FWA



Biotechnology Innovation Organization
1201 New York Ave NW
Suite 1300
Washington, DC, 20005

March 20, 2024

The Honorable Pamela Beidle, Chair
Senate Committee on Finance
Miller Senate Office Building, 3 East Wing
11 Bladen St., Annapolis, MD 21401 – 1991

RE: **FWA – HB 567 Maryland Online Data Privacy Act**

Dear Chair Beidle and Members of the Committee:

The Biotechnology Innovation Organization (BIO) would firstly like to thank the Committee for adopting BIO's proposed amendments to the Senate crossfile of this bill, SB 541. BIO previously submitted proposed amendments in written testimony for the House and Senate Hearings. BIO would therefore ask that the Finance Committee vote HB 567 FWA adopting the same amendments proposed by BIO that this Committee adopted to the Senate crossfile, SB 541.

BIO is the world's largest trade association representing biotechnology companies, academic institutions, state biotechnology centers, and related organizations across the United States and in more than 30 other nations. BIO members develop medical products and technologies to treat patients afflicted with serious diseases, to delay the onset of these diseases, or prevent diseases from occurring.

Here is where the amendments would be placed in the House version of the bill:

AMENDMENT NO. 1

On Page 3 in line 25 strike "CAN BE" and substitute "**ARE**".

14-4601.

(2) "BIOMETRIC DATA" INCLUDES:

(i) A FINGERPRINT;

(ii) A VOICE PRINT;

(iii) AN EYE RETINA OR IRIS IMAGE; AND

(iv) ANY OTHER UNIQUE BIOLOGICAL CHARACTERISTICS THAT ~~CAN BE~~ **ARE USED TO**

UNIQUELY AUTHENTICATE A CONSUMER'S IDENTITY.

Rationale - Overly broad. Biometric data should be limited to *data that are used the authenticate* identity, as opposed to *data that can be used to authenticate* identity. This amendment would narrow the application for that purpose. Illinois BIPA biometric information privacy act [740 ILCS 14/section 10](#), and Washington Chapter [19.375](#) RCW [19.375.010](#) (1). The majority of state biometric privacy laws are modeled after BIPA.

AMENDMENT NO. 2

On page 15 in line 12, after "**HIPAA;**" insert "**AND**

(III) INFORMATION THAT IS DE-IDENTIFIED IN ACCORDANCE WITH THE REQUIREMENTS FOR DE-IDENTIFICATION SET FORTH IN 45 C.F.R. 164.514 THAT IS DERIVED FROM INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION AS DESCRIBED IN HIPAA OR PERSONAL INFORMATION CONSISTENT WITH THE HUMAN SUBJECT PROTECTION REQUIREMENTS OF THE U.S. FOOD AND DRUG ADMINISTRATION;

Rationale – We recommend expanding the definition of 'de-identified data' to include data de-identified according to HIPAA standards. HIPAA's framework streamlines data gathering, empowers patients to control their PHI, and promotes healthcare research and innovation. While HB 567 aligns with many aspects of HIPAA, it lacks the de-identification standard crucial for harmonizing data collection practices among our members for research.

Maintaining adherence to current HIPAA and research requirements is essential for BIO members. HIPAA provides clear guidelines for PHI use and disclosure, balancing patient privacy with research needs. Its de-identification standard ensures secure and private use of healthcare data for research purposes.

Excluding this standard would pose operational challenges for biomedical research companies in Maryland. This aligns with consumer privacy laws in 12 out of 13 states with HIPAA de-identification provisions.

California – [CCPA](#) – Section 179.146(a)(4)(A)(i)

Colorado – [SB 190 2021](#) – 6-1-1304 (1)(g)(I)

Connecticut – [CT Personal Data Privacy Act](#) – Section 3(b)(8)

Indiana – [Consumer Data Protection Act](#) - Section 2(6)

Iowa – [SF 262 \(2023\)](#) - Section 2 (3)(j)

Montana – [SB 0284 2023](#) – Section 4(1)(i)

New Hampshire – [SB 255](#) 507-H:3 II(h)

Oregon – [SB 619 2023](#) – Section 1(11)(a), (b), (A), (B) – OR legislation tracks closely to our proposed MD amendment altering definition of deidentified data

Tennessee – [HB 1181 2023](#) – 47-18-3210 (a)(13)

Texas – [Data Privacy and Security Act](#) – 541.003 (7)

Utah – [SB 0227 2022](#) – 13-61-102(2)(g)(ix)(A),(B)

Virginia – [H 2307 2021](#) Consumer Data Protection Act – 59.1-576(C)(7)

Thank you for the opportunity to comment and we urge the Committee to pass with these amendments included. Please do not hesitate to contact us for any further information.

Sincerely,

/s/

Laura Srebnik

Director, State Government Affairs – Eastern Region

The Biotechnology Innovation Organization (BIO)

1201 New York Ave., NW

Suite 1300

Washington, DC 20005

206.293.1195 (mobile)

National Insurance Crime Bureau One Pager UPDATED.

Uploaded by: Philemon Kendzierski

Position: FWA

National Insurance Crime Bureau – SB 541 / HB 567

The National Insurance Crime Bureau (NICB) is a nonprofit organization that works with state and local law enforcement, the Maryland Insurance Administration (MIA), and member insurance companies to detect, prevent and deter insurance crimes.

NICB respectfully requests an amendment to SB 541/HB 567 to ensure that existing insurance fraud detection operations are not inhibited by the passage of this legislation. This amendment was included in SB 541, and we request that the House conform with this change.

- **NICB is already recognized by provisions of Maryland Law** designed to avoid interference with insurance fraud detection and investigation.
 - Md. Insurance Code § 27-802(c)(iii) grants immunity from civil liability to NICB for reporting suspected insurance fraud.
- Currently, provisions of SB 541 / HB 567 (§14-4612 on page 31) protect NICB’s ability to cooperate with law enforcement agencies.
 - However, as introduced, SB 541 / HB 567 would have required NICB to respond to consumer requests for the deletion of personal data (§14-4605).
- While SB 541/HB 567 as introduced would have allowed NICB to deny a request to delete personal data related to a fraud investigation¹, **NICB’s obligation to respond to the consumer would expose otherwise covert insurance fraud investigations and alert a criminal they may be the subject of an investigation².**
- The addition of a narrow entity exemption for NICB, that was included in the final version of SB 541, is consistent with the language, intent, and spirit of the insurance fraud immunity statute³, and would allow NICB to carry out our fraud-fighting mission unhindered.
 - Other states, most recently Delaware, have recognized this need and provided specific entity exemptions for NICB to continue their work.
- NICB respectfully requests that HB 567 conform to SB 541 by amending the bill as follows:

Proposed Amendment:

(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*

¹ Under §14-605(B)(4) with proposed amendments, when NICB is faced with a request by a consumer to delete personal data relating to a fraud investigation for which that consumer is a suspect, NICB would **not** be permitted to delete the data as it relates to an active investigation.

² Under §14-605(B)(1) with proposed amendments, NICB would be required to acknowledge to the subject of an investigation that NICB was processing the consumer’s data, potentially tipping off the subject to their being investigated for insurance fraud.

³ Md. Insurance Code § 27-802/ COMAR 31.04.15.05 requires insurance companies to report suspected insurance fraud to the MIA’s Fraud Division. Member insurance companies utilize NICB’s Fraud Bureau Reporting Program to comply this requirement. NICB shares this data with the Fraud Division.

NICB Letter for HB 567 Senate - MD Online Privacy

Uploaded by: Philemon Kendzierski

Position: FWA



March 30, 2024

The Honorable Pamela Beidle and Members of the Committee
Senate Finance Committee
Maryland General Assembly

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

Dear Chair Beidle 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. **We respectfully request for House Bill 567 to be conformed with the Senate version and the inclusion of the following exemption amendment:**

(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.

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 Senate Bill 541 and News Sections of Articles 13 and 14 of the Annotated Code of Maryland

Senate Bill 541 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 S.B. 541 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 S.B. 541 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.

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,

A handwritten signature in black ink, appearing to read 'Eric M. De Campos', with a long horizontal line extending to the right.

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

2024 HB0567 Testimony Against 2024-03-21.pdf

Uploaded by: Alan Lang

Position: UNF

Testimony Against HB0567

Please vote against HB0567 for the following reasons.

- It is too long and difficult to follow so that one can determine the possible benefits (for example, how well does it augment existing law such as the Maryland Personal Information Protection Act and the Maryland Consumer Protection Act)
- The bill imposes these restrictions on businesses, but does not require compliance by State and local agencies or courts that may capture similar data
- It may require hiring staff for implementation.
- It will establish a significant regulatory framework over online and biometric data, which could meaningfully affect any small business subject to this bill.

Alan Lang
242 Armstrong Lane
Pasadena, MD 21122
410-336-9745
Alanlang1@verizon.net

HB 567 - UNF - MHLA.pdf

Uploaded by: Amy Rohrer

Position: UNF

MHLA

Maryland Hotel Lodging Association

Testimony in Opposition to HB 567
Maryland Online Data Privacy Act of 2024
March 21, 2024 – Senate Finance Committee

The Maryland Hotel Lodging Association (MHLA) serves as the sole statewide trade association dedicated to advocacy for Maryland’s 750+ hotels. Our industry employs more than 25,000 individuals and provides the state with \$1 billion in state and local taxes, \$5 billion in total wages and salaries, and \$9 billion in total gross domestic product.

We are supportive of measures to enhance data privacy and our members did not express concerns with HB 567 as introduced. However, amended language added under **14-4607** (p. 23, line 19 – p. 24, line 3) has caused significant concern by major hotel brands across the country and is the reason for our strong opposition to the bill in its current form.

Hotel loyalty programs are voluntary and transparent with customers informed of the benefits offered and the data sharing involved through disclosure prior to opting in. The bill’s numerous disclosure and opt-out obligations regarding data sales and transfers to third parties would apply to loyalty programs, which makes the punitive restrictions added by amendment, as referenced above, unfair and unnecessary. Holding loyalty programs to a substantially higher standard than other controllers (i.e. data brokers, social media companies, or metasearch companies) does not make sense from either a practical or a policy perspective.

Please note that MHLA has signed onto a joint statement of opposition (submitted separately) further outlining our concerns with HB 567. As noted in the joint statement, **we urge you to exclude the unworkable language added to the loyalty programs clause by amendment to HB 567, and instead adopt the language provided in the Senate’s companion bill SB 541 that properly preserves *bona fide* customer loyalty programs.**

Respectfully submitted,

Amy Rohrer
President & CEO
Maryland Hotel Lodging Association

SPSC - MD HB 567 (Omnibus) - Testimony 03.20.pdf

Uploaded by: Andrew Kingman

Position: UNF

STATE PRIVACY & SECURITY COALITION

March 20, 2024

Chair Pamela G. Beidle
Vice Chair Katherine A. Klausmeier
Senate Committee on Finance
Miller Senate Office Building
3 East Wing, 11 Bladen St.
Annapolis, MD 21401-1991

Re: Comprehensive Privacy (HB 567) – Unfavorable

Dear Chair Beidle, Vice Chair Klausmeier, 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 writes with three specific amendments to HB 567, in addition to conforming the bill with its Senate companion. We appreciate that Maryland is taking a comprehensive approach to privacy legislation and respectfully request amendments that prevent this bill from depriving consumers of control over their sensitive data, access to new products or features, and that will better protect minors' privacy.

This committee has clearly worked hard to make SB 541 better. The changes made prior to the committee voting the bill out were critical changes that will make providing strong privacy protections to consumers clearer. We would encourage the committee to align HB 567 with SB 541, including:

- Conforming the definition of "Biometric Data" to that in SB 541;
- Striking the prohibition on content personalization;
- Removing the phrase "or processors" where it was added in the House amendments;
- Adding a Right to Cure

Data Minimization: §14-4607(a)(2) and (b)(1)(I)

The data minimization provisions will cause Maryland consumers to have a radically different experience than any other US or EU citizen. The data minimization language found in the current draft ***does not give consumers the ability to say "I don't want you to collect my sensitive data."***

As currently drafted, the data minimization provisions allow businesses to collect whatever information they deem "strictly necessary" (if sensitive) or "reasonably necessary" (if non-sensitive), with no ability for the consumer to control such data. ***This is detrimental to Maryland consumers and businesses alike.*** Instead, there should be a clear standard of opt-in consent for sensitive data, with clear rules around how a business can use that data (data minimization language from the CA/GDPR/CT frameworks), and when they are limited for using such data for additional purposes (purpose limitation language from the CA/GDPR/CT frameworks).

STATE PRIVACY & SECURITY COALITION

The current language is a departure from – and is not interoperable with – data minimization provisions in the CA, GDPR, and CT frameworks. Put simply, ***570 million consumers are covered by the data minimization provisions in these frameworks; there are zero consumers covered under the framework Maryland proposes.***

The ramifications of taking a novel approach are likely to be significant. Without moving to the historically vetted, universal data minimization framework found in all other significant privacy frameworks, Maryland consumers cannot get access to new features or services unless they request them, and even then, the current language will make it more difficult for businesses to let them know these new features exist. This will isolate Maryland consumers without providing additional privacy protections for them.

The consumer experience in Maryland will likely differ from all other states in noticeable ways for everyday products and services, such as:

- Using data to predict or identify disease outbreaks in population clusters (because a consumer is unlikely to specifically request this use of their data).
- Using mapping or geolocation to help facilitate everyday services like ridesharing or tracking packages for delivery because it is not “strictly necessary” for the consumer’s use of the product;
- Reaching existing customers or finding new ones via online advertising, because such data can only be processed in the context of a product or service specifically requested by the consumer; and
- Automatically updating a calendar’s time zone when traveling to and from Maryland, because a consumer does not specifically request it;
- Introducing features such as email improvements (like “nudges” for emails that need follow-up or a response), because a consumer does not specifically request it.

We have attached our suggested language for the committee’s consideration.

Standard of Knowledge for Minor Data

The standard of knowledge laid out in the current draft requires that controllers “know or should have known” that a consumer is under 18 years old. This standard is an unusual one that departs significantly from the “actual knowledge or willful disregard” standard found in most other states with similar political dynamics (states with a different formulation have adopted an “actual knowledge” standard only).

The standard laid out in the current draft creates similar problems around age verification that we have raised previously in other contexts, and that organizations like the ACLU, NY Times, and GLAAD have also raised. Such a standard could effectively require websites that provide targeted advertising to consumers to verify the age of all consumers. We do not believe this is a pro-privacy stance for Maryland consumers, and businesses do not want to collect this type of sensitive information if they do not have to.

STATE PRIVACY & SECURITY COALITION

We would recommend that the standard be amended to reflect the “actual knowledge and willful disregard” standard that is conventional and provides the same protections without the negative privacy implications. Again, we have attached the suggested amendments.

Data Protection Assessments for “Each Algorithm Used”

This would be a new standard that no other state has enacted, and with good reason: requiring that a data protection assessment (DPA) include an assessment for each algorithm used would run this document to tens of thousands of pages; even a simple spreadsheet can contain scores of algorithms that it is running. This requirement would be a massive compliance issue with no corresponding consumer benefit.

The current framework already ***already requires assessment of automated processing around consumer data that covers a “reasonably foreseeable risk” of:***

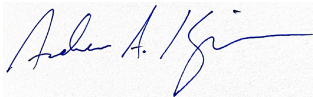
- Unfair/abusive/deceptive treatment of a consumer;
- Unlawful disparate impact on a consumer
- Financial/physical/reputational injury to a consumer
- Physical or other intrusion on the solitude or seclusion or the private affairs or concerns of a consumer in which the intrusion would be offensive to a reasonable person; or
- Other substantial injury to a consumer.
- The existing language ensures that any processing activity around automated processing (including algorithms and AI) that could negatively impact a consumer are already considered; the language we propose deleting is unnecessary and provides no benefit to consumer privacy.

We have attached this proposed amendment as well.

Lastly, we point out what we believe is a typo at the end of the bill – Section 2 of the bill states that the exemptions section would not come into effect until April 1, 2026. Given that this section is intended to operate in conjunction with the rest of this bill, we would simply request that the April 1, 2026 date be moved to the October 1, 2025 effective date of this bill.

SPSC members believe that consumers and businesses alike are best served by strong privacy protections that do not isolate consumers and provide clear compliance requirements for businesses. We would be happy to discuss any of these issues further if helpful.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

STATE PRIVACY & SECURITY COALITION

SUGGESTED AMENDMENTS

Data Minimization

14-4607(a)(2): A controller or processor may not:

~~EXCEPT WHERE THE COLLECTION OR PROCESSING IS STRICTLY~~

~~2 NECESSARY TO PROVIDE OR MAINTAIN A SPECIFIC PRODUCT OR SERVICE~~

~~3 REQUESTED BY THE CONSUMER TO WHOM THE PERSONAL DATA PERTAINS AND~~

4 ~~UNLESS THE CONTROLLER OBTAINS THE CONSUMER'S CONSENT~~, COLLECT,

5 PROCESS, OR ~~SHARE~~ **SELL** SENSITIVE DATA CONCERNING A CONSUMER **UNLESS THE CONTROLLER OBTAINS THE CONSUMER'S CONSENT**;

14-4607(b)(1)(I): A controller or processor shall:

6 (I) **LIMIT THE COLLECTION OF PERSONAL DATA TO WHAT IS**

7 **ADEQUATE, RELEVANT, AND REASONABLY NECESSARY AND PROPORTIONATE IN RELATION TO THE PURPOSES FOR WHICH SUCH DATA IS PROCESSED, AS DISCLOSED TO** ~~TO PROVIDE OR MAINTAIN A~~

~~8 SPECIFIC PRODUCT OR SERVICE REQUESTED BY~~ THE CONSUMER TO WHOM THE

9 DATA PERTAINS;

Children's Knowledge Standard

14-4607(5): A controller or processor may not:

PROCESS THE PERSONAL DATA OF A CONSUMER FOR THE PURPOSES OF TARGETED ADVERTISING IF THE CONTROLLER ~~KNEW OR SHOULD HAVE KNOWN~~ **HAS ACTUAL KNOWLEDGE OR WILLFULLY DISREGARDS** THAT THE CONSUMER IS AT LEAST 13 YEARS OLD AND UNDER THE AGE OF 18 YEARS;

14-4607(6): A controller or processor may not:

SELL THE PERSONAL DATA OF A CONSUMER WITHOUT THE CONSUMER'S CONSENT IF THE CONTROLLER ~~KNEW OR SHOULD HAVE KNOWN~~ **HAS ACTUAL KNOWLEDGE OR WILLFULLY DISREGARDS** THAT THE CONSUMER IS AT LEAST 13 YEARS OLD AND UNDER THE AGE OF 18 YEARS;

DPA Algorithms

14-4610(B)

A CONTROLLER SHALL CONDUCT AND DOCUMENT, ON A REGULAR

17 BASIS, A DATA PROTECTION ASSESSMENT FOR EACH OF THE CONTROLLER'S

18 PROCESSING ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM TO A

19 CONSUMER, ~~INCLUDING AN ASSESSMENT FOR EACH ALGORITHM THAT IS USED.~~

HB567_MRA_UNF PDF.pdf

Uploaded by: cailey locklair

Position: UNF

MARYLAND RETAILERS ALLIANCE

The Voice of Retailing in Maryland



HB567 Maryland Online Data Privacy Act of 2024 Finance Committee March 21st, 2024

Position: Unfavorable

Comments: The Maryland Retailers Alliance (MRA) is opposed to changes and omissions that were made to HB567 during the legislative process in the House of Delegates. We would urge the committee to reject this amended bill as presented and amend it to match the Senate's work on SB571 with some small additional amendments. We would recommend changes in the following policy areas. Thank you for your consideration.

1. Customer Loyalty Plan Provisions

- REQUESTED AMENDMENT:
 - STRIKE ALL REVISIONS IN REPRINT PG. 23, LINES 19-3 ON THE NEXT PAGE; REVERT LANGUAGE TO ORIGINAL FORM.
- REASONING:
 - The State should protect the right of Maryland consumers and retailers to have loyalty programs on the terms they choose so long as the programs are bona fide. The State should not be in the business of writing customer loyalty programs, especially because customers have to opt-in to participate in them.
 - Although the House bill would permit controllers outside of a loyalty program to sell data or use it for targeted advertising without an opt-in from the consumer, it would prohibit controllers that operate bona fide loyalty programs – which can be joined only with an opt-in – from making the same transfer in their loyalty program. This is inconsistent and unpredictable public policy, injecting confusion and uncertainty into the law.
 - We oppose the revised language in the bill that would prevent Maryland consumers from enjoying the same benefits from participating in retailers' loyalty plans that consumers would have in all other states. The bill should revert to the previous language of this section that we could support.

2. Cross Liability Protections

- REQUESTED AMENDMENT (previously requested by MRA in letter dated Feb. 14):
 - Page 35, LINE 11-15, inclusive – STRIKE AND REPLACE WITH:

“A controller or processor that discloses personal data to a processor or third party in accordance with this subtitle shall not be deemed to have violated this subtitle if the processor or third party that receives and processes such personal data violates this subtitle, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third party would violate this subtitle. A third party or processor receiving personal data from a controller or processor in compliance with this subtitle is likewise not in violation of this subtitle for the transgressions of the controller or processor from which such third party or processor receives such personal data, provided, at the time the receiving processor or third party did not have actual knowledge that the disclosing controller or processor would violate this subtitle.”

- REASONING:
 - The protection provided to third party controllers or processors in 14-4611(D) needs to run both ways to also 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 that the processor or third party intends to violate the law with the consumer data received from the controller.
 - We urge the committee to provide common-sense liability protections to protect controllers that are complying with the law from being held liable for violations by processors or third parties, and the suggested language above (modeled on liability protection language adopted in other state privacy laws) ensures that all parties have the same cross-protections.

3. **Data Minimization**

- **REQUESTED AMENDMENT:**
 - PG. 21, lines 18-20: Strike in its entirety section 14-4607(A)(1)
 - PG. 21, line 21-22: Strike “strictly necessary” and replace with “reasonably necessary”
- **REASONING:**
 - No state has passed opt-in requirements for targeted advertising. All states operate on an opt-out basis which is a pro-consumer, pro-business decision that makes sense.
 - The definition of sensitive data includes things that could be implied about a person based on purchases or clicks on certain items (for example, race based on cosmetic choices or religion based on holiday celebration items), but this information is based on assumptions made by technological assessments of online activity. Basing laws on possible inferences about a person based on their online research or retail purchases is inappropriate and problematic.

4. **Private Right of Action**

- **REQUESTED AMENDMENT:**
 - We urge the committee to insert language that makes it clear that the law does not authorize private right of action. We would request the following: “Nothing in this bill shall be construed as providing the basis for, or subject to a private right of action.”
 - We urge the committee to insert a right to cure in HB567 in the same form as the Senate bill. This is critical to the many small businesses across the state who are not familiar with data privacy laws and may need an opportunity to correct a disclosure to a consumer.

MD HB 567 Joint Opposition Letter.pdf

Uploaded by: cailey locklair

Position: UNF



Statement of Opposition to HB 567

March 18, 2024

The undersigned organizations write to express our opposition to HB 567, the Maryland Online Data Privacy Act of 2024. Unlike every other U.S. state privacy law, this House bill as drafted would deprive Marylanders (but not the residents of other states) of their right to choose among a wide variety of customer loyalty programs offered by all types of businesses, frustrating their voluntary choices and desire for benefits, and hurting Maryland businesses. **We strongly urge conferees to exclude the unworkable language added to the loyalty programs clause by amendment to HB 567, and instead adopt the language provided in the Senate's companion bill SB 541 that properly preserves *bona fide* customer loyalty programs.**

Loyalty programs are a critical and ever-growing facet of today's business models employed by Maryland companies in a range of industries, including restaurants, retailers, hotels, and other sectors. Today, nearly 50% of restaurants currently offer a customer loyalty program of some kind and the vast majority of retailers employ these voluntary programs where consumers choose to receive discounts by opting into them. These programs are not their principal business model but rather are designed to provide discounts or rewards to their best customers to encourage future engagement. Further, these programs are already inherently privacy-protective because they typically require customers to affirmatively opt into the plan in order to receive discounts, rewards, or other benefits as a member of the program.

More importantly, it is clear that consumers overwhelmingly want these programs to remain legal.¹ Generally, most states that have enacted omnibus privacy laws contain language similar to SB 541 providing appropriate antidiscrimination provisions while also sufficiently preserving these programs. However, including the amendment with additional data-sharing limitations within HB 567 would result in Maryland becoming the first state in the nation to threaten loyalty programs.

¹ According to a survey conducted by Bond Brand Loyalty Inc., 79% of consumers say loyalty programs make them more likely to continue doing business with brands that offer them and 32% of consumers strongly agree that a loyalty program makes their brand experience better. Bond Brand Loyalty Inc., The Loyalty Report (2019) available at https://cdn2.hubspot.net/hubfs/352767/TLR%202019/Bond_US%20TLR19%20Exec%20Summary%20Launch%20Edition.pdf.

Specifically, HB 567 creates duplicative limitations on loyalty programs that are unnecessary because these businesses' loyalty plans already must comply with the bill's numerous disclosure and opt-out obligations regarding data sales and transfers to third parties. Even worse, the language effectively restricts these voluntary and transparent loyalty programs that protect consumer privacy more than uses of data that do not first require a consumer's opt-in after disclosure. As a result, HB 567 would ultimately impose the highest level of regulation **only** on Main Street businesses offering loyalty programs while continuing to permit other companies to sell or share data with less restriction under the bill.

In these respects, HB 567 goes far beyond the loyalty plan language within all other state privacy laws currently in effect and would inhibit the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships.

We appreciate lawmakers' interest in ensuring there are no unwarranted exemptions from the bill's existing requirements on data-sharing and transfers to third parties. The loyalty language of SB 541 does not exempt businesses with loyalty plans from the bill's existing protections. Rather, SB 541 clarifies that its *anti-discrimination* provisions do not prevent offering loyalty plan price discounts or preferred service.

We have significant concerns that Maryland consumers will be immensely frustrated if they were to lose points or benefits from loyalty programs they belong to and enjoy in other states. We therefore urge conferees to permit businesses serving Maryland consumers to offer loyalty programs they support and benefit from by adopting the language within SB 541.

Thank you for your attention to this important matter.

Sincerely,

Maryland Hotel Lodging Association
Maryland Retailers Alliance
NFIB in Maryland
Restaurant Association of Maryland

MSPC Ltr re MD HB 567 (Loyalty) - Mar 18 2024.pdf

Uploaded by: cailey locklair

Position: UNF



March 18, 2024

Members of the Conference Committee on HB567/SB541
Maryland General Assembly
Legislative Services Building
90 State Circle
Annapolis, MD 21401

Re: Customer Loyalty Program Treatment in HB567/SB541

Dear House and Senate Conferees:

The Main Street Privacy Coalition (MSPC), a coalition of 20 national trade associations representing more than a million American businesses,¹ writes to express our opposition to HB 567, the Maryland Online Data Privacy Act of 2024. Unlike every other U.S. state privacy law, this House bill as drafted would deprive Marylanders (but not the residents of other states) of their right to choose among a wide variety of customer loyalty programs offered by all types of Main Street businesses, frustrating consumers' voluntary choices and desire for benefits, and hurting Maryland businesses. **We strongly urge conferees to exclude the unworkable language added to the loyalty programs clause by amendment to HB 567, and instead adopt the language provided in the Senate's companion bill SB 541 that properly preserves *bona fide* customer loyalty programs.**

The MSPC members represent a broad array of companies that line America's Main Streets. From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, including franchise establishments, MSPC member companies interact with consumers day in and day out. Our members' businesses can be found in every town, city and state in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities. Collectively, the industries that MSPC trade groups represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing \$4.5 trillion (or 21.8%) to the U.S. gross domestic product.

Loyalty programs are a critical and ever-growing facet of today's business models employed by Maryland companies in our industry sectors. These programs are not their principal business model but rather are designed to provide discounts or rewards to their best customers to encourage future engagement. Further, these programs are already inherently privacy-protective because they typically require customers to affirmatively opt into the plan in order to receive discounts, rewards, or other benefits as a member of the program.

More importantly, it is clear that consumers overwhelmingly want these programs to remain legal.² Generally, most states that have enacted omnibus privacy laws contain language similar to SB 541, providing appropriate antidiscrimination provisions while also sufficiently

¹ The Main Street Privacy Coalition website and member list may be accessed at: <https://mainstreetprivacy.com>.

² According to a survey conducted by Bond Brand Loyalty Inc., 79% of consumers say loyalty programs make them more likely to continue doing business with brands that offer them and 32% of consumers strongly agree that a loyalty program makes their brand experience better. Bond Brand Loyalty Inc., The Loyalty Report (2019) available at https://cdn2.hubspot.net/hubfs/352767/TLR%202019/Bond_US%20TLR19%20Exec%20Summary%20Launch%20Edition.pdf.

preserving these programs. However, the House amendment language within HB 567 would result in Maryland becoming the first state in the nation to threaten loyalty programs.

Specifically, HB 567 creates duplicative limitations on loyalty programs that are unnecessary because these businesses' loyalty plans already must comply with the bill's numerous disclosure and opt-out obligations regarding data sales and transfers to third parties. Even worse, the language effectively restricts these voluntary and transparent loyalty programs that protect consumer privacy more than uses of data that do not first require a consumer's opt-in after disclosure. As a result, HB 567 would ultimately impose the highest level of regulation **only** on Main Street businesses offering loyalty programs while continuing to permit other companies to sell or share data with less restriction under the bill.

In these respects, HB 567 goes far beyond the loyalty plan language within all other state privacy laws currently in effect and would inhibit the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships.

We appreciate lawmakers' interest in ensuring there are no unwarranted exemptions from the bill's existing requirements on data-sharing and transfers to third parties. Importantly, the loyalty language of **SB 541 does not exempt businesses with loyalty plans** from the bill's existing protections. Rather, SB 541 clarifies that its *anti-discrimination* provisions do not prevent offering loyalty plan price discounts or preferred service.

We have significant concerns that Maryland consumers will be immensely frustrated if they were to lose points or benefits from loyalty programs they belong to and enjoy in other states. We therefore urge conferees to permit Main Street businesses serving Maryland consumers to offer them the same loyalty programs they support and benefit from in all other states by adopting the language within SB 541.

Thank you for your attention to this important matter.

Sincerely,

Main Street Privacy Coalition

UNF-Maryland Online Data Privacy Act of 2024-MTC-C

Uploaded by: Drew Vetter

Position: UNF



TO: The Honorable Pam Beidle, Chair
Members, Senate Finance Committee
The Honorable Sara Love

FROM: Kelly Schulz, CEO, Maryland Tech Council
Mary Kane, President & CEO, Maryland Chamber of Commerce

DATE: March 20, 2024

Re: Senate Bill 541/House Bill 567 - Maryland Online Data Privacy Act of 2024 – Oppose unless amended

Dear Members of the Maryland General Assembly,

On behalf of the Maryland Tech Council’s (MTC) 800 technology-sector member companies, I write to comment on the current status of *Senate Bill 541/ House Bill 567 – Maryland Online Data Privacy Act of 2024*. At present, the Senate and House of Delegates have passed differing versions of this legislation that will now be considered in the opposite chamber. We anticipate that further changes will be made as the General Assembly seeks to reconcile these differences and pass Maryland’s first comprehensive online data privacy law.

The MTC supports the concept of a comprehensive data privacy law for Maryland, and appreciates the willingness of the sponsors of this legislation to engage the MTC and our members on the details of the bill. We acknowledge that the Senate and House sponsors, as well as the Senate Finance Committee and House Economic Matters Committee, have extensively incorporated stakeholder feedback into the introduced and amended versions of these bills. We are sincerely appreciative of those efforts.

The MTC took a position of “oppose, unless amended” on the bills and submitted testimony for the hearings that emphasized two concepts – consistency and compliance. We argued, and continue to maintain, that this bill should be as consistent as possible with similar data privacy laws already in place in other states. We also believe this legislation should be tailored to ensure that its provisions are not overly burdensome for compliance. These concepts are particularly important for our small and mid-size companies that are subject to this bill but do not have the compliance resources that larger companies possess. To that end, we encouraged the committees to conform the definition of key terms to definitions in existing law in other states, we encouraged the inclusion of a “right to cure” for companies to address compliance issues before being subject to enforcement, and we requested delaying the effective date of the bill to ensure companies have adequate time to prepare for compliance.

We have had the opportunity to review the bills passed by the Senate and House of Delegates, respectively. We were encouraged to see some of our recommendations adopted. It is clear that meaningful efforts have been made to be responsive to industry feedback on this legislation. However, as these bills continue to make their way through the legislative process, we wanted to take the opportunity to supplement our feedback based on the current versions of the bills. Below we will highlight amendments to the bill that should be maintained in the final bill. Additionally, following an analysis of both bills and

upon further discussion with our members, we submit some additional amendments to consider including in the final version of this legislation.

Provisions to Maintain

A number of amendments were included in SB 541 as passed by the Senate. We highlight a few below and urge the General Assembly to maintain these amendments in the final version of the bill.

1. *Definition of Biometric Data.* The Senate bill included an amendment to the definition of biometric data to include “any other unique biological characteristics that **are** used to uniquely authenticate a consumer’s identity,” rather than the original language of “**can be**” used. The language in the original version of the Senate bill and still contained within the House bill is overly broad. The Senate language more closely aligns Maryland with the majority of state privacy laws.
2. *De-identified Data.* The Senate bill added exception language under §14-4603 to include data that is de-identified according to HIPAA standards. Including this language is crucial for preserving the groundbreaking and innovative life sciences research being conducted in Maryland. HIPAA’s framework already streamlines data gathering, empowers patients to control their Personal Health Information (PHI), and promotes healthcare research and innovation. These standards are clear with respect to PHI and disclosure, and strike the appropriate balance of patient privacy and research needs. This language in the Senate bill would align Maryland with the language in similar consumer privacy laws in 12 out of the 13 states that have them. Maryland is a national leader for life sciences; it is imperative that this bill not result in operational disruptions to potentially life-saving research.
3. *Content Personalization.* The Senate bill eliminated a provision under §14-4607 that would have prevented a controller from collecting data for the sole purpose of content personalization or marketing without an opt-in from the consumer. This amendment represents a meaningful improvement to the bill because a core aspect of many online services is to provide personalized recommendations based on a consumer’s prior activity with the same service. Content personalization is one of the functions that consumers ask for most, and while they may readily consent to it, bombarding them with prompts specific to viewing personalized content would significantly degrade their online experience.
4. *Controller Obligations.* The House bill was amended to extend controller obligations in §14-4607 to processors in sub-sections (A) and (B)(1). This is not consistent with any of the existing data privacy regimes. Controllers and processors have different responsibilities, and these requirements should not be conflated. Processors store or process data as directed by the controller and have a contractual relationship with the controller, but not with the customer. The Senate bill rightly limits these obligations to controllers, as did the original version of the House bill.
5. *Third-Party Controller Protections.* Language was added to §14-4612 of the Senate bill to protect a compliant controller or processor from liability for misconduct by a third-party controller or processor to whom data was disclosed, and likewise protect third-party controllers or processors if the data they received from another party was collected in a non-compliant manner, as long as there was no actual knowledge of violation. These are standard liability protections for controllers and processors where their counterparty violates the privacy law without their knowledge.
6. *Right to Cure.* The Senate bill was amended to include a “right to cure” under §14-4614, which would authorize the Consumer Protection Division of the Office of the Attorney General to give

data controllers or processors time to cure a violation before being subject to an enforcement action. MTC member companies want to comply with this law. They should not be subject to punitive actions for minor violations of a complicated new law. Maintaining the right to cure is an important compliance feature of the legislation.

7. *Effective Date.* Both the Senate and House bills extended the effective date of the bill by one-year to October 1, 2025 from October 1, 2024. Again, delaying the effective date will assist with compliance with the law. Many of our small and medium size members do not have teams of compliance officers or attorneys that can quickly make the system changes necessary to comply with this law. Giving them additional time to prepare will be helpful. We appreciate that both the Senate and House bills contain this change.

Additional Amendments to Consider

Each of the amendments mentioned above represent notable improvements to the bill as introduced. However, several of our members and the tech community at large continue to have concerns about this legislation. Should the General Assembly consider additional amendments to the bill as the Senate and House versions are reconciled, we urge the bodies to consider the following.

1. *Align Data Protection Assessment (DPA) Requirements with the Majority of Other States.* The DPA requirements in both bills are overly burdensome and beyond similar requirements in other states. The “regular basis” of the required DPA should be streamlined to a more limited and specific standard. Performing the same intensive, time-consuming assessment over and over on the same processes that have not changed does not offer any meaningful privacy protection. Additionally, the requirement to perform an assessment “on each algorithm used” would be unique to Maryland and could involve thousands of algorithms that assist with very minor processing outcomes. For example, think about requiring an assessment on each function within an Excel spreadsheet. The DPA section already requires assessment of automated processing around consumer data that covers a “reasonably foreseeable risk” and the “each algorithm” language provides no benefit to consumer privacy and should be eliminated.
2. *Convert Data Minimization to Opt-out.* §14-4607(B)(1) limits “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 recommend amending this language to be consistent with the data minimization standards in California, Connecticut, and Europe. Our members are concerned that under the current language, consumers cannot get access to new website features or services unless they request them. This could result in Maryland consumers getting a different experience with respect to new features and services compared to consumers throughout the rest of the country.
3. *Include Local Preemption Language.* The MTC recommends adding language to §14-4614 that states “this subtitle supersedes and preempts any local law or ordinance regarding the processing of personal data by the controller or processor.” This will ensure that local governments do not create any new data privacy standards that are in conflict with this law. Including such a preemption clause is particularly important for our small and medium size members if local governments around the State pass local privacy laws.
4. *Narrow the Definition of Sensitive Data Related to Kids.* Included in the definition of “sensitive data” in §14-4601(GG)(3) is “personal data of a consumer that the controller knows or has reason to know is a child.” This standard appears again in §14-4607(4) and (5). This standard creates an

age inference requirement that could result in the collection of more personal data about users to determine whether they are a child. The “knew or should have known” standard does not exist in any other state’s privacy law, making this provision an outlier. We advocate amending this provision to an “actual knowledge or willful disregard” standard.

We reiterate our support for passing comprehensive data privacy legislation this year. Online data privacy has been a major topic of discussion for several years now. A lot of work has gone into getting SB 541/HB 567 to where it is today. Again, we are sincerely appreciative of the opportunity to be included in these deliberations and for the willingness of the General Assembly to consider the perspective of the tech community on this bill. We appreciate how close the Legislature is to passing this bill, but are hopeful that the information we have presented in this letter can be considered. We are willing to participate in any additional discussions that occur on this topic and would be pleased to address any questions. Thank you.

Sincerely,



Kelly Schulz
Chief Executive Officer



Mary D. Kane
President & CEO
Maryland Chamber of Commerce

HB 567_MDCC and MTC Joint Letter_Maryland Online D

Uploaded by: Hannah Allen

Position: UNF



TO: The Honorable Pam Beidle, Chair
Members, Senate Finance Committee
The Honorable Sara Love

FROM: Kelly Schulz, CEO, Maryland Tech Council
Mary Kane, President & CEO, Maryland Chamber of Commerce

DATE: March 20, 2024

Re: Senate Bill 541/House Bill 567 - Maryland Online Data Privacy Act of 2024 – Oppose unless amended

Dear Members of the Maryland General Assembly,

On behalf of the Maryland Tech Council’s (MTC) 800 technology-sector member companies, I write to comment on the current status of *Senate Bill 541/ House Bill 567 – Maryland Online Data Privacy Act of 2024*. At present, the Senate and House of Delegates have passed differing versions of this legislation that will now be considered in the opposite chamber. We anticipate that further changes will be made as the General Assembly seeks to reconcile these differences and pass Maryland’s first comprehensive online data privacy law.

The MTC supports the concept of a comprehensive data privacy law for Maryland, and appreciates the willingness of the sponsors of this legislation to engage the MTC and our members on the details of the bill. We acknowledge that the Senate and House sponsors, as well as the Senate Finance Committee and House Economic Matters Committee, have extensively incorporated stakeholder feedback into the introduced and amended versions of these bills. We are sincerely appreciative of those efforts.

The MTC took a position of “oppose, unless amended” on the bills and submitted testimony for the hearings that emphasized two concepts – consistency and compliance. We argued, and continue to maintain, that this bill should be as consistent as possible with similar data privacy laws already in place in other states. We also believe this legislation should be tailored to ensure that its provisions are not overly burdensome for compliance. These concepts are particularly important for our small and mid-size companies that are subject to this bill but do not have the compliance resources that larger companies possess. To that end, we encouraged the committees to conform the definition of key terms to definitions in existing law in other states, we encouraged the inclusion of a “right to cure” for companies to address compliance issues before being subject to enforcement, and we requested delaying the effective date of the bill to ensure companies have adequate time to prepare for compliance.

We have had the opportunity to review the bills passed by the Senate and House of Delegates, respectively. We were encouraged to see some of our recommendations adopted. It is clear that meaningful efforts have been made to be responsive to industry feedback on this legislation. However, as these bills continue to make their way through the legislative process, we wanted to take the opportunity to supplement our feedback based on the current versions of the bills. Below we will highlight amendments to the bill that should be maintained in the final bill. Additionally, following an analysis of both bills and

upon further discussion with our members, we submit some additional amendments to consider including in the final version of this legislation.

Provisions to Maintain

A number of amendments were included in SB 541 as passed by the Senate. We highlight a few below and urge the General Assembly to maintain these amendments in the final version of the bill.

1. *Definition of Biometric Data.* The Senate bill included an amendment to the definition of biometric data to include “any other unique biological characteristics that **are** used to uniquely authenticate a consumer’s identity,” rather than the original language of “**can be**” used. The language in the original version of the Senate bill and still contained within the House bill is overly broad. The Senate language more closely aligns Maryland with the majority of state privacy laws.
2. *De-identified Data.* The Senate bill added exception language under §14-4603 to include data that is de-identified according to HIPAA standards. Including this language is crucial for preserving the groundbreaking and innovative life sciences research being conducted in Maryland. HIPAA’s framework already streamlines data gathering, empowers patients to control their Personal Health Information (PHI), and promotes healthcare research and innovation. These standards are clear with respect to PHI and disclosure, and strike the appropriate balance of patient privacy and research needs. This language in the Senate bill would align Maryland with the language in similar consumer privacy laws in 12 out of the 13 states that have them. Maryland is a national leader for life sciences; it is imperative that this bill not result in operational disruptions to potentially life-saving research.
3. *Content Personalization.* The Senate bill eliminated a provision under §14-4607 that would have prevented a controller from collecting data for the sole purpose of content personalization or marketing without an opt-in from the consumer. This amendment represents a meaningful improvement to the bill because a core aspect of many online services is to provide personalized recommendations based on a consumer’s prior activity with the same service. Content personalization is one of the functions that consumers ask for most, and while they may readily consent to it, bombarding them with prompts specific to viewing personalized content would significantly degrade their online experience.
4. *Controller Obligations.* The House bill was amended to extend controller obligations in §14-4607 to processors in sub-sections (A) and (B)(1). This is not consistent with any of the existing data privacy regimes. Controllers and processors have different responsibilities, and these requirements should not be conflated. Processors store or process data as directed by the controller and have a contractual relationship with the controller, but not with the customer. The Senate bill rightly limits these obligations to controllers, as did the original version of the House bill.
5. *Third-Party Controller Protections.* Language was added to §14-4612 of the Senate bill to protect a compliant controller or processor from liability for misconduct by a third-party controller or processor to whom data was disclosed, and likewise protect third-party controllers or processors if the data they received from another party was collected in a non-compliant manner, as long as there was no actual knowledge of violation. These are standard liability protections for controllers and processors where their counterparty violates the privacy law without their knowledge.
6. *Right to Cure.* The Senate bill was amended to include a “right to cure” under §14-4614, which would authorize the Consumer Protection Division of the Office of the Attorney General to give

data controllers or processors time to cure a violation before being subject to an enforcement action. MTC member companies want to comply with this law. They should not be subject to punitive actions for minor violations of a complicated new law. Maintaining the right to cure is an important compliance feature of the legislation.

7. *Effective Date.* Both the Senate and House bills extended the effective date of the bill by one-year to October 1, 2025 from October 1, 2024. Again, delaying the effective date will assist with compliance with the law. Many of our small and medium size members do not have teams of compliance officers or attorneys that can quickly make the system changes necessary to comply with this law. Giving them additional time to prepare will be helpful. We appreciate that both the Senate and House bills contain this change.

Additional Amendments to Consider

Each of the amendments mentioned above represent notable improvements to the bill as introduced. However, several of our members and the tech community at large continue to have concerns about this legislation. Should the General Assembly consider additional amendments to the bill as the Senate and House versions are reconciled, we urge the bodies to consider the following.

1. *Align Data Protection Assessment (DPA) Requirements with the Majority of Other States.* The DPA requirements in both bills are overly burdensome and beyond similar requirements in other states. The “regular basis” of the required DPA should be streamlined to a more limited and specific standard. Performing the same intensive, time-consuming assessment over and over on the same processes that have not changed does not offer any meaningful privacy protection. Additionally, the requirement to perform an assessment “on each algorithm used” would be unique to Maryland and could involve thousands of algorithms that assist with very minor processing outcomes. For example, think about requiring an assessment on each function within an Excel spreadsheet. The DPA section already requires assessment of automated processing around consumer data that covers a “reasonably foreseeable risk” and the “each algorithm” language provides no benefit to consumer privacy and should be eliminated.
2. *Convert Data Minimization to Opt-out.* §14-4607(B)(1) limits “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 recommend amending this language to be consistent with the data minimization standards in California, Connecticut, and Europe. Our members are concerned that under the current language, consumers cannot get access to new website features or services unless they request them. This could result in Maryland consumers getting a different experience with respect to new features and services compared to consumers throughout the rest of the country.
3. *Include Local Preemption Language.* The MTC recommends adding language to §14-4614 that states “this subtitle supersedes and preempts any local law or ordinance regarding the processing of personal data by the controller or processor.” This will ensure that local governments do not create any new data privacy standards that are in conflict with this law. Including such a preemption clause is particularly important for our small and medium size members if local governments around the State pass local privacy laws.
4. *Narrow the Definition of Sensitive Data Related to Kids.* Included in the definition of “sensitive data” in §14-4601(GG)(3) is “personal data of a consumer that the controller knows or has reason to know is a child.” This standard appears again in §14-4607(4) and (5). This standard creates an

age inference requirement that could result in the collection of more personal data about users to determine whether they are a child. The “knew or should have known” standard does not exist in any other state’s privacy law, making this provision an outlier. We advocate amending this provision to an “actual knowledge or willful disregard” standard.

We reiterate our support for passing comprehensive data privacy legislation this year. Online data privacy has been a major topic of discussion for several years now. A lot of work has gone into getting SB 541/HB 567 to where it is today. Again, we are sincerely appreciative of the opportunity to be included in these deliberations and for the willingness of the General Assembly to consider the perspective of the tech community on this bill. We appreciate how close the Legislature is to passing this bill, but are hopeful that the information we have presented in this letter can be considered. We are willing to participate in any additional discussions that occur on this topic and would be pleased to address any questions. Thank you.

Sincerely,



Kelly Schulz
Chief Executive Officer



Mary D. Kane
President & CEO
Maryland Chamber of Commerce

HB 567_Opposed_Marriott and Under Armour.pdf

Uploaded by: Marta Harting

Position: UNF



SENATE FINANCE COMMITTEE

March 21, 2024

STATEMENT OF OPPOSITION TO HOUSE BILL 567

As Maryland-headquartered companies, Marriott and Under Armour oppose House Bill 567 due to its punitive and unnecessary restrictions on consumer loyalty programs. The bill unfairly prohibits the transfer and sharing of data within loyalty programs, but includes no equivalent prohibitions for data brokers, social media companies, or metasearch companies. In doing so, HB 567 inexplicably burdens loyalty programs beyond all other types of businesses.

Loyalty programs, by their very design, prioritize customer privacy by requiring individuals to affirmatively opt into the program to access discounts, rewards, or other benefits. This opt-in requirement ensures that consumers have full control over their participation in the program and the sharing of their personal information.

HB 567's proposed restrictions overlook the privacy safeguards already in place within loyalty programs. These programs operate transparently, allowing customers to make informed decisions about their participation based on the benefits offered and the data sharing involved.

While we are generally supportive of efforts to enhance data privacy, HB 567 poses an unnecessary risk to loyalty programs. The consequences of these restrictions, both intended and unintended, threaten to invalidate program partnerships and features that are incredibly popular with consumers.

While other states have enacted data privacy laws, **no other state in the country has adopted restrictions on loyalty programs like those contained in HB 567.** If enacted, HB 567 would make our home state of Maryland the only state in the country without an exception to preserve loyalty programs, depriving Maryland residents of the benefits of these programs in which they voluntarily participate.

Our loyalty programs are essential to the success of our global businesses. We urge you to amend HB 567 by striking the House amendment on page 23, line 19, through page 24, line 3, to ensure that Maryland's privacy regulations strike the right balance between protecting consumer data and fostering innovation and consumer choice within loyalty programs.

Marriott International, Inc. is a global lodging leader headquartered in Bethesda, Maryland. Since its founding in the 1920s as a small restaurant chain in Washington, DC, the company has grown to comprise more than 8,000 lodging properties in 129 countries and territories, including over 100 hotels and 10,000 associates here in the State of Maryland. Marriott's loyalty program is one of the largest in the world.

Under Armour, Inc., headquartered in Baltimore, Maryland, is a leading inventor, marketer, and distributor of branded athletic performance apparel, footwear, and accessories. Designed to empower human performance, Under Armour's innovative products and experiences are engineered to make athletes better.

BSA Letter on Maryland Online Data Privacy Act 3.2

Uploaded by: Matthew Lenz

Position: UNF



The Honorable Pamela G. Beidle
Miller Senate Office Building, 3 East Wing
11 Bladen St., Annapolis, MD 21401 - 1991

March 20, 2024

Dear Chair Beidle,

BSA | The Software Alliance¹ supports strong privacy protections for consumers and appreciates the Maryland legislature's work to improve consumer privacy through HB567/SB541, the Maryland Online Data Privacy Act. In our federal and state advocacy, BSA works to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data.

As you advance a comprehensive consumer data privacy bill, BSA urges you to ensure your efforts reflect the fundamental distinction between controllers and processors, which underpins privacy laws worldwide. **We are particularly concerned that HB567's data minimization standard upends this fundamental distinction, by applying the data minimization obligation to processors.** While we recognize the important role of data minimization in protecting consumer privacy, any data minimization provision should avoid undermining the clear distinction between controllers and processors, which is foundational to privacy and data protection laws worldwide.

We strongly recommend any data minimization standard apply only to controllers, not processors, to avoid upending the distinction between controllers and processors. We also encourage you to ensure any data minimization provision recognizes that companies need to collect personal data to continue improving their products as new consumer demands arise and technology evolves.

¹ BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

I. HB567's data minimization provision should be revised to apply to controllers, not processors.

Distinguishing between controllers and processors is a foundational aspect of privacy laws worldwide and in every state.² Laws that recognize these different roles better protect consumer privacy by crafting different obligations for different types of businesses based on their different roles in handling consumers' personal data. Both HB567 and SB541 appear to recognize the importance of this distinction. Both bills create a set of obligations for controllers, which are the companies that determine the purpose and means of processing consumers' personal data. Both bills also create a set of obligations for processors (sometimes called service providers), which are companies that process data on behalf of a controller and pursuant to its instructions.

HB567's data minimization provision would upend the distinction between controllers and processors by applying this obligation not only to controllers, but also to processors. HB567's data minimization standard provides that a controller or *processor* shall "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." Other parts of Section 14-4607 would similarly apply obligations designed for consumer-facing companies to processors, including limits on collecting and processing sensitive personal data.

This approach undermines the fundamental distinction between controllers and processors and creates new risks to consumer privacy.

Applying data minimization obligations to processors disregards their role in handling consumers' personal data — which is to process that data on behalf of a controller and subject to its instructions. It is the controller that decides how and why to process a consumer's personal data. The controller is therefore the entity that can effectively implement a data minimization obligation, since minimizing the amount of data a company collects requires that company to revisit its decisions on how and why it collects that data in the first place. Those decisions are made by controllers — not by processors. The processor's role is instead to process data in line with the controller's instructions; those instructions will reflect the controller's choices in minimizing the amount of data it collects from consumers.

Applying data minimization obligations to processors also undermines consumer privacy protections, rather than strengthening them. For example, a processor subject to a data minimization requirement may have to review consumer data that its business customers store on its service, to establish that it processes data only as necessary, proportionate, and limited under the law. Without such a requirement, a processor often will not review personal data that is stored on its service — and many cases, processors are contractually prohibited from reviewing this data, as part of their privacy and security commitments. Applying a data minimization obligation to processors therefore has the counterproductive result of requiring

² BSA | The Software Alliance, The Global Standard: Distinguishing Between Controllers and Processors in State Privacy Legislation, *available at* <https://www.bsa.org/files/policy-filings/010622ctrlrprostatepriv.pdf>.

the processor to look at more data than it would otherwise — contrary to the goal of data minimization. A more privacy-protective approach, and the one taken in all state privacy laws,³ is to apply consumer-facing obligations like data minimization only to businesses that determine the purpose and means of processing a consumer’s data. Controllers then engage processors in line with those limitations, so data remains protected when held by processors.

We strongly encourage you to revise HB567 so that any data minimization obligation applies only to controllers, not processors, consistent with all other state privacy laws.

II. Any data minimization standard should recognize that consumers benefit from improved products and services.

In addition to our concern about undermining the fundamental distinction between controllers and processors, we are concerned that the data minimization standard in both HB567 and SB541 may inadvertently harm consumers by limiting the ability of companies to improve existing products and develop new ones in response to consumer demand. This risk is present even when the bills’ data minimization standard is limited to controllers.

HB567’s data minimization provision limits the collection of personal data “to what is reasonably necessary and proportionate to provide or maintain a specific product or service.” Similarly, SB 541 would 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.” This standard has the potential to significantly impact companies’ ability to perform activities reasonably expected by consumers. Most notably, it does not clearly account for companies’ need to collect data to improve existing products or to create new products that address future consumer needs.

Companies need to use personal data to improve products and better serve customers. For example, banks, retailers, and other companies may use specialized software to route different customer service complaints to different internal teams. That software will work better when it has access to personal data, like the customer’s account number and order information. To improve their service, a company may decide to collect new data from consumers to support new functions – like collecting the customer’s city or zip code to help connect the customer to physical bank or store locations nearby that could provide additional assistance. Limiting the company’s ability to collect new or additional types of information would greatly restrict its ability to deliver effective customer service and lower the quality of the customer experience.

³ See, e.g., Cal. Civil Code 1798.100(c); Colorado CPA Sec. 6-1-1308(3); Connecticut DPA Sec. 42-520(a)(1); Delaware Personal Data Privacy Act, Sec. 12D-106(a)(1); Florida Digital Bill of Rights Sec. 501.71(1)(a); Iowa Senate File 262 Sec. 7(6)(b); Indiana Senate Enrolled Act No. 5 (Chapter 4, Sec. 1(1)); Montana Consumer Data Privacy Act Sec. 7(1)(a); New Hampshire Senate Bill 255 Sec. 507-H:6(l)(a); New Jersey Senate Bill 332/Assembly Bill 1971 Section 9.a.(1); Oregon CPA Sec. 2(5); Tennessee Information Protection Act 47-18-3204(a)(1); Texas Data Privacy and Security Act Sec. 541.101(a)(1); Virginia CDPa Sec. 59.1-578(A.1).

Other state privacy laws recognize the need for companies to improve existing products and develop new products. Failing to account for these activities risks freezing existing technologies where they are today — which will not benefit consumers. In many cases, companies will need to process personal data to improve the functionality of their products and to develop new products as current technologies become outdated or obsolete.

In other states, thirteen state privacy laws require controllers to 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.” California’s privacy law similarly requires that a business’ “collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed.” In contrast, HB567’s creates a new standard and does not clearly recognize that companies will need to use personal data to improve existing products and services that consumers rely on — and to develop new technologies that will benefit consumers.

In order for consumers in Maryland to continue to benefit from improved products and services, we urge you to adopt the data minimization approach in other state privacy laws and clarify that the bill does not limit companies’ ability to develop or improve products and services.

Thank you for your leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,



Olga Medina
Director, Policy

CC: Members of the Senate Finance Committee

MD Data Privacy Testimony 3.20.24.pdf

Uploaded by: Sharon Sykes

Position: UNF



March 21, 2024

Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

Re: House Bill 567 – Maryland Online Data Privacy Act of 2024

Dear Committee Members:

On behalf of the American Hotel & Lodging Association, I write to express my concerns with HB 567, which would threaten the viability of consumer loyalty programs.

If enacted, Maryland will be the first state in the nation at serious risk of losing loyalty programs. Not only will Maryland be a national and regional outlier on this issue, it could send visitors to other nearby states if hotels cannot operate loyalty programs in Maryland. Major event planners would move conferences to other states with hotels that can legally operate these programs.

Loyalty programs are a major component of leisure and business travel. Frequent travelers take advantage of these programs to save money on travel. Not accepting hotel loyalty programs in Maryland would discourage leisure and business travelers from visiting, resulting in fewer bookings and revenue for small business hotel owners.

Loyalty programs provide discounts or rewards to hotel guests to encourage return visits to their properties. By definition, loyalty programs prioritize privacy by requiring guests to opt into the plan to receive the benefits of the program.

Many states have already passed data privacy laws that provide antidiscrimination provisions while preserving loyalty programs. While we appreciate the desire of lawmakers to enhance data privacy, prohibiting the transfer and sharing of data within the program places a punitive and unnecessary burden on loyalty programs.

We urge you to preserve customer loyalty programs by adopting the language in companion bill SB 541 which will allow hotels to continue offering loyalty programs guests support and enjoy using.

If you have any questions, please do not hesitate to contact me at ssykes@ahla.com or 804.240.9919.

Sincerely,

Sharon T. Sykes
American Hotel & Lodging Association

Joint Ad Trade Letter Regarding Maryland HB 567.pd

Uploaded by: Travis Frazier

Position: UNF



March 20, 2024

Senator Pamela Beidle
Chair of the Maryland Senate
Finance Committee
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Senator Katherine Klausmeier
Vice Chair of the Maryland Senate
Finance Committee
123 James Senate Office Building
11 Bladen Street
Annapolis, MD 21401

RE: HB 567 – Maryland Online Data Privacy Act

Dear Chair Beidle and Vice Chair Klausmeier:

On behalf of the advertising industry, we write to ask the Senate Finance Committee (“Committee”) to align **HB 567**¹ with the version of SB 541 the Committee approved and the full Senate passed on March 14, 2024.² As described in more detail below, this action would align HB 567 with data privacy laws enacted in other states. We provide this letter to offer our non-exhaustive list of concerns about this legislation.

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product (“GDP”) in 2020.³ By one estimate, over 160,000 jobs in Maryland are related to the ad-subsidized Internet.⁴ We would welcome the opportunity to engage with you further on the non-exhaustive list of issues with HB 567 we outline here.

I. A Consent Requirement for Content Personalization and Marketing Would Negatively Impact Maryland Residents and Hinder Economic Growth

SB 541 was amended to remove a requirement to acquire consent from consumers before collecting data for the purpose of content personalization or marketing.⁵ No other state privacy law imposes an opt-in consent requirement for such marketing uses. The Committee decided to excise this consent requirement from SB 541, and we ask it to do the same when it considers HB 567.

Rather than providing consumers meaningful new privacy protections, an opt-in consent requirement would hinder Marylanders’ ability to seamlessly engage online. If enacted, this

¹ Maryland HB 567 (Gen. Sess. 2024), located [here](#).

² Maryland SB 541 (Gen. Sess. 2024), located [here](#).

³ John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf.

⁴ *Id.* at 127.

⁵ See SB 541 § 14-4607(A).

requirement would exacerbate notice fatigue for Maryland consumers, who would be inundated with consent requests to collect data for routine, responsible uses as consumers navigate the Internet. Such a shift would virtually ensure Maryland residents have a vastly different online experience than consumers in neighboring or nearby states, such as Virginia, Delaware, and New Jersey, and would not receive the same opportunities to access resources available due to the ad-subsidized Internet as consumers from all other states. Maryland should not proceed with a blanket opt-in approach for content personalization and marketing that starkly diverges from the approach in all other states that have enacted consumer data privacy legislation.

II. An Opportunity to Cure Violations Would Encourage Compliance with Law

As passed by the Senate, SB 541 would permit entities to take steps cure alleged violations until April 1, 2027, if a cure is deemed possible.⁶ We ask the Committee to similarly amend HB 567 to permit this cure opportunity. The ability to cure allows well-meaning businesses to take steps to rectify alleged violations before being subject to monetary penalties. This opportunity would benefit small and mid-sized businesses in particular, as such entities may have fewer resources to dedicate to compliance and thus could be caught up in lawsuits alleging technical violations of the law. A cure opportunity would allow these businesses to fix alleged violations and could potentially save them from the need to pay enterprise-threatening penalties that could put them out of business.

* * *

⁶ SB 541 at § 14-4614.

We and our members strongly support meaningful privacy protections for consumers supported by reasonable and responsible industry practices and support a national standard for data privacy accordingly. We therefore respectfully ask you to amend HB 567 to match SB 541, and we would welcome the opportunity to engage further and work with you to hone a workable privacy framework that benefits Maryland businesses and consumers alike.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies, 4A's
202-355-4564

Lartase Tiffith
Executive Vice President, Public Policy
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Members of the Senate Finance Committee

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP