

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:***

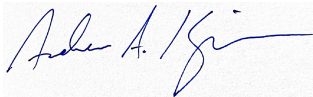
- Unfair/abusive/deceptive treatment of a consumer;
- Unlawful disparate impact on a consumer
- Financial/physical/reputational injury to a consumer
- Physical or other intrusion on the solitude or seclusion or the private affairs or concerns of a consumer in which the intrusion would be offensive to 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.~~