Maryland Online Data Privacy Act of 2024

February 14, 2024

Position: Unfavorable as introduced, neutral with amendments

Background: SB541 Establishes generally the manner in which a controller or a processor may process a consumer's personal data; authorizing a consumer to exercise certain rights in regards to the consumer's personal data; requiring a controller of personal data to establish a method for a consumer to exercise certain rights in regards to the consumer's personal data; etc.

.

Comments:

1. Page 4, line 23: STRIKE “status” and INSERT in its place: “condition or diagnosis.”
    a. This change further clarifies the meaning of the term and mirrors CT law.

2. Page 5, line 13: INSERT “intentionally” before “designed or manipulated.”
    a. Dark pattern violations are like fraud and should be considered an intentional act of deceit.

3. Page 6, line 1: STRIKE OR DEFINE “(8) access to essential goods or services”.
    a. This is problematic without a precise definition of “essential goods and services”. Further, this category is not traditionally included in the list.

4. Page 10, line 20: STRIKE “(1) Data revealing” and ADJUST remaining numbering.
    a. This edit clarifies the definition of “Sensitive Data” by removing an ambiguous qualifier that could unintentionally broaden the term to include non-sensitive data as explained below. It maintains the same list of data elements that defines “Sensitive Data” without the unnecessary and problematic qualifier.
    b. This inclusion of the qualifier “data revealing” should be struck as it broadens the defined term of “sensitive data" to potentially include "non-personal data”. This non-personal data may imply inaccurate information about consumer (e.g., buying a cross might “reveal” one is Christian; buying cosmetics might “reveal” race). A law based on possible inferences drawn from retail purchases would be problematic.

5. Page 11, line 17: STRIKE "controller's" and INSERT "unaffiliated" before "websites or online applications".
    a. The current definition of "target advertising" could include providing ads based on a consumer's activities on a business's first-party website or mobile app, which has no precedence of being considered targeted advertising in state privacy laws.
    b. This issue could also be addressed by adding "advertisements based on a consumer's activity displayed by a controller on any first-party website or mobile app owned or operated by that control" to the list of exemptions of "targeted advertising" beginning on page 10, line 20.

6. Page 12, line 8: REPLACE "produces" with "provides".
    a. "Provides" is a more standard term used for this policy in other states. "Produces" could have unclear meaning and unintended consequences.

7. Page 12, line 12: REPLACE "35,000 consumers" with "100,000 consumers".
    a. Setting the threshold at 35,000 is far too low to protect small businesses. Most states use 100K.

8. Page 12, line 9: REPLACE "35,000 consumers" with "100,000 consumers" AND on page 12, line 16, REPLACE "20%" with "50%".
    a. This should say at least 100,000 consumers and derived more than 50% of revenue from the sale to remain consistent with almost every other state.
    b. These edits ensure that Main Street businesses, including 98% of retailers that are single-location stores with less than 100 employees, are properly exempted from regulations as they are in most other states.

9. Page 15, line 27: ADD ", unless retention of the personal data is required by law" after "consumer"
    a. Create an exception that allows a controller to dismiss a consumer's request to delete and retain information if it is required by another area of law.

10. Page 19, lines 27 through page 20 lines 5: STRIKE lines in their entirety, from "(1) collect personal data..." through "share sensitive data concerning a consumer;" ADJUST remaining numbering.
    a. Section 14-4607(A)(1) and (2) are highly problematic. Like other consumer-facing businesses, retailers typically grow by attracting new customers. For example, retailers opening new store locations traditionally obtain lists of local households to send mailers announcing the new store opening. The law must preserve the same ability to collect data in the online environment for the purpose of marketing to prospective customers.

Personalized marketing does not create a harm for a consumer and should not be treated like sensitive information.

b. Further, the law should not limit collection or processing to that "strictly necessary" to provide or maintain a "specific product or service requested by the consumer". Retailers have always marketed products to inform the public of what is available for purchase. The inclusion of "strictly necessary" would limit the ability to provide this information to consumers.

11. Page 21, line 5: ADD "and processor" after "controller".
    a. Data minimization provisions should apply equally to both processors and controllers alike, and not to controllers alone. There is no legitimate public policy justification for limiting this requirement to controllers only; processors oppose data minimization requirements for their own benefit. The policy should establish an equal playing field.

12. Page 21, line 21: REPLACE "15" with "45"
    a. Extend the amount of time controllers have to respond to consumer requests to be in line with response requirements on Page 17, lines 5 and 8 and consistent with requirements in other states' consumer privacy laws.

13. Page 27, line 16: INSERT "designed" before "to ensure".
    a. Controllers cannot guarantee that a processor will adhere to instructions. Including "designed" protects controllers when processors do not follow instructions that are intended to limit consumer data processing.

14. Page 28, line 15: STRIKE "(V) Other substantial injury to a customer".
    a. "Other substantial injury" is not defined, so this potential risk is unclear and should be removed.

15. Page 32, line 29 through p. 33, line 2, 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.

a. The protection provided to third party controllers or processors in 14-4611(D) needs to run both ways to protect controllers from the independent misconduct of third-party processors and controllers, as it does in most state privacy laws. Controllers must similarly be protected from the violations of the law by processors and third parties and held harmless unless they have actual knowledge the processor or third party intends to violate the law with the consumer data they receive from the controller.

16. Page 33, lines 10-12: ADD "or processor" after "If a controller" and ADD "or processor" before "shall demonstrate that the processing:"
    a. This obligation should apply equally to both controllers and processors.

17. Page 34, lines 11-12: STRIKE lines 11-12 in entirety, from "(B) This section" to "other remedy provided by law".
    a. We would ask that private right of action be prohibited AND making clear that AG enforcement is an exclusive remedy by INSERTING the following language:
    "THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE ENFORCEMENT AUTHORITY TO ENFORCE VIOLATIONS OF THIS ACT. (D) NOTHING IN THIS ACT SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BE SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS OR ANY OTHER LAW."

18. Page 34, line 18: REPLACE "2024" with "2025".
    a. Controllers need adequate time to prepare for compliance with these requirements, especially the tens of thousands of retailers who are single-location stores that have not had to comply with other states' privacy laws to date and must contract with service providers to help them implement these new obligations. Note that when California did a study on the cost of implementing their state's requirements (which are approximately the same as those in this bill) for even the smallest of controllers (less than 50 employes), it was approximately $100,000 to implement for first time.

19. Page 34 – In Section 14-4613: INSERT a notice-and-cure provision permitting the AG to notify businesses of potential infractions and permitting up to 30 or 60 days for the businesses to come into compliance with the law.
    a. This is a standard provision in all state privacy laws and should be included in this bill. A notice-and-cure period is especially important when a state first adopts a privacy law and many businesses have not yet had an opportunity to comply with these regulations. It permits them to have a direct dialogue with the AG to ensure they are implementing the law correctly, especially with the subjective determinations required throughout a bill like this.
    b. Importantly, the California AG reported in their first year of compliance that approximately 75% of all businesses notified had resolved the alleged violation and come into full compliance with the provisions within 30 days.

c. A notice-and-cure provision helps increase compliance with the new law and keep state budgets in check by avoiding costly enforcement actions and it is therefore a mechanism welcomed by most state AGs and businesses alike.

With specific regard to loyalty rewards programs and suggested amendment 16, the bill clearly states that:

(E) IF A CONTROLLER SELLS PERSONAL DATA TO THIRD PARTIES OR PROCESSES PERSONAL DATA FOR TARGETED ADVERTISING OR FOR THE PURPOSES OF PROFILING THE CONSUMER IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS, THE CONTROLLER SHALL CLEARLY AND CONSPICUOUSLY DISCLOSE THE PROCESSING, AS WELL AS THE MANNER IN WHICH A CONSUMER MAY EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING.

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

We suggest adding language clarifying that the disclosure requirements related to data sales also applies to loyalty plans, and in fact, you do not get your exemption for loyalty plans unless you are in compliance with those disclosure obligations in subsection (E) of the same section 14-4607 where the loyalty plan language is located.

Suggested amendment in bold.

14–4607.

* * *

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

* * *

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

We welcome working with the sponsor and committee to resolve these issues.

171 CONDUIT STREET | ANNAPOLIS, MD 21401 | O: 410-269-1440
WWW.MDRA.ORG