March 28, 2024

House Economic Matters Committee
Room 231
House Office Building
Annapolis, Maryland 21401

RE: SB 541 - "Maryland Online Data Privacy Act of 2024" (Unfavorable)

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

On behalf of the Computer & Communications Industry Association (CCIA)[1], I write to respectfully raise several outstanding concerns regarding SB 541.

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, SB 541 still would diverge from existing frameworks in several key ways, as further detailed below. We appreciate your consideration.

CCIA suggests further amendments to definitions and controller obligations to facilitate interoperability.

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.

Key definitions

As drafted, key definitions in SB 541 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 suggests clarifying that the definition of "sensitive data" would encompass the personal data of a *known* child. This would be consistent with the *actual knowledge* standard under COPPA and remove ambiguity.

CCIA also has concerns surrounding the bill's inclusion of "third-party controller" under §14-4612(D)(1). The term itself is undefined in the bill and invites confusion surrounding the distinction between a "controller", a "processor", an "affiliate" and other entities that would be considered a "third party". CCIA recommends striking any references to "third-party controller", and any similar language,entirely to more clearly address the distinctions between processors, controllers, and third parties without creating unnecessary confusion.

Controller obligations

SB 541 would restrict collection of personal data to what is "reasonably necessary and proportionate". Given this departure from other existing privacy laws, this would result in additional compliance confusion and challenges for businesses currently seeking to meet and adhere to evolving compliance requirements. To minimize such friction, CCIA would recommend aligning such controller obligations with those included under Connecticut and Virginia's laws.

Data protection assessments

SB 541 would require a data protection assessment to include "an assessment for each algorithm that is used" which, again, diverges from requirements imposed in other states with no clear benefit to consumers. Given the broad scope of this definition, companies would be subject to burdensome reporting requirements. For example, businesses in every industry sector may choose to employ algorithms to address a variety of use cases ranging from increasing competitiveness to enhancing their products and services. This could also encompass routine and low-risk applications such as filtering and spell-check to credit-scoring algorithms up to generative artificial intelligence models. The use of AI systems has enabled small businesses to effectively market their products to the right consumers at affordable prices and allows for better customer experience and cheaper prices. CCIA

would therefore recommend that this provision be eliminated and clarify that the focus of data protection assessments are limited to high-risk activities.

Content personalization and marketing

SB 541 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 amendments regarding the enforcement provisions.

CCIA appreciates Maryland lawmakers' consideration of appropriate enforcement mechanisms for a comprehensive data privacy framework and requests further clarity that SB 541 would only allow for attorney general enforcement authority and 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