February 9, 2024

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

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

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 SB 541, unless amended.

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

CCIA strongly supports the protection of consumer data and understands that Maryland residents are rightfully concerned about the proper safeguarding of their data. CCIA also appreciates the significant effort that lawmakers have undertaken to strike the appropriate balance for meaningful protections while preserving benefits consumers receive and the ability for innovation to thrive. As you know, in the absence of a comprehensive law at the federal level, there is a growing number of states that have enacted their own laws. The majority of these laws harmonize a key set of definitions and concepts related to privacy. While we appreciate the sponsors' work on this bill, as written, SB 541 still would diverge from existing frameworks in several key ways.

Definitions and controller obligations should be clear and interoperable.

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

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

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

definitions in 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”, “consumer health data”, and “targeted advertising”. We also suggest aligning the definition of “geofence” based on existing state laws, such as in Washington and New York. As currently written, the bill’s definition of “geofence” is inconsistent and conflicts with the bill’s definition of “precise geolocation data”.

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

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

Finally, SB 541 would require a controller to obtain consumer consent prior to collecting personal data for content personalization or marketing. CCIA recommends striking this language as it is a novel provision in the context of other state data privacy laws, hindering the development of new products and services. This provision would also limit businesses' ability to conduct ad measurement, which would limit digital advertising for businesses large and small and have significant impacts on the internet economy.

CCIA requests further clarification regarding the enforcement provisions.

CCIA appreciates Maryland lawmakers’ consideration of appropriate enforcement mechanisms for a comprehensive data privacy framework and requests further clarity that SB 541 would not permit consumers to bring legal action against businesses that have been accused of violating new regulations. Every state that has established a comprehensive consumer data privacy law to date has opted to invest enforcement authority with their respective state attorney general. Private rights of action on other issues in states, such as under the Illinois Biometric Information Privacy Act, have resulted in plaintiffs advancing frivolous claims with little evidence of actual injury. These lawsuits also prove extremely costly and time-intensive for all parties involved, including the state, and it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state. in other states have resulted in plaintiffs advancing frivolous claims with little evidence of actual injury. These lawsuits also prove extremely costly and time-intensive for all parties involved, including the state, and it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state. Further, every state

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

* * * * *

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

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association