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 sponors, 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 Biometrtic 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 approprirate 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