Testimony in Support of House Bill 576:

Maryland Online Data Privacy Act of 2024

Favorable With Amendments

March 21,2024

Chair Beidle and distinguished members of the Finance Committee, it is my pleasure to offer testimony in favor with amendments for **House Bill 576: Maryland Online Data Privacy Act of 2024**. If enacted, this bill would provide the strongest consumer data privacy law in the country. Our amendments would maintain that standard.

We at Microsoft applaud you for advancing data privacy legislation. At Microsoft, we have long taken the privacy of our customers seriously, and we have a long track record of supporting responsible, thoughtful reform.

The data minimization provisions would hamstring research and innovation. They prohibit companies from collecting any personal data unless it "is reasonably necessary and proportionate to provide or maintain a specific product or service requested by [a] consumer".

As drafted these sections would seriously hinder our ability to improve or create new, innovative technologies. People expect their technology to improve. They like to receive new products, features, and services. As terrific as Microsoft Word was in 1998, people like it much better with updated features like Track Changes, Sharing Documents, or the ability to insert links or photos. It would inhibit our ability to create services like Microsoft Reading Coach, which helps teachers accelerate students' ability to learn,[1] or to build services like Seeing AI, which narrates the world for people with vision impairments.[2] All of that innovation relies upon data.

We also acknowledge that some have expressed concerns that the data minimization provisions in existing privacy laws, which mostly require companies to limit their data collection to the purposes outlined in their privacy policies, are not strong enough and that companies should face stricter guardrails about what they can and cannot collect.

We would ask the committee to consider, instead, tying companies' data minimization obligations to **consumer's reasonable expectations**. In other words, companies would be obligated to **"limit the collection of personal data to what is reasonably necessary and proportionate to:**

(1) provide or maintain a product or service requested by the consumer to whom the data pertains; or;
(2) a consumer's reasonable expectations considering the context in which the personal data is collected and the relationship between the consumer and the controller.

This approach provides a sensible alternative. It would be **much stronger** than the minimization provisions in other laws because it would prevent companies from setting the terms of their own

[1] For more on Microsoft Reading Coach, see: https://www.youtube.com/watch?v=fHZdcLxdzFQ.
[2] For more on Seeing AI, see: https://www.microsoft.com/en-us/garage/wall-of-fame/seeing-ai/.

data collection and from hiding abusive data collection practices in lengthy privacy policies. It would also be more flexible than the bill's current language, addressing concerns that the current minimization provisions are too rigid and will hamper innovation, because it would tie companies' obligations to consumer expectations—expectations which will invariably differ in different contexts.

In addition, we recommend that the minimization provisions be applied not to processors, but to controllers, as originally drafted. By applying the minimization provisions to processors, the bill diverges from 30 years of privacy law and threatens to undermine the legal protections that have permitted all governments, organizations, and businesses large and small to use enterprise cloud services.

For several important reasons, privacy laws globally have long differentiated between the obligations that apply to "controllers" and those that apply to "processors." Under that framework, the controller is the entity that "determines the purposes and means" of processing personal data. In other words, it is calling the shots about what's being collected, how it's being used or shared, and why. It is typically the entity that has a relationship with consumers, and it is directly responsible for satisfying consumers' requests to exercise their privacy rights

The processor is only permitted to process personal data pursuant to the instructions given it by the controller in a binding contract. The processor cannot call the shots about what is done with (or "determine the purposes and means" of processing) personal data. If it did so, it would not only violate the law and its contract with the controller, but it would itself become a controller (and therefore on the hook for complying with all of the obligations that apply to controllers). The processor's obligations are, among other things, to ensure that the controller can comply with its obligations under the law.

These roles are function- and context-specific, which means that the same corporate entity could be serving as a controller in one scenario but a processor in another.

This concept—the controller/processor distinction—has been critical to provide assurances to all customers, including governments, nonprofits, and businesses large and small, that if they decide to move their data to an enterprise cloud service, the data will remain the customer's, and the cloud service will not start rifling through it or using it for its own purposes. Without the concept, the entire system of enterprise cloud services could come crashing down.

For these reasons, we recommend:

Removing the "Or Processor" amendments attached by the House at various points throughout, conforming it in this instance to the Senate bill.

We ask you to humbly consider our suggested amendments and look forward to dully supporting the amended bill. We urge a report of Favorable With Amendment.