February 7, 2023

Senate Finance Committee
Attn: Tammy Kraft, Committee Manager
3 East Wing
Miller Senate Office Building
11 Bladen Street
Annapolis, Maryland 21401

Re: SB 169 - the Biometric Data Privacy Act (Oppose)

Dear Chair Griffith and Members of the Senate Finance Committee:

On behalf of the Computer & Communications Industry Association (CCIA)[1], I write to respectfully oppose SB 169, the Biometric Data Privacy Act. 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 biometric data. However, as currently written SB 169 goes far beyond protecting such data, which could result in degraded consumer services and experience. We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

1. Align key definitions with privacy standards to promote regulatory interoperability and mitigate unnecessary compliance burdens.

By introducing a definition and compliance obligations relating to "personal information", SB 169's scope extends beyond the subject of "biometric" data, with multiple implications. To meet compliance requirements under a new privacy regime, businesses inevitably face logistical and financial challenges. Given the significant costs associated with developing privacy management systems, even minor statutory divergences between frameworks for

[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 or the scope of compliance obligations, can create significant burdens for covered organizations.[3] SB 169's definition of personal information includes, *inter alia*, "information that indirectly relates to a device" and therefore goes far beyond what could reasonably be linked to an individual. As such, this definition should be more narrowly tailored to avoid unnecessary regulatory burdens.

2. Privacy protections should take a risk-based approach.

Privacy protections should be directed toward managing data collection and processing practices that pose a high risk of harming consumers or are unexpected in the context of a service. Consent mechanisms can be a powerful tool for promoting transparency and consumer control. However, it is important to recognize that the provision of many services, both online and offline, requires the collection and processing of certain user information. Requiring specific user consent for any data collection or processing would be inconsistent with consumer expectations, introduce unnecessary friction resulting in the degradation of user experience, and likely overwhelm consumers, resulting in "consent fatigue" that would lessen the impact of the most important user controls.[4]

As drafted, SB 169's written consent requirements would uniquely burden consumers and businesses alike without any obvious benefit to privacy interests. SB 169's provision mandating disclosure of biometric information to individuals or their authorized representatives similarly fails the risk-return calculus. This provision omits any form of authentication, and could therefore put Marylanders at even greater risk. Moreover, by prohibiting the use of biometric information except when "strictly necessary", and by simultaneously prohibiting different levels of products or services, SB 169 might result in Marylanders being denied innovative products in the marketplace.

3. Sufficient time is needed to allow covered entities to understand and comply with newly established requirements.

SB 169 fails to provide covered entities with a sufficient onramp to achieve compliance. A successful privacy framework should ensure that businesses have an appropriate and reasonable opportunity to clarify the measures that need to be taken to fully comply with new requirements. Recently enacted privacy laws in California, Colorado and Virginia included two-year delays in enforcement of those laws. CCIA recommends that any privacy legislation advanced in Maryland include a comparable lead time to allow covered entities to come into

[3] A study commissioned by the California Attorney General estimated that in-state companies faced $55 billion in initial compliance costs for meeting new privacy requirements, with small businesses facing disproportionately higher shares of costs. Berkeley Economic Advising and Research, LLC, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," (August, 2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

[4] See Article 29 Data Protection Working Party, WP 259, *Guidelines on Consent Under Regulation 2016/679*, 17 (Apr. 10, 2018), ("In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing."), https://ec.europa.eu/newsroom/article29/items/623051.

compliance and would therefore recommend amending the current October 1, 2023 effective date included in SB 169 to a later date.

4. Investing enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

SB 169 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Maryland's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – 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 – California, Colorado, Connecticut, Utah and Virginia – has opted to invest enforcement authority with their respective state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA recommends that the legislation include a cure period of at least 30 days. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government's limited resources on enforcing the law's provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential privacy changes rather than shifting focus to defending against litigation.

* * * * *

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