Computer & Communications Industry Association
Tech Advocacy Since 1972

March 22, 2022

Chair Kelley and Vice-Chair Feldman
Maryland Senate Finance Committee
11 Bladen St.
Annapolis, MD 21401

Re: CCIA Comments in Opposition to SB 335, The Biometric Identifiers Privacy Act

Dear Chair Kelley, Vice-Chair Feldman, and Members of the Senate Finance Committee:

On behalf of the Computer & Communications Industry Association (CCIA),[1] I write in respectful opposition to SB 335, the Biometric Identifiers 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, especially SMEs, have regulatory certainty in meeting their compliance obligations and that consumers are able to understand and 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 drafted a set of principles to promote fair and accountable data practices.[2]

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 335's scope extends beyond the subject of "biometric" data, with multiple implications. In meeting 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 definitions or the scope of compliance obligations can create significant burdens for covered organizations.[3] SB 335's definition of personal information includes, *inter alia*, 'information that indirectly relates

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For almost 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
[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," at 11 (August, 2019), https://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

to a device' and therefore sweeps far beyond what could reasonably be linked to an individual. This definition should be more narrowly tailored to avoid unnecessary regulatory burdens.

2. **Employ risk-based protections.**

Privacy protections should be directed toward managing data collection and processing practices that pose a risk of harm to 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, add unnecessary friction resulting in the degradation of user experiences, and likely overwhelm consumers, resulting in "consent fatigue" that diminishes the impact of the most important user controls.[4] As drafted, SB 335's written consent requirements would uniquely burden businesses, as well as consumers, without any obvious benefit to privacy interests. SB 335'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 335 might result in Marylanders being denied innovative products in the marketplace.

3. **Ensure practicable compliance to provide covered entities with predictability in meeting new obligations.**

SB 335 fails to provide businesses with a sufficient onramp for compliance. A successful privacy framework must ensure that businesses have sufficient opportunity and clarity to meet their compliance obligations. Recently enacted privacy laws in California, Colorado, and Virginia all contain 2-year delays in enforcement. We recommend that any privacy legislation advanced in Maryland include a comparable on-ramp to enable compliance, and therefore would recommend amending the current October 1, 2022 effective date under SB 335.

4. **Vest enforcement authority with the Attorney General's Office.**

New privacy regulations would be best enforced by the Office of the Maryland Attorney General. The inclusion of a private right of action with a statutory award, entirely unmoored from the need to demonstrate any actual injury, has led to spurious class action litigation in other jurisdictions, as plaintiffs' attorneys seeking lucrative settlements for alleged bare-procedural violations, primarily benefiting plaintiffs' attorneys with little connection

[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/itemdetail.cfm?item_id=623051.

to the remedy of any genuine consumer injury. The drawbacks of private rights of action are readily apparent in the history of state and federal privacy statutes and other state biometric regulations.[5]

On behalf of our business constituents and their consumers, CCIA seeks a strong, flexible, and modern privacy framework for the digital economy. We look forward to working with the Assembly to reach this critical goal. Should you have additional questions, please feel free to contact me.

Sincerely,

Matthew Schruers
President
Computer & Communications Industry Association (CCIA)

[5] *See*, U.S. Chamber Institute for Legal Reform, *Ill-suited: Private Rights of Action and Privacy Claims* (July, 2019), https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf.