

STATE PRIVACY & SECURITY COALITION

February 8, 2023

Chair Melony Griffith
Vice Chair Katherine Klausmeier
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: SB 169 (Biometrics) – Opposition

Dear Chair Griffith and Vice Chair Klausmeier,

The State Privacy & Security Coalition, a coalition of over 30 companies and five trade associations in the retail, automotive, technology, telecom, and payment card sectors, writes in opposition to SB 169, which would decrease consumer safety and significantly impact the state's economy. The bill is based on an outdated Illinois law, the Biometric Information Privacy Act (BIPA), that was passed in 2008 – less than a year after the smartphone was invented. The abuse of the private right of action (PRA) in the law, as well as the evolution of the online ecosystem, has led to bipartisan efforts in Illinois to reform the statute so as to eliminate the problems that have plagued it since its passage.

SPSC strongly supports consumer protections for personal data that can identify individuals. Effective privacy legislation should appropriately balance increased consumer control over their data and how it is used, while balancing the need for operational workability and cybersecurity.

Fortunately, privacy law has evolved since 2008, and in fact has evolved rapidly in the last two years. States such as Connecticut and Colorado have passed comprehensive privacy laws that cover a broad swath of personal data. These bills provide:

- strong, opt-in protections for consumers with regard to biometrics and other sensitive data;
- a greater number of consumer rights (access, deletion, correction, portability), opt-out of sale, targeted advertising, and profiling;
- strong obligations on businesses to document data processing activities that present a heightened risk of harm; and
- strong contractual requirements for entities that handle personal data – including biometrics – on behalf of the entities that collect the data.

These laws provide stronger protections for biometric data than SB 169, but do so in a way that much more accurately reflects the divided responsibilities of “controllers” and “processors.” We would strongly urge the legislature to consider moving forward with the Colorado or Connecticut model rather than pursue legislation that, in Illinois, has caused startups to avoid offering products in the state and safety products that are diminished due to the omnipresent litigation threat.

STATE PRIVACY & SECURITY COALITION

The Private Right of Action Will Make Consumers Less Safe

First, including a private right of action for statutory damages would create massive class action litigation exposure for any *alleged* violations of the law by commercial entities, significantly deterring uses of biometric data including for anti-fraud, authentication and other security purposes that benefit consumers. As in Illinois, the result would be to enrich trial lawyers without striking a balance that allows the use of biometric data for purposes that benefit Maryland residents. Put simply, a private right of action means businesses will be much less likely to offer services that keep Maryland residents' identities safe.

The litigation numbers bear this out: in the last five years, trial lawyers have filed *nearly 1000 class action lawsuits based on BIPA*. 14 years of experience with Illinois' law have shown that this approach leads businesses to decline to offer their full suite of services to state residents, or avoid offering their services in the state at all, due to the overzealous litigation this legislation catalyzed. For this reason, Illinois is considering amending the law in order to address this significant unintended consequence and bring beneficial services back to Illinois consumers.

This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest on the merits of the case, but instead on the opportunity to inflict asymmetrical discovery costs on businesses both small and large – with a cost to defend these frivolous actions averaging \$500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal discovery costs, huge negotiating leverage for nuisance settlements, even if the defendant is compliant with the law. In fact, ***only a single case has ever been brought to trial.***

Furthermore, studies have revealed that private rights of action fail to compensate consumers ***even when a violation has been shown***, and instead primarily benefit the plaintiff's bar by creating a "sue and settle" environment.¹ This is not to say that Maryland lacks effective enforcement options outside the trial bar – to the contrary, it has a strong consumer protection statute that the Attorney General can use *right now* to punish bad actors. On the other hand, the PRA in Illinois has not only failed to meaningfully protect consumers, but actually made them less safe, as anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.

SB 169 Has Significant Anti-Privacy and Anti-Security Consequences

Additionally, SB 169 provides an access right for consumers with regard to their biometric information and other types of "personal information." We believe that implementing the overbroad provisions related to this right will present real, if unintended, threats of harm to consumers. Additionally, the vast majority of biometric information is hashed, meaning that it is

¹ Mark Brennan et al., *Ill-Suited: Private Rights of Action and Privacy Claims*, U.S. Chamber Institute for Legal Reform (July 2019).

STATE PRIVACY & SECURITY COALITION

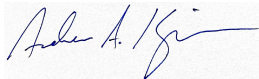
converted to a lengthy numeric value. Consumers will not derive any meaning from this numerical sequence, or any understanding of how their information is used that is not already covered by a business's privacy policy.

Disclosing actual biometric identifiers upon consumer request also poses significant security concerns, as the bill does not allow a private entity to refrain from disclosing biometric identifiers or other sensitive information like Social Security Numbers to an individual if the business cannot reasonably authenticate the request. Even California's privacy law recognizes and accounts for this security concern, making clear that a business "shall not disclose in response to a[n access request] a consumer's...unique biometric data."²

SB 169 includes a provision allowing for "authorized representatives" of consumers to request and obtain this very sensitive data, but provides no methods that would allow the business to verify that a) the consumer is who they say they are, and b) the authorized representative has the proper authority to exercise this right. The lack of these types of authentication and security provisions leave consumers extremely vulnerable to being taken advantage of. Vulnerable populations such as the elderly could easily designate their authority to a scammer, believing that the individual is safeguarding their data.

These are just some of the significant issues with SB 169 as drafted. Again, we would urge this committee to consider alternative, more modern, and more expansive data privacy protections for Maryland consumers that are more balanced, work across state lines, and do not create risks of frivolous litigation.

Respectfully,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

² See 11 CCR §999.313(c)(4).