

# STATE PRIVACY & SECURITY COALITION

February 20, 2023

Chairman C.T. Wilson  
Vice Chair Brian M. Crosby  
House Economic Matters Committee  
Room 231  
House Office Building  
Annapolis, MD 21401

**Re: HB 807 (Comprehensive Privacy & Biometrics) – Unfavorable**

Dear Chair Wilson and Vice Chair Crosby,

The State Privacy & Security Coalition, a coalition of over 30 companies and six trade associations in the retail, automotive, technology, telecom, and payment card sectors, writes in opposition to HB 807, but with the hope that the bill can be amended to a place where we no longer oppose it. The bill includes provisions based on an outdated Illinois law, the Biometric Information Privacy Act (BIPA), that was passed in 2008 – less than a year after the smartphone was invented.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. It is also a primary reason why not a single other state has enacted this statute.

However, HB 807 also contains language based on the Connecticut privacy bill that passed in 2022, and is going into effect in July of this year. If HB 807 is amended to match that legislation, SPSC would not oppose the bill.

SPSC's members support strong protections for consumers' personal data. 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.

Connecticut and other states such as 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.

Additionally, the Connecticut legislation – like all other comprehensive privacy bills that states have passed – has exclusive enforcement by the Attorney General for privacy violations, and

# STATE PRIVACY & SECURITY COALITION

also has a Right to Cure. These are integral and critical parts of businesses being willing and able to institute these complex, expansive consumer privacy protections.

## Connecticut's Treatment of Biometric Information

One of the many advantages that the Connecticut framework has over a sectoral approach is that it encompasses ***all data that is linked or reasonably linkable to an individual***. In other words, it covers not just one type of data like biometrics, but anything that is “reasonably linkable” to an individual.

However, since HB 807 attempts to also incorporate HB 33's biometrics language, we believe it is helpful to outline the protections consumers would have for biometric information under the Connecticut framework. These include:

- Classifying biometric data as “sensitive data,” along with precise geolocation data, health data, children’s data, among other sets of data.
- Establishing affirmative opt-in consent requirements for any collection or processing of biometric data.
- Requiring businesses to disclose the purposes for processing such data.
- Requiring businesses to obtain affirmative opt-in consent if the purposes for processing change.
- Requiring businesses to obtain affirmative opt-in consent if a business wants to use the biometric data for another purpose than that which it first told the consumer.
- Requiring businesses to document the processing of biometric data, and documenting both the risks and the benefits to such processing.
  - Documenting how the business intends to mitigate the risks from processing biometric data, if risks are identified.
- Requiring processors (vendors who provide services to the consumer-facing entities) to contractually agree to:
  - A duty of confidentiality with regard to processing the biometric data
  - Deleting or returning all of the biometric data to the controller once the contract is completed
  - Allow the controller to conduct assessments of the processor’s contractual compliance for handling biometric data.
- Providing the consumer with the rights to:
  - Confirm whether the controller is processing biometric data and access such data (unless there are security risks to providing the consumer with the actual biometric data);
  - Require the controller to delete biometric data;
  - Correct inaccurate data;
  - Port such data from one controller to another (again, unless there are security risks to providing the consumer with the actual biometric data)

# STATE PRIVACY & SECURITY COALITION

As you can see, the Connecticut framework provides extensive protections and consumer rights with regard to biometric data (and, critically, all other types of data that are not already regulated by federal law such as the Health Insurance Portability and Accountability Act (HIPAA)).

We believe that this framework is a much better balanced approach that better serves consumers and is much clearer for businesses to comply with.

Notably, in the 15 years since BIPA's enactment in Illinois, ***not a single state has enacted it***. Connecticut, following Virginia, Colorado, and Utah, ***was the fourth state to enact a version of this law since 2021***, with a number of other states expected to pass a version of the law this year.

## The Private Right of Action Will Make Consumers Less Safe

A critical component to add to HB 807's existing language is enforcement by the Attorney General, along with a right to cure. Retaining the private right of action will make this bill untenable, and would continue to create opposition from the business community. There are several reasons for this.

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***.

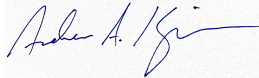
# STATE PRIVACY & SECURITY COALITION

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.<sup>1</sup> 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.

The Right to Cure is also a critical component of any comprehensive privacy enforcement mechanism. The right to cure helps all parties – the Attorney General's Office, consumers, and businesses. It helps the Attorney General's Office by streamlining compliance; all that is required to put a business on notice that it is in violation of the statute is a letter; in response, a business has a period of time to fix the violation and expressly state it will not commit the violation in the future. This helps the consumer by keeping their privacy protections in place with a short time for resolution, omitting the need for lengthy and costly litigation. Finally, it helps businesses by increasing cooperation with the Attorney General's office while still holding businesses accountable to the consumer.

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

---

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