

**SB 335: Commercial Law – Consumer Protection – Biometric Identifiers Privacy
Position: FAVORABLE WITH AMENDMENTS**

SB 335, the Biometric Identifiers Privacy Act, is a good start for protecting the privacy of Marylanders' biometric data. However, there are some points where it falls short in its privacy protections, and a few places where the burden of compliance may have unintended effects. Therefore, I support it with the changes described below.

SB 335 is clearly modeled after Illinois's similarly-named Biometric Information Privacy Act (BIPA). In the years since BIPA was passed, we've had a chance to see how businesses and courts treat its protections. BIPA provides a private right of action, which deputizes aggrieved citizens to enforce the law, rather than having the state itself do so. Although unusual, it has not interfered with successful pursuit of claims under the act, and indeed courts have ruled that claimants do not need to show an injury to be considered "aggrieved."

However, SB 335 fails to remedy certain flaws with BIPA. BIPA does not establish a statute of limitations for claims, leading to a [muddled decision](#) by the Illinois Appellate Court in *Tims v. Black Horse Carriers, Inc.*, in which they held that different safeguards of the law had different statutes of limitation. **Maryland could explicitly set a statute of limitations for claims under SB 335.** Additionally, both BIPA and SB 335 classify genetic markers not as a "biometric identifier," but as "confidential and sensitive information," which is not afforded any special protections by this law. One's DNA is absolutely a biometric identifier, and **SB 335 should classify it as such.**

SB 335 differs from the Illinois law in several important ways. Some of these aim to confer additional protections to Marylanders. For instance, SB 335 explicitly constrains not just the party that collected biometric information but also any processors they use. Likely inspired by the non-discrimination requirement of the California Consumer Privacy Act (CCPA), SB 335 forbids offering reduced services or higher prices to users who decline to provide biometric identifiers or exercise their rights under SB 335. However, unlike CCPA, SB 335 does not allow businesses to adjust prices or services commensurate to the value provided by biometric identifiers, only to refuse service altogether. **SB 335 should offer a similar middle-ground option to CCPA.**

BIPA sets a time limit for the destruction of biometric identifiers: 3 years after collection or after fulfilling the purpose for which they were collected, whichever comes first. SB 335 shortens the maximum retention time to 1 year, and requires that companies also destroy the data within 1 month of receiving a verified request to do so from the person who provided it. This last addition is commendable, but **shortening the maximum**

holding period to 1 year is a mistake, because any added protection from data minimization isn't worth the cross-jurisdictional inconsistency in data destruction requirements.

Unlike BIPA, SB 335 does not apply to uses of employee biometric data for operational purposes. This is a significant shortcoming, as much of the case for biometric privacy — concerns about intrusiveness and the security of private and unchangeable data — apply equally to employee biometrics as to customer ones. Many of the cases brought under BIPA concern employees seeking to assert their privacy rights against their employers, and SB 335 would not offer Maryland workers similar protections. Moreover, SB 335 does not apply to financial service providers. **SB 335 should not have these expansive carve-outs.**

SB 335 improves on BIPA by allowing persons to request copies of their biometric information from entities holding it, as well as information on the purpose of the biometric information and with whom it might be shared. However, unlike BIPA, it fails to require private entities to share, before the biometric data is first collected, information about the purpose of the collection and the term for which the data may be held. **SB 335 should require proactive disclosure prior to collection** to ensure that consent required by SB 335 is informed.

I support a favorable report on SB 335 if the bill is amended as recommended above.

— David W. Edelstein, IAPP Certified Information Privacy Technologist