STATE PRIVACY & SECURITY COALITION

The State Privacy & Security Coalition (SPSC) **Opposes Maryland HB 259**

The State Privacy and Security Coalition, a coalition of 30 leading communications, media, technology, retail, payment and automotive companies and 7 major trade associations, opposes HB 259, which seeks primarily to replicate the 2008 Illinois Biometric Information Privacy Act (BIPA).

Our members recognize the importance of consumer privacy and the sensitivity of biometric data that can identify individuals, and appreciate the updates made to the definitions in this bill. However, we caution against replicating several of the serious problems in the Illinois Biometric Information Privacy Act (BIPA), which has produced significant unintended consequences for both businesses and consumers in that state – so much so that there is bipartisan support to amend the law 14 years later. These include BIPA's 1) private right of action (PRA), 2) overbroad definitions that cover even collection of information that does not identify an individual, which exacerbates the negative effects of its other problems, and 3) failure to exempt uses and provision of biometric data for fraud and security purposes.

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 *more than 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.

Furthermore, although we appreciate ideas to restrict the PRA, such as by specifying damages "up to" the statutory minimum, this is unlikely to solve the problem of frivolous lawsuits. This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest even on the outcome of the case, but instead on the opportunity to inflict asymmetrical eDiscovery costs on businesses – with a cost to defend these non-meritorious actions averaging $500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal eDiscovery costs, huge negotiating leverage for nuisance settlements, even if the defendant is compliant.

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. This is not to say that Maryland lacks effective enforcement options outside the trial bar. In Texas, for example, the attorney general recently launched a comprehensive investigation of biometrics violations by large digital platforms. 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.

BIPA's Definitions Are Outdated and Do Not Reflect the Modern Online Ecosystem

Second, BIPA is written in such an overbroad manner that it covers information that *does not identify an individual*. Because the statute was drafted less than a year after the smartphone was invented, it does not reflect the modern understanding of biometric information as information that is used to identify individuals. This means that common and harmless features consumers use everyday, such as entertainment filters that measure face geometry but do not seek to identify an individual, are subject to BIPA litigation.

The definitions are further out of date because they cover any and all entities "in possession of" a biometric identifier, which includes incidental collection of biometric data that would not be stored and therefore poses minimal privacy risk to consumers. Again, the statute shows its age by wrapping in entities such as cloud storage providers, who have no way of obtaining consent from the consumer and no way of determining whose information they are storing. *This anonymity enhances consumer privacy*. BIPA's language exacerbates the problems described above by wrapping in a broad swath of businesses under its mandates, including those who do not ever store, disclose, or sell consumer biometric data.

BIPA Does Not Include a Cybersecurity Exception and Therefore Weeds Out Fraudsters Instead of Identifying Them

Finally, many biometric services proactively keep users, subscribers, and customers safe. Replicating BIPA would put Maryland citizens at much greater risk of fraud because biometrics are a leading means of fraud prevention. For example, biometric data is used to secure access to highly sensitive buildings, to detect fraudulent callers, and to prevent fraudulent takeovers of financial accounts.

Because BIPA does not allow for the use of biometric data for security or fraud prevention without written opt-in consent—and does not even have a clear security exception—it would put Maryland residents at great risk of security and fraud threats. Fraudsters, terrorists and other criminals simply will not consent to use of their biometric data for fraud prevention or security, so they would not be able to be screened by private businesses. This is not hyperbole – businesses in Illinois are already avoiding using biometric data for fraud or security purposes because of the huge class action risk. This issue is even more acute in the post-COVID-19 era. Cybersecurity has never been more important, and the pandemic has resulted in an exponential

increase in cybercrime activity against both private and public sector entities, including a 600 percent spike overall. It is critical for the safety of both sectors that Maryland not remove an important tool to leverage in combatting cyber threats and preserving secure systems and identities.

For all these reasons, our coalition opposes using BIPA as a model. Instead, we strongly encourage Maryland to look to the Washington state biometrics law, as well as the protections for consumers included in the Virginia and Colorado omnibus privacy laws – protections that are, in fact, stronger than those that exist in the California privacy regime (CCPA & CPRA). These laws still require opt-in consent from the consumer, but reflect a more modern and widely-accepted approach to definitions and cybercrime.

Although Maryland may certainly decide to revise the Washington model rather than importing it wholecloth, this law is a product of lessons learned in the wake of BIPA. Its language solves many of the worst problems created in Illinois. In addition to providing for a security and fraud exemption, for example, the Washington law specifies a scope that covers "enroll[ing] a biometric identifier in a database." This is substantially clearer and more appropriate than the overbroad language in the BIPA law covering any and all collection.

Of course, the Washington law could still be updated in places. For example, the "enroll" language could be further clarified by adjusting that law's "commercial purpose" language to generally align with the Virginia and Colorado omnibus privacy language addressing profiling that results in "consequential decisions" affecting the consumer. This would focus the law's application on impact to the consumer, rather than the Washington law's emphasis on whether biometric information is being used for a marketing purpose. With these and perhaps additional refinements, we believe that the Washington law is a sound starting point for a version that is tailored to the concerns of Maryland consumers while avoiding the problems caused by BIPA.

We thank you in advance for your continued work and consideration, which we hope will succeed in making Maryland a true leader in sound biometrics privacy protection. Of course, we would be happy to discuss any of these issues further with you, if helpful.

Respectfully submitted,

Anton van Seventer
Counsel

T +1 202 799 4642
F +1 202 799 5642
M +1 503 789 4852
anton.vanseventer@us.dlapiper.com

DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004

DLA PIPER

dlapiper.com