TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622
www.technet.org | @TechNetMidAtla1

February 7, 2023

The Honorable Melony Griffith
Miller Senate Office Building, 3 East Wing
11 Bladen Street, Annapolis, MD 21401

RE: SB 169 Biometric Data Privacy

Dear Chair Griffith and Members of the Committee,

On behalf of TechNet's member companies, I respectfully submit this letter of opposition to SB 169. TechNet's members place a high priority on consumer privacy; however, as drafted, this bill would create significant hardships for Maryland employers and could result in stifling important advances in safety and security for consumers.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over five million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, and Washington, D.C.

TechNet members recognize the importance of consumer privacy and the sensitivity of biometric data that can identify individuals. TechNet believes that privacy laws should provide strong safeguards for consumers, while allowing companies to innovate, provide security, and create jobs. Consumer trust is a top priority for our members, and that includes transparency on methods used to collect and use personal data. As currently drafted, this bill presents several problems for Maryland employers, consumers, and innovation.

Data Security

Biometrics has a critical role to play in the security and anti-fraud space, as it represents a generational improvement over "knowledge-based" security questions that are easily-answered – favorite foods, colors of first cars, etc. To ensure consumers retain cutting-edge protection, it is critical that laws regulating biometric privacy have an unqualified security and fraud exemption. Modern opt-in consent statutes in Washington, Virginia, and Colorado all recognize the crucial need for robust fraud and security exemptions. Unfortunately, the bill as drafted does not allow businesses that provide anti-fraud services to operate in a way that protects consumers. Using data to prevent and identify fraud, and protect consumers, should not be subject to this bill's requirements.

Processor Limitations and Consent

TechNet agrees with the spirit of the bill to limit processor uses of data through the contract with the private entity. However, a processor will not know, nor have the means to know, whether the private entity obtained the biometric information lawfully or with consent. For services and products where individuals are acutely aware of the biometric component, this creates unnecessary friction without further protecting consumer privacy.

Disclosing Biometric Data Without Confirmation

The bill still requires the disclosure of actual biometric information, without even confirming that the individual, or the "authorized representative", are who they say they are. This puts consumer information in danger of criminals and allows criminals to cover their tracks. No other privacy law requires the disclosure of biometric data.

Private Right of Action

TechNet opposes the inclusion of a private right of action because any unintentional or perceived violation could result in damaging liability for companies. The inclusion of a PRA 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. Studies have also revealed that private rights of action fail to compensate consumers even when a violation has been shown.

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

Well-meaning businesses, small and large, could be subject to frivolous lawsuits with little or no actual value delivered to the consumer. In turn, some businesses may choose to stop doing business in Maryland or be forced to cease operations altogether. The State Attorney General should have exclusive authority over any perceived violations. Every biometrics and omnibus privacy statute enacted, aside from the troublesome Illinois Biometric Information Privacy Act (BIPA), has relied on this exclusive authority.

TechNet joins industry partners and strongly encourages Maryland to look to the protections for consumers included in the Virginia, Colorado, and Connecticut omnibus privacy laws – protections that are, in fact, stronger than those that exist in the California privacy regime – that still require opt-in consent from the consumer but reflect a more modern and widely-accepted approach. We also urge you to consider that every single omnibus privacy bill enacted across the country to date includes biometrics protections. We believe it makes sense to consider how biometrics best fits into a larger consumer privacy conversation to further protect Maryland residents and businesses.

We would welcome the opportunity to work with your office to address issues of privacy protection without unintended consequences. Please consider TechNet's members a resource in this effort. Thank you for your time and we look forward to continuing these discussions with you.

Margaret Durkin

Margaret Durkin
Executive Director, Pennsylvania & the Mid-Atlantic
TechNet
mdurkin@technet.org