ANTHONY G. BROWN
Attorney General

CANDACE MCLAREN LANHAM
Chief of Staff

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

February 8, 2023

TO: The Honorable Melony Griffith, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 169 – Biometric Data Privacy – SUPPORT

The Office of the Attorney General supports Senate Bill 169 ("SB 169"), sponsored by Senators Feldman, Augustine, Brooks, Elfreth, Jackson, Jennings, King, Kramer, McCray, Rosapepe, Salling, Washington, and West. Senate Bill 169 provides Marylanders with privacy protections for biometric data to ensure that businesses do not keep this sensitive data longer than necessary, do not sell it, and obtain consumer consent before sharing it. Senate Bill 169 complements Maryland's Personal Information Protection Act which ensures that businesses that collect personal information maintain it securely[1] by creating timelines for the destruction of biometric data and restrictions on its transfer which, in turn, will reduce the number of breaches involving biometric data.

Biometric technologies measure and analyze people's unique physical and behavioral characteristics, such as fingerprints, iris scans, voiceprints, and facial recognition. Businesses currently use this information to, among other things, verify identity, customize the consumer experience, and enhance security. For example, the broad applications of facial recognition systems include supplanting time clocks at job sites,[2] replacing keys for housing units,[3] and aiding security at stadiums.[4] But it is important to recognize that biometric technology is not just

[1] The Maryland Personal Information Act covers biometric data, but it generally requires companies that collect or store consumers' personal information to: (1) reasonably protect it, and (2) notify consumers and the Attorney General's Office if there is a data breach that exposes that information. Md. Code Ann., Com. Law §§ 14-3503; 14-3504. Senate Bill 169 adds provisions specific to the unique nature of biometric data.

[2] *4 Reasons to Use Time Clocks With Facial Recognition*, Buddy Punch (Jun. 19, 2018), available at https://buddypunch.com/blog/time-clocks-facial-recognition.

[3] Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times (Mar. 28, 2019), available at https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html.

[4] Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y.

used when a consumer knowingly provides the information, such as when they use a fingerprint or facial scan to unlock their phones. In many cases, the general public is unknowingly surveilled and has little control over the application of this technology. For example, recently the owner of Madison Square Gardens Entertainment used facial recognition to identify and bar attorneys involved in disputes against the company from entering its venues.[5]

Senate Bill 169 establishes reasonable limits on the collection, use, and storage of biometric data. It prohibits businesses from collecting biometric data without consumer consent.[6] It also prohibits businesses from selling or sharing consumer biometric data.[7] In addition, SB 169 requires that biometric information be destroyed when it is no longer in use.[8] Several other states have already enacted laws to protect consumers' biometric information, including California[9], Illinois[10], Texas[11], and Washington.[12] And New York City, a city with a population larger than the entire State of Maryland, enacted a biometric ordinance that went into effect 18 months ago.[13] These protections are particularly important given the uniqueness of biometric identifiers. Unlike account numbers, once biometric data has been breached, it is compromised forever—you cannot change your fingerprint or iris if it gets stolen. Data thieves have already begun to target biometric data.[14]

Senate Bill 169 provides for an extremely limited remedy for individuals. Unlike the laws already in effect in Illinois and California, there is no broad private right of action. Instead, SB 169, like the New York City biometric law, provides for a private right of action only where a company violates the law by *selling* biometric data. And SB 169 further limits the scope of relief because an individual must suffer actual damages in order to recover. The scope of relief is thus very narrowly tailored and only provides for a remedy when a company profits off of violating the law and causes harm to an individual. Given the high cost when an individual's biometrics are compromised, businesses must be held accountable if they sell or misuse an individual's biometric data. A private right of action supplements the limited resources of the Attorney General's office and is necessary to ensure that accountability.

The Office of the Attorney General urges a favorable report.

Times (Mar. 13, 2018), available at https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

[5] https://www.rollingstone.com/music/music-news/madison-square-garden-face-scan-1234650989/.

[6] Section 14-4504(a)(1).

[7] Section 14-4503.

[8] Section 14-4502(a).

[9] Cal. Civ. Code § 1798.100 *et seq*.

[10] 740 ILCS 14.

[11] Tex. Bus. & Com. § 503.001.

[12] Wash. Rev. Code § 19.35.

[13] 2021 NYC Local Law No. 3, NYC Admin. Code §§ 22-1201–22-1205.

[14] Data thieves have already begun to target biometric data. In 2021, Nevada Restaurant Services, Inc. disclosed a privacy breach that exposed, among other personal information, customers' biometrics. https://www.prnewswire.com/news-releases/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event-301369180.html. And in 2019, data thieves breached an international database and gained access to more than a million fingerprints and other sensitive data, including photographs of people and facial recognition data. Scott Ikeda, *Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data*, CPO Magazine (Aug. 27, 2019), available at https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/.

Cc: Members, Finance Committee
The Honorable Brian Feldman
The Honorable Malcolm Augustine
The Honorable Benjamin Brooks
The Honorable Sarah Elfreth
The Honorable Michael Jackson
The Honorable J.B. Jennings
The Honorable Nancy King
The Honorable Benjamin Kramer
The Honorable Cory McCray
The Honorable Jim Rosapepe
The Honorable Johnny Salling
The Honorable Mary Washington
The Honorable Chris West