BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.
(410) 576-6566 (F)

WRITER'S DIRECT DIAL NO.
(410) 576-7296

January 27, 2021

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 16 – Biometric Identifiers and Biometric Information Privacy – SUPPORT

The Office of the Attorney General supports Senate Bill 16 ("SB 16"). SB 16 provides Marylanders with privacy protections for biometric data to ensure that businesses do not keep this sensitive data longer than necessary and do not sell it without consumer consent. SB 16 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.

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 for security purposes. For example, the broad applications of facial recognition systems include supplanting time clocks at job sites,[2] replacing keys for housing units,[3] aiding security at stadiums,[4] and expediting check-in at hotels.[5] But it is important to recognize that biometric technology is not just used when a consumer knowingly provides the information such

[1] The Maryland Personal Information Act covers biometric data, but it simply 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.
[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. Times (Mar. 13, 2018), available at https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.
[5] *Facial recognition is coming to hotels to make check-in easier—and much creepier*, Fast Company (April 1, 2019), available at https://www.fastcompany.com/90327875/facial-recognition-is-coming-to-hotels-to-make-check-in-easier-and-muchcreepier.

as when they use a fingerprint or facial scan to unlock their phones. In many cases, the general public is unknowingly surveilled and targeted by facial recognition and has little control over the application of this technology.

Businesses currently have few limitations on their ability to harvest and aggregate Marylanders' biometric information, and they have no restrictions on using this data once it has been collected. SB 16 establishes reasonable limits on the use and storage of biometric data. It prohibits businesses from selling or sharing biometric data without consumer consent.[6] The Division understands that Senator Augustine will be offering an amendment that helps ensure that consumer consent is knowing and voluntary and we fully support the amendment. SB 16 also requires that biometric information be destroyed when it is no longer in use.[7] These protections are particularly important given the uniqueness of biometric identifiers. Unlike account numbers, which can be changed if compromised, biometrics are unique to an individual—you cannot change your fingerprint or iris if it gets stolen. Data thieves have already begun to target biometric data; 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.[8]

Several other states have already enacted laws to protect consumers' biometric information, including California[9], Illinois[10], Texas[11], and Washington.[12] SB 16 does not go nearly as far as any of those laws. All it asks is that companies that use biometric identifiers discard them when they are no longer in use and that they not profit from this unique information without consumer consent.

The Office of the Attorney General urges a favorable report.

Cc: Members, Finance Committee
The Honorable Malcolm Augustine

[6] Section 14-4303(a)
[7] Section 14-4302(a).
[8] 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/.
[9] Cal. Civ. Code § 1798.100 *et seq*.
[10] 740 ILCS 14.
[11] Tex. Bus. & Com. § 503.001.
[12] Wash. Rev. Code § 19.35.