BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

February 2, 2022

TO: The Honorable C.T. Wilson, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: House Bill 259 – Biometric Identifiers Privacy – SUPPORT

The Office of the Attorney General supports House Bill 259 ("HB 259"), sponsored by Delegates Love, Carey, Charkoudian, Hill, Jackson, Lehman, R. Lewis, Qi, Rogers, and Watson. HB 259 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. HB 259 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 as when they use a fingerprint or facial scan to unlock their phones. In many cases, the general

[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.

public is unknowingly surveilled and has little control over the application of this technology.

HB 259 establishes reasonable limits on the collection, use, and storage of biometric data. It prohibits businesses from collecting biometric data without consumer consent. It also prohibits businesses from selling or sharing consumer biometric data.[6] In addition, HB 259 requires that biometric information be destroyed when it is no longer in use.[7] Several other states have already enacted laws to protect consumers' biometric information, including California[8], Illinois[9], Texas[10], and Washington.[11] 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.[12] 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.[13]

Like the laws already in effect in Illinois and California, HB 259 provides for a private right of action. 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.

Cc: Members, Economic Matters Committee
The Honorable Sara Love
The Honorable Ned Carey
The Honorable Lorig Charkoudian
The Honorable Terri Hill
The Honorable Carl Jackson
The Honorable Mary Lehman
The Honorable Robbyn T. Lewis
The Honorable Lily Qi
The Honorable Mike Rogers
The Honorable Courtney Watson

---

[6] Section 14-4404(a)
[7] Section 14-4402(a).
[8] Cal. Civ. Code § 1798.100 *et seq*.
[9] 740 ILCS 14.
[10] Tex. Bus. & Com. § 503.001.
[11] Wash. Rev. Code § 19.35.
[12]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. 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/.
[13] 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/.