

BRIAN E. FROSH
Attorney General

WILLIAM D. GRUHN
Chief

ELIZABETH F. HARRIS
Chief Deputy Attorney General



CAROLYN QUATTROCKI
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

(410) 576-6566 (F)

(410) 576-7296

February 26, 2020

TO: The Honorable Dereck E. Davis, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: House Bill 307 – Biometric Identifiers and Biometric Information Privacy
– SUPPORT WITH AMENDMENT

The Office of the Attorney General supports House Bill 307 (“HB 307”) with amendment. HB 307 provides Marylanders with privacy protections not currently available to them.¹ Several other states have already enacted laws to protect consumers’ biometric information, including California², Illinois³, Texas⁴, and Washington.⁵ Given the sensitivity of biometric information, this legislation is critically important.

Businesses currently have few limitations on their ability to harvest and aggregate Marylanders’ biometric information, and they do so frequently without consumer consent or knowledge. 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, facial recognition data, names, addresses and passwords.⁶ And unlike a stolen password or credit card number, biometric data cannot be changed.

HB 307 requires entities to provide notice and receive consent before collecting biometric information and prohibits businesses from selling or sharing biometric data.⁷ The bill grants

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 Cal. Civ. Code § 1798.100 *et seq.*

³ 740 ILCS 14.

⁴ Tex. Bus. & Com. § 503.001.

⁵ Wash. Rev. Code § 19.35.

⁶ 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/>.

⁷ Section 14-4203 (a)-(c).

individuals the power to protect their biometric information from collection. HB 307 also requires that biometric information be destroyed when it is no longer in use.⁸ These protections are particularly important when businesses collect highly sensitive personally identifiable information such as fingerprints and facial imagery. Maintaining this type of personally identifiable information is an invitation to data thieves. For years, cybersecurity experts have been spreading the mantra that “it’s not if you will get breached, but when.” With such a fatalistic view, it is critically important that we take proactive steps to limit the harm done by breaches before they occur, rather than waiting until after the damage is done.

Proposed Amendment to Conform Definitions to MPIPA

HB 307 defines “biometric identifier” as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.”⁹ The Office of the Attorney General believes that HB 307 should be amended to use the existing definition of biometric in MPIPA. MPIPA defines “biometric data” as: “[D]ata of an individual generated by automatic measurements of an individual’s biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual’s identity[.]”¹⁰

With its amendment noted, the Office of the Attorney General urges a favorable report.

Cc: Members, Economic Matters Committee
The Honorable Sara Love

⁸ Section 14-4202(a).

⁹ Section 14-4201(b).

¹⁰ Md. Code Ann., Com. Law §§ 14-3501(e)(1)(i)(6).