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 28, 2021

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

FROM: Hanna Abrams, Assistant Attorney General

RE: House Bill 218 – Biometric Identifiers and Biometric Information Privacy – FOLLOW UP QUESTIONS

There were a number of questions that arose during yesterday's hearing that I was unable to address due to the simultaneous hearings of this bill in the House and the Senate. House Bill 218 offers very important protections for Marylanders whose biometric information such as fingerprints and iris scans is collected by businesses.

1. **Will HB 218 create massive liability for companies that we have seen in other states?**

This law was carefully drafted to avoid the issues that have led to concerns about private lawsuits against companies. The lawsuits about which concerns have been raised were filed alleging violations of the Illinois biometric law, which requires consent before collecting biometric data. Specifically, they alleged that companies had collected and used information about faces derived from photographs without user consent. HB 218 does not create these same concerns. Although the Division believes that businesses should be obtaining consent before collecting biometric data from consumers, HB 218 ***does not*** require companies to obtain consent when they collect biometric data and therefore does not create the same liability risks.

Second, HB 218, like the Washington law, specifically excludes photographs in the definition for "biometric identifier." Consumers have sued companies like Facebook, Google, Shutterfly, and Snapchat whose services involve allowing users to group their photographs by automatically recognizing faces. HB 218 does not create liability for scanning faces. In fact, HB 218 goes one step further than the Washington law – in addition to excluding photographs from the definition of "biometric identifier," it also explicitly excludes photographs from the definition of "biometric information."[1] In other words, if a person uploads a photograph to a service like Shutterfly and the service scans the photos, it does not qualify as "biometric information"; this law would not cover that photograph.

[1] "'Biometric information' does not include information derived from an item or a procedure excluded under the definition of a biometric identifier." Section 4301(c)(2).

Because HB 218 does not require consent at the collection point and excludes facial scanning from a photograph, it does not pose the same risks to businesses that the Illinois biometric law creates. HB 218 simply requires companies to maintain biometric data with reasonable security, destroy it after it is no longer in use, and refrain from selling it without consumer consent.

2. How does this bill compare with biometric laws in Illinois, Texas, and Washington?

A complete comparison would require lengthy analysis, but briefly, the key features include:

Illinois Biometric Information Privacy Act (BIPA)[2]

Under BIPA, a private entity cannot collect or store biometric data without first providing notice, obtaining written consent, and making certain disclosures. BIPA also bars the sharing of the data with others except in very narrow circumstances, and bars (without exception) the sale or profiting from the data. BIPA requires companies to destroy biometric data within three years after the person's last interaction with the company. BIPA also contains a private right of action that permits recovery of statutory damages $1,000 for negligent violations and $5,000 for intentional violations by any "aggrieved" person.

Texas Capture or Use of Biometric Identifier Act (CUBI)[3]

CUBI requires private entities who "capture" biometrics for a commercial purpose to provide notice and obtain consent. CUBI also requires companies to destroy biometric identifiers no later than one year after the initial purpose for collecting the data has been satisfied. CUBI prohibits companies from selling, leasing, or disclosing biometric identifiers without consent. CUBI contains an exemption to the consent requirement in the event of user's "disappearance or death."[4] Violations of CUBI can be subject to civil penalties of up to $25,000 per violation with no maximum cap, but it can only be enforced by the Texas Attorney General; there is no private right of action.

Washington Biometric Privacy Act[5]

The Washington law prohibits "enrolling" a biometric identifier for a commercial purpose without notice, consent and providing an opt out method. According to the statute, to "enroll" means "to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual."[6] There is no set retention period, so long as the biometric identifiers are not maintained longer than reasonably necessary. The Washington law contains the broadest exemption to the prohibition against selling: it allows a private party to sell a consumer's biometric data to third parties so long as the third party "contractually promises" not to further disclose or enroll the information.[7] It also creates a broad "security exemption," exempting entities that collect, capture, enroll, or store biometric identifiers "in furtherance of a

[2] 740 ILCS 14/1 to 14/99.
[3] Tex. Bus. & Com. Code Ann. § 503.001.
[4] Tex. Bus. & Com. Code Ann. § 503.001(c)(1)(A).
[5] RCW 19.375.010 to 19.375.900.
[6] RCW 19.375.010(5).
[7] RCW 19.375.020(3)(e).

security purpose."[8] The law does not provide for a private right of action, but allows for civil penalties of up to $2,000 per violation.

3. Are there any examples of biometric data breaches?

In 2019, the security service Suprema's Biostar software was breached exposing 23 gigabytes of data including pictures of users attached to facial recognition data and fingerprint data. Biostar is a web-based security platform that uses fingerprints and facial recognition for remote access from mobile devices. The technology was used by over 5,700 organizations in 83 countries to manage their fingerprint and facial recognition systems. [9]

Also in 2019, Perceptics, a US Customs and Border Protection (CBP) subcontractor, suffered a data breach exposing the biometrics of up to 100,000 people.[10] Specifically, the breached data included photos of people's faces used as part of the agency's facial recognition program. According to CBP, the subcontractor acted in violation of the agency's security and privacy rules at the time.

4. Will HB 218 lead to private plaintiffs obtaining criminal sanctions against companies?

No. This bill does provide for a private right of action, but will only allow aggrieved consumers to obtain monetary relief. Private individuals cannot obtain criminal penalties under HB 218.

HB 218 provides important protections to Marylanders and the Office of the Attorney General urges a favorable report.

Cc: Members, Economic Matters Committee
The Honorable Sara Love

[8] RCW 19.375.020(7).
[9] https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/
[10] https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/