March 29, 2022

The Honorable Chair Delores G. Kelley
Senate Finance Committee
Maryland General Assembly
Miller Senate Office Building
11 Bladen St., Annapolis, Maryland

Dear Chair Kelley and Members of the Committee:

We, a diverse coalition of civil rights and technology justice organizations, write to express strong opposition to amendments made in the House Economic Matters Committee to HB 259, the Biometric Data Privacy Act. We respectfully urge the Senate Finance Committee to strengthen the legislation by undoing the recent weakening amendments. We do not support the bill as currently amended and look forward to working with members of this Committee to restore the bill to a place where it will provide strong protection to Maryland residents against the full range of damaging, non-consensual collection and use of their sensitive biometric identifiers.

As introduced, HB 259 and its Senate counterpart, SB 335, imposed strong consent requirements before businesses can collect or use our unique biometric identifiers, as well as an effective enforcement mechanism in the form of a private right of action. House amendments to HB 259 have weakened these and other provisions of the bill in the following ways:

1. **Serious deficiencies in consent requirements:** Consent is no longer required for the collection, use, or disclosure of biometric identifiers for "fraud prevention or security purposes." In lieu of a consent requirement, businesses only need to post written notice at the entrances to a facility using biometric collection technology. Although the amended bill gestures at narrowing this exception by requiring such collection, use, or disclosure to be "directly tied to the service being provided by the private entity", and "only … what is strictly necessary" for fraud prevention and security purposes, this language fails to protect Maryland residents against abuse. The amended bill would leave undisturbed some of the most troubling uses of face recognition technology by businesses, including those which have resulted in Black people being turned away or ejected from business premises as a result of a false face recognition "match" to a photo of a suspected shoplifter or someone else barred from entry. Additionally, companies like Clearview AI, which has amassed a database of more than 10 billion faceprints and aims to reach 100 billion in the next year, would likely claim the benefit of this exception to continue collecting people's biometric identifiers en masse, without obtaining consent.

2. **Severe narrowing of the private right of action:** The private right of action (PRA) is severely restricted to cover only violations of the bill's ban on the sale of biometric identifiers. Enforcement of any other violation of the Act (including the core requirement of consent for the collection, use, or disclosure of biometric identifiers) is limited to state regulators and the state Attorney General. Because government agencies lack the resources and personnel to fully enforce the protections of this law, the amendment will mean that Maryland residents whose rights are violated will lack redress and that businesses will not have adequate incentives to comply with the law. Importantly, non-consensual collection, use, and disclosure of our biometric identifiers open us up to exactly the same dangers as the sale of that data: risks of identity theft, persistent tracking, and civil rights harms.

   Moreover, the remaining PRA has additional new limitations, including the elimination of the statutory damages provision, meaning that people can only obtain a remedy if they can prove actual damages. Because the harms of privacy violations can be extremely difficult to identify or prove, statutory damages provisions are common in privacy and consumer protection laws and are critical to ensuring that people can obtain redress for violations of their rights. House amendments have also eliminated the ability to seek injunctive or declaratory relief, which are important tools for ending ongoing violations.

3. **Introduces uncertainty to the definition of biometric identifier.** The House amendments deleted "faceprints" from the definition of biometric identifier (now called "biometric data"). Although the catch-all definition would still encompass the collection of faceprints, this term should be restored to the exemplary list of biometric identifiers in order to avoid costly and unnecessary litigation later. Face recognition technology is perhaps the fastest-growing, and most concerning, type of biometric collection technology today, and the bill should leave no doubt that protections against abuse apply to it.

4. **Creates an expansive loophole to disclose people's biometric identifiers to the government without legal process.** The original bill allowed law enforcement to obtain information with a valid warrant or subpoena. The amendments go far beyond that reasonable provision, by allowing the government to request people's biometric identifiers if there is a "reasonable" and "good faith" belief that a law has been violated. This will result in unjustified violations of Marylanders' privacy.

We cannot in good faith support this legislation unless, at a minimum, the following changes are made:

- Restore the consent requirement for all collection, use, and disclosure of biometric identifiers by private entities;
- Restore the strong private right of action for violations of the core protections of this bill, including the consent requirement for collection, use, and disclosure of biometric identifiers;
- Restore the term “faceprint” to the definition of biometric identifier (now called “biometric data”); and
- Delete the new expansive exception for voluntary disclosures to law enforcement, leaving the reasonable exception for responding to valid legal process.

We welcome the opportunity to discuss ways the Committee can strengthen this legislation to create strong and enforceable privacy protections that all Marylanders deserve to have. If you have any questions, please contact Daniel Marks, American Civil Liberties Union, at dmarks1@aclu.org.

Sincerely,

Access Now
ACLU
Consumer Federation of America
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
Privacy Rights Clearinghouse