



Consumer Federation of America

1620 I Street, N.W., Suite 200 * Washington, DC 20006

January 31, 2022

The Honorable Chair C.T. Wilson, Esq.
House Economic Matters Committee
Maryland General Assembly
Lowe House Office Building, Room 231
6 Bladen St., Annapolis, MD 21401

RE: Support Biometric Identifiers Privacy Act, HB 259

Dear Chair Wilson and Members of the Committee:

Consumer Federation of America (CFA), an association of more than 250 consumer organizations across the United States, including in Maryland, urges you to support HB 259, the Biometric Identifiers Privacy Act (BIPA). Biometric identifiers such as faces, voices, fingerprints, and retinas are the most intimate types of data about individuals, and the most immutable. Unlike account numbers, addresses and even names, biometric identifiers cannot be changed. If they are misused or shared inappropriately, or not adequately safeguarded, the harm to individuals may be significant and difficult to resolve.

Alarms have been raised, for instance, about Clearview, a company that collects photographs of people from social media sites and other sources on the internet and uses them to offer face recognition services to law enforcement agencies and other customers.¹ Not only are the photos gathered and used without the individuals' knowledge or consent, but face recognition technology is notoriously inaccurate in some circumstances, especially in identifying Black people.² A Reuters investigation found that Rite Aid was using face recognition to attempt to identify shoplifters in stores predominately located in "tough" neighborhoods, and that the system "regularly" misidentified people, who were wrongly labeled as miscreants and forced to leave the stores.³ The company claimed that individuals were notified about the use of this technology through signage in the stores.

Simply entering a place of business should not be considered consent to have one's biometric identifiers collected, used and shared. Furthermore, it is unfair to make people choose between being able to obtain the products and services they need and being subject to this type of privacy-invasive and discriminatory practice, particularly in communities where there may be little choice of businesses to patronize.

¹ See J. Dale Shoemaker, "If your face is online, SC police may have had access to it. What does this mean for you?" The Sun News (June 29, 2021), available at <https://www.msn.com/en-us/news/technology/if-your-face-is-online-sc-police-may-have-had-access-to-it-what-does-this-mean-for-you/ar-AALAIoA>.

² See blog by Alex Najibi, "Racial Discrimination in Face Recognition Technology," Harvard University Graduate School for Arts and Sciences (October 24, 2020), available at <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>.

³ See Jeffrey Dastin, "Rite Aid deployed facial recognition systems in hundreds of U.S. stores," Reuters (July 28, 2020), available at <https://www.reuters.com/investigates/special-report/usa-riteaid-software/>.

Of course, face recognition is not the only use of biometrics that is concerning. Last year CFA and a number of other groups wrote to Red Rock Amphitheater and event promoters urging them not to use Amazon's One Palm scanning technology or any other biometric surveillance.⁴ Iris scans, fingerprints and other biometric identifiers are also increasingly being used for commercial purposes.

States have begun to address the need to ensure biometric privacy and security for their residents. Illinois, Texas, and Washington – very different states in terms of population and politics – have enacted laws in this regard. Now similar safeguards are being proposed in Maryland. BIPA would:

- Require companies to provide notice and obtain written consent before collecting, using, or disclosing individuals' biometric identifiers such as iris, face, voice, and palm prints and fingerprints.
- Require businesses to delete biometric identifiers one year after individuals' last interaction with them or upon individuals' request.
- Require individuals' biometric identifiers to be safeguarded against unauthorized disclosure when collected, stored, and used.
- Prohibit companies from disclosing or sharing individuals' biometric identifiers without consent, except under very specific circumstances as required by law.

The Maryland legislation also has a private right of action, a crucial provision that has enabled Illinoisans to hold companies like Clearview and Facebook accountable for breaking the law by capturing and using people's biometric identifiers without consent.⁵ People must be able to enforce their rights. No state attorney general has sufficient resources to bring legal action in every case in which that is merited. Private rights of action are essential to obtain redress for consumers and change business practices for the better.

Maryland will protect its residents and be a leader in biometric privacy and racial justice by enacting BIPA. We ask you to advance HB 259 with a favorable report. Thank you for considering our views on this important issue.

Sincerely,



Susan Grant, Senior Fellow
Consumer Federation of America

⁴ See <https://consumerfed.org/testimonial/groups-ask-event-venues-and-promoters-to-reject-use-of-amazon-palm-scanning-technology/>.

⁵ Facebook was sued under the Illinois law for tagging users' photos using facial recognition without their consent, see Taylor Hatmaker, "Facebook will pay \$650 to settle class action suit centered on Illinois privacy law," TechCrunch (March 1, 2021), available at <https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/>.