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

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

Dear Chair Wilson, Chair Kelley, and Members of the Committees:

We, the undersigned civil rights, civil liberties, and community-based organizations, write to ask for your favorable support of HB0259 and SB033*5, the Biometric Identifiers Privacy Act (BIPA)*. Biometric identifiers, which represent the unique measurements of our faces, voices, fingerprints, retinas, and other biological characteristics, should remain under the control of each individual. Corporate interests should not be permitted to collect this data and use it for commercial purposes without people's knowledge and expressed consent.

Unregulated corporate uses of biometric identifiers pose profound and unprecedented threats to upholding crucial civil rights and civil liberties of Maryland residents. For these reasons, **we specifically urge you to pass legislation that establishes limits on how companies can collect and handle Maryland residents' sensitive biometric identifiers** in the following ways:

- Require companies to provide notice and obtain written consent before collecting, using, or disclosing a person's biometric identifier (including iris, face, voice, and palm prints; fingerprints; etc).
- Require businesses to delete a Marylander's biometric identifiers one year after the individual's last interaction with the business or upon the individual's request,
- Require safeguards against unauthorized disclosure when individuals' data is collected, stored, and used;
- Prohibit companies from disclosing or sharing an individual's biometric identifiers without consent, except under very specific circumstances as required by law.

As companies like Clearview, Facebook, Amazon, and others invest in developing biometric technologies for the purposes of their own profit, we are in danger of losing control over the most basic elements of our privacy and security. Companies have demonstrated their inability to proactively self-regulate by repeatedly capturing people's biometric identifiers without consent, using them in harmful ways, and failing to protect them against disclosure.[1]

[1] Arisha Hatch, Big Tech companies cannot be trusted to self-regulate: We need Congress to act, TechCrunch, March 2021. https://techcrunch.com/2021/03/12/big-tech-companies-cannot-be-trusted-to-self-regulate-we-need-congress-to-act/

BIPA will ensure that everyone in Maryland retains control over their biometric identifiers while still being able to avail themselves of useful services those identifiers might enable. It will also ensure that Marylanders can hold companies that violate their biometric privacy accountable, by allowing them to take companies that violate these protections to court.

Presently, Maryland law places zero restrictions on the ways corporations can collect, use, and even sell Maryland residents' biometric identifiers. This means that companies can secretly use face recognition technology, fingerprint and iris scanners, and other technology, to easily identify and track people, including patients at drug treatment centers, teenagers at clothing stores, families at grocery stores, concerned citizens attending protest demonstrations, or other various forms of personal tracking in places of public accommodation.

If companies lose control of biometric identifiers they have collected, through hacking, leaks, or employee misconduct, those identifiers could be used to access people's sensitive private devices, accounts, and physical spaces. This creates extreme risks to the privacy and security of all Maryland residents. Moreover, because of flaws in how some biometric technologies operate and disparities in how they are deployed, the harms of non-consensual collection of biometric identifiers fall disproportionately on people of color and members of other marginalized communities.

Biometric technology has proven to be inaccurate and discriminatory.[2]

Certain biometric identification technologies – particularly facial recognition technologies – currently do not perform to the standards advertised by their creators. **This technology is particularly dangerous to Black people, LGBTQ people, people with disabilities, women, immigrants, Brown people, sex workers, and members of other marginalized communities.** For example, MIT scholar Joy Buolamwini discovered that facial recognition systems did not detect her face until she placed a white mask over it. A Black woman and doctoral candidate at the MIT Media Lab, Buolamwini decided to investigate. In her landmark 2018 study, Buolamwini and her colleagues reported alarming racial and gender disparities in a range of facial recognition and classification technologies marketed by some of the most prominent technology companies in the world. While the systems were relatively accurate when analyzing the faces of white men, Buolamwini found they failed up to 1 in 3 times when classifying the faces of Black women.[3] Subsequent studies, including by the federal government's National Institute of Standards and Technology, demonstrate that face recognition technology has

[2] https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/
[3] Joy Buolamwini et al., "Gender Shades," MIT Media Lab, available at https://www.media.mit.edu/projects/gender-shades/overview/

significantly higher rates of misidentification when used on people of color, with Asian and African American people up to 100 times more likely to be misidentified than white men.[4]

Likewise, a 2018 ACLU of Northern California facial recognition technology test revealed that Amazon's facial surveillance product 'Rekognition' falsely matched 28 Members of Congress with a mug-shot database. Although Rekognition falsely matched legislators across party, gender, age, and racial and geographic demographics, the test revealed a disproportionate error rate.[5] More specifically, six members of the Congressional Black Caucus were misidentified, including civil rights hero Rep. John Lewis (D-Ga.).[6]

The use of flawed biometric identification technologies can have real, harmful consequences. Last year, a Detroit-area roller skating rink threw out a 14-year-old Black girl because the rink's facial recognition system wrongly identified her as a different person suspected of disrupting the rink's business.[7] Her mother had already driven away after dropping her off, and she was left outside, alone. Had strong biometric information protections been in place, this traumatic experience would never have happened to her.

Similarly, a 2020 Reuters investigation revealed that **RiteAid had quietly deployed face recognition cameras in hundreds of its stores–including in Baltimore–with the cameras mostly placed in stores "in largely lower-income, non-white neighborhoods."**[8] RiteAid employees told Reuters that the system "regularly misidentified people," and in particular that "it doesn't pick up Black people well." Misidentifications resulted in people being incorrectly flagged as matches with photos of past shoplifting suspects and being told to leave stores before completing their purchases.[9]

The surveillance and tracking of Black people, in particular, has a pernicious and largely unaddressed history, beginning during the antebellum era. From 18th-century lantern laws (when Black, mixed-race, and Indigenous enslaved people carried lanterns with them if they were out after sunset)[10] to the FBI and police surveillance of Black activists in recent years,[11] Black people have been, and continue to be, targeted for simply existing. Incidents like the latter are largely underreported because surveillance is pervasive and unregulated. By supporting BIPA,

---

[4] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[5] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers*, N.Y. Times (Jul. 26, 2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html

[6] https://www.aclunc.org/blog/amazon-s-face-recognition-falsely-matched-28-members-congress-mugshots

[7] https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her

[8] https://www.reuters.com/investigates/special-report/usa-riteaid-software/

[9] *Ebid.*

[10] https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/

[11] https://www.aclu.org/press-releases/leaked-fbi-documents-raise-concerns-about-targeting-black-people-under-black-identi-1

legislators in the Maryland General Assembly can hold corporations accountable for racializing surveillance technology.[12]

Private rights of action are required to hold companies accountable.

Without a strong enforcement mechanism, the law will fail to hold corporations accountable for misconduct.[13] The private right of action is necessary to ensure that people's rights can actually be protected and vindicated. Illinois' experience is instructive.[14] Since the Illinois Legislature unanimously passed BIPA in 2008, Illinoisans have been able to hold companies like Facebook[15] and Clearview AI accountable for clearly breaking the law by capturing and using people's biometric identifiers without consent. One lawyer whose firm represented Facebook users in a suit said it best, "From people who are passionate about gun rights to those who care about women's reproductive issues, the right to participate in society anonymously is something that we cannot afford to lose"--and enabling people to sue when their rights are violated helps to ensure that we won't.[16]

In contrast, in Texas and Washington, which have similar biometric privacy laws but without a private right of action, residents have not been able to enforce their biometric privacy rights. The state attorney general simply lacks the resources and staffing to enforce this law against all of the companies that may seek to profit off of people's biometric identifiers. **The inclusion of a private right of action will also save the state time and money. Rather than asking the government to invest hours and dollars in lawsuits, individuals will be able to vindicate their own rights.**

Focus groups conducted in 2021 found that Maryland voters, across racial and ideological lines, strongly support BIPA and agree that it should be a high priority for state legislators.[17] Voters were presented with the most persuasive arguments for and against, and each time voters came out believing that the benefits of the policy outweigh any concerns. When presented with information about the private right of action, voters uniformly rejected the idea that the law

---

[12] https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/
[13] Adam Schwartz, You Should Have the Right to Sue Companies That Violate Your Privacy, EFF, January 2019. https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy; https://www.nytimes.com/2019/01/06/opinion/facebook-privacy-violation.html
[14] https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying
[15] https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEBrHbxKPyHPswRRR0DSB6DKl2M9R0EBZOxNcySbBlwamvYP6BIUlBLI3H0pxpUJbN2WxW5dnBHep21MFvJZDMkhBQUJQWydNycnJJXGXR0BB9Nz2TLKGT60aE_knpKS9h81g_wUGH-GZNO7-9lzibAkpYKMcwB3HDqK2nXCbhMh
[16] https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html
[17] Strategies 360 conducted four virtual focus groups on December 1st-2nd, 2021 among (1) moderate/conservative Black Democrats, (2) Black women, (3) White moderate suburban Democrats, and (4) White Republicans and right-leaning independents. Participants came from 12 counties across the state and reflected a range of levels of educational attainment, socioeconomic status, and background.

would hurt Maryland's economy and believed this would ensure a level of accountability against companies who might otherwise escape responsibility. Maryland voters and experts agree: legislators should grant ordinary Maryland residents the power to defend their own privacy.

Currently, decisions about how to use this dangerous technology are being made by private entities behind closed doors. Legislators can change this.

Maryland has the chance to become a leader in biometric privacy and racial justice, and the time is now. We urge you to vigilantly and vigorously protect the privacy rights of your constituents by passing the Biometric Identifiers Privacy Act. By ensuring that control and power remain in the hands of Maryland residents, this law will protect privacy while also creating the trust necessary to promote innovation. We respectfully ask this Committee to advance HB0259 and SB0335 with a favorable report.

Thank you for your consideration of this urgent matter. If you have any questions, please contact Daniel Marks, American Civil Liberties Union at dmarks1@aclu.org.

Sincerely,

Access Now

ACLU

Center for Democracy and Technology

Color Of Change

Consumer Federation of America

Defending Rights and Dissent

Electronic Frontier Foundation (EFF)

Electronic Privacy Information Center (EPIC)

Encode Justice

Kairos Action

Maryland Consumer Rights Coalition

Maryland PIRG

Restore the Fourth

S.T.O.P