Testimony for the House Economic Matters Committee
February 2, 2022

HB 259 – Commercial Law – Consumer Protection – Biometric Identifiers Privacy

SUPPORT

The ACLU and ACLU of Maryland support HB 259, which would require that companies obtain individuals' consent before collecting, using, or disclosing those individuals' sensitive biometric identifiers. This is a crucial and reasonable protection that will allow people and companies to enjoy the benefits of advances in technology while helping to prevent abuse. Illinois has had a similar law on the books for more than a dozen years.[1] Maryland should follow suit.

Biometric identifiers, including fingerprints, iris and retina scans, facial recognition scans, and voiceprints, are unique to each individual. They can be used to instantaneously identify and track people, and if they are disseminated or leaked, the harm may be irreparable because, unlike a credit card number or social security number, they cannot be changed. Without strong and enforceable legal protections, Maryland residents will be left vulnerable to violations of their privacy, security, and civil rights. Those risks will be experienced by everyone, but members of marginalized and vulnerable communities—including people of color, LGBTQ people, immigrants, survivors of intimate partner violence, and others—will experience some of the greatest harms. Abusive collection and use of biometric identifiers is becoming increasingly widespread, and the time for the Legislature to act is now.

HB 259 would provide the following protections, which are currently lacking under Maryland law:

- Require companies to provide notice and obtain written consent before collecting, using, or disclosing a person's biometric identifier (including iris, face, voice, palm, and finger prints);
- Prohibit companies from withholding services from people who choose not to consent to collection or use of their biometric identifiers;
- 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;

[1] Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/1–14/25.

- Require safeguards against unauthorized disclosure when an individual's biometric identifier 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; and
- Saves taxpayer dollars by empowering individuals to sue companies who violate their rights under the act.

Without these safeguards, Maryland residents will remain unprotected from privacy, security, and civil rights harms stemming from collection, use, and dissemination of their personal biometric identifiers without consent.

Collection and use of biometric identifiers without consent violates Marylanders' privacy

Recent advances in technology have given corporations incredible powers to quickly identify, track, and surveil people through collection and analysis of biometric identifiers. These capabilities can be used both to identify people in an instant, and to pervasively track their movements in the physical world and online, such as by using face recognition to automatically track a person across a network of video surveillance cameras. The ability of these technologies to capture biometrics at a distance, or from video and photos, can easily be carried out without knowledge or consent of affected individuals. Even biometric identifiers that traditionally had to be collected from individuals in-person, such as fingerprints and iris scans, can now be captured remotely.[2] Without the protections of HB 259, people may never know they have been identified or tracked, much less have the ability to refuse consent.

These concerns are not hypothetical. The face recognition company Clearview AI has amassed a database of more than 10 billion faceprints captured from photos of people it has downloaded from their social media pages and other websites—all without providing notice to those people or obtaining their consent.[3] Clearview's customers can upload an individual's photo and use the company's face recognition software to match the photo against other photos of the same person in the database, providing a chilling ability to identify people and create a record of their activities and associations online. Until recently, Clearview's thousands of users included

[2] Thomas Brewster, *Inside America's Secret $2 Billion Research Hub*, Forbes (July 13, 2020), https://www.forbes.com/sites/thomasbrewster/2020/07/13/inside-americas-secretive-2-billion-research-hub-collecting-fingerprints-from-facebook-hacking-smartwatches-and-fighting-covid-19/#293521ad2052; Brook Hays, *Iris Scanner Can ID a Person from 40 Feet Away*, UPI (May 22, 2015), https://www.upi.com/Science_News/2015/05/22/Iris-scanner-can-ID-a-person-from-40-feet-away/7071432303037/.

[3] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

retailers like Best Buy, Macy's, Kohl's, Walmart, and Home Depot; banks including Bank of America and Wells Fargo; private investigators and law firms; the NBA; and wealthy socialites.[4] One New York billionaire used Clearview's app to surreptitiously identify his daughter's new boyfriend when he came across his daughter out on a date; he later bragged that he used the app to capture people's faceprints "as a hobby."[5] Only after Illinois residents sued Clearview for capturing their faceprints without consent in violation of the Illinois Biometric Information Privacy Act did the company promise to stop offering access to corporations and private individuals.

The ACLU is currently suing Clearview under the Illinois law, representing organizations that work with undocumented immigrants, survivors of sexual assault and domestic violence, current and former sex workers, and individuals who regularly exercise their right to protest. By capturing and selling access to people's biometric identifiers without consent, Clearview has threatened to empower abusive ex-partners and serial harassers, exploitative companies, and others to track and target members of these vulnerable communities. For example, for a survivor of intimate partner violence, even obtaining a legal name change and moving across the state would not be enough to evade an abusive ex-partner with access to this technology; a single photo of the survivor tagged with their new name and uploaded by an acquaintance to an obscure corner of the internet would be enough for the abuser to track them down. Illinois law protects against these abuses. Maryland law should too.

Although Clearview's conduct is particularly egregious, it is far from the only company to have secretly collected people's biometric identifiers and used them in ways most people would never have agreed to had they known about it. One company that marketed an online digital photo storage service secretly used people's uploaded photos to train a face recognition system that it sold to police.[6] Numerous retailers, concert venues, and stadiums have begun quietly using face recognition technology to identify and track shoppers and event attendees.[7] Few of these

---

[4] Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And The NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement; Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.

[5] Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, *supra* note 4.

[6] Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools*, NBC News (May 9, 2019), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

[7] Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, N.Y. Mag. (Oct. 20, 2018), https://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html; BBC News, *Musicians Call for Facial Recognition Ban at Gigs* (Sept. 10, 2019), https://www.bbc.com/news/technology-

companies are willing to disclose their use of biometric technologies; when the ACLU asked 20 top American retailers whether they used face recognition cameras on their customers, only two would answer.[8] Landlords have started installing face recognition systems in apartment buildings, granting themselves the power to automatically track the comings and goings of every resident, and to identify their guests and romantic partners as they arrive and depart.[9] The notice and consent requirements in HB 259 would be critical protection against such abuse.

Collection and storage of biometric identifiers without consent puts Marylanders at risk of data breaches and identity theft.

The protections in HB 259 are also critical for helping people keep control over their biometric identifiers, thus securing them against inclusion in companies' databases that may be subject to breaches or other damaging dissemination. Unlike many forms of sensitive data, such as a passport number, credit card number, or even Social Security number, we cannot change our biometric identifiers after they have been stolen or misused. Unfortunately, breaches of databases containing people's biometric identifiers are all too common, putting people at risk of identity theft and similar harms. Examples include:

- The security company Suprema, which sells biometric lock systems to control access to secure areas, left the "fingerprints of over 1 million people, as well as facial recognition information" exposed in a publicly accessible database.[10]
- Students who were required to use the remote exam proctoring company ProctorU have sued alleging that their biometric identifiers were exposed in a data breach that affected

49647244; Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

[8] Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?*, ACLU (Mar. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face.

[9] Tanvi Misra, *The Tenants Fighting Back Against Facial Recognition Technology*, Bloomberg CityLab (May 7, 2019), https://www.bloomberg.com/news/articles/2019-05-07/when-facial-recognition-tech-comes-to-housing; Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. Times (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html.

[10] Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, U.K. Police and Defence Firms* (Aug. 14, 2019), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

the records of almost 500,000 students.[11] Maryland colleges are among those that use ProctorU.[12]

- A ransomware attack on the Personal Touch Holding Corporation exposed the data of more than 33,000 Marylanders last year. Fingerprints were among the data exposed.[13]
- Breaches of Continental Airlines and a company called Trade Center Management Associates, LLC, in 2009 and 2010 exposed hundreds of Maryland residents' fingerprint data.[14]
- A cyber attack on a private company contracting with the federal government compromised approximately 184,000 images of travelers from a facial recognition pilot program operated by U.S. Customs and Border Protection.[15]

HB 259's requirements of notice and consent, its requirement that companies delete people's biometric identifiers after a specified time period or upon request, and its limitations on how biometric identifiers are stored, used, and disseminated will help minimize the risk of sensitive biometric identifiers being lost to hacks or data leaks like these.

Collection and use of biometric identifiers without consent subjects Marylanders to discrimination and other civil rights harms

Multiple studies by the federal government, academic researchers, and the ACLU show that face recognition algorithms have markedly higher misidentification rates for Black people, people of color, women, and children.[16] Face classification algorithms, which seek to identify people by

[11] Kirsten Errick, *Students Sue Online Exam Proctoring Service ProctorU for Biometrics Violations Following Data Breach*, Law St. Media (Mar. 15, 2021), https://lawstreetmedia.com/news/tech/students-sue-online-exam-proctoring-service-proctoru-for-biometrics-violations-following-data-breach.

[12] *See, e.g.*, Montgomery College, *Academic Testing*, https://www.montgomerycollege.edu/admissions-registration/academic-testing.html (last visited Jan. 28, 2022).

[13] Md. Office of the Att'y General, *Maryland Information Security Breach Notices* (Mar. 23, 2021), available at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx#InplviewHashac628f51-0774-4b71-a77e-77d6b9909f7e=WebPartID%3D%7BAC628F51--0774--4B71--A77E--77D6B9909F7E%7D.

[14] Baltimore Sun, *Data Breach Disclosures* (last updated 2014), http://data.baltimoresun.com/from-cms/ag-incident-reports/.

[15] Office of the Inspector General, U.S. Dep't of Homeland Sec'y, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot (Sept. 21, 2020), available at https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[16] *See* Nat'l Inst. of Standards and Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; John J. Howard, Yevgeniy B. Sirotin & Jerry L. Tipton, *Quantifying the Extent to*

demographic category, have likewise been shown to be significantly less accurate when used on people of color, transgender and gender nonconforming people, and women.[17] Other biometric technologies that purport to be able to infer information beyond identity, such as face scanning to determine a person's emotional state or eye scanning to detect whether they are telling the truth, are similarly, if not more, flawed.

The harms of using these faulty biometric technologies are very real. In Michigan, a 14-year-old Black girl was ejected from a skating rink after a face recognition system incorrectly matched her to a photo of someone who was suspected of previously disrupting the rink's business.[18] The rink made the girl, who had never been to the rink before and whose mother had already left after dropping her off, leave the building. During the Covid-19 pandemic, students of color have reported that face recognition technology in remote exam proctoring software has failed to recognize them, threatening to lock them out of important academic and professional-licensing exams.[19]

When biometric technologies are disproportionately deployed in communities of color, the harms are compounded. When Rite Aid quietly deployed face recognition cameras to look for shoplifters, it installed them almost exclusively in stores in low-income communities of color, subjecting shoppers in those neighborhoods—but not nearby higher income and whiter neighborhoods—to biometric tracking. Predictably, because the technology worked relatively poorly on people of color, it resulted in at least one case of a Black shopper being told to leave a store based on an incorrect match to a photo of a suspected shoplifter.[20] Rite Aid installed face recognition cameras in a number of cities, including Baltimore.

---

which Race and Gender Features Determine Identity in Commercial Face Recognition Algorithms, Dep't Homeland Sec'y Sci. & Tech. (May 2021), https://www.dhs.gov/sites/default/files/publications/quantifying-commercial-face-recognition-gender-and-race_updated.pdf; K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race* (2019), https://arxiv.org/abs/1904.07325; Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 6, 1789–1801 (Dec. 2012), available at https://ieeexplore.ieee.org/document/6327355; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU Free Future (July 26, 2018), https://bit.ly/2OkETHe.

[17] Joy Buolamwini & Timni Gebru, *Gender Shades*, 81 Proc. of Machine Learning Rsch. 1 (2018), available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[18] Randy Wimbley & David Komer, *Black Teen Kicked Out of Skating Rink After Facial Recognition Camera Misidentified Her*, Fox2 Detroit (July 14, 2021), https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her.

[19] Monica Chin, *ExamSoft's Proctoring Software Has a Face-Detection Problem*, The Verge (Jan. 5, 2021), https://www.theverge.com/2021/1/5/22215727/examsoft-online-exams-testing-facial-recognition-report.

[20] Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, Reuters (July 28, 2020), https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

Companies are now using face recognition technology in numerous other troubling ways. Walgreens, for example, is deploying "face-detection technology that can pick out a customer's age and gender" and show them tailored ads.[21] This invasive practice raises concerns about shoppers being steered to discounts or products based on gender stereotypes. Even more consequentially, face and voice recognition technology is being used to collect and analyze biometric data during employment interviews. Vendors of predictive interview hiring tools dubiously claim to measure an applicant's skills and personality traits through automated analysis of verbal tone, word choice, and facial expressions.[22] This technology raises an enormous risk of amplifying employment discrimination against people due to accents, disabilities, skin color, or because they are transgender, nonbinary, or gender nonconforming.[23] Indeed, Maryland has already recognized these problems in the employment context, prohibiting use of face recognition technology during job interviews without the applicant's consent.[24] The General Assembly now has the opportunity to protect Marylanders against similar harms in other areas as well.

A private right of action is essential to ensuring Marylanders' rights

One of the most important aspects of HB 259 is its enforcement mechanism, a private right of action for individuals whose rights have been violated. The scale and scope of potential harms associated with exploitation of people's sensitive biometric identifiers are too extensive to be left to overburdened state agencies, or to promises of self-policing by companies.

Without a private right of action, people have little practical ability to seek relief in cases where their biometric identifiers are unscrupulously collected or misused. This eliminates a powerful tool that can incentivize companies to comply with the law in order to avoid lawsuits. Where companies nonetheless choose to ignore the law, the private right of action allows affected individuals to obtain redress for the harm they have suffered.

---

[21] Kiely Kuligowski, *Facial Recognition Advertising: The New Way to Target Ads at Consumers*, Bus. News Weekly (Dec. 21, 2021), https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html.

[22] Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn (2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[23] Ctr. for Democracy and Tech., *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?* (2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf.

[24] H.B. 1202 (2020), codified at Md. Code Ann., Lab. & Empl. § 3-717.

A private right of action is also important because government agencies often do not have the financial and personnel resources to investigate and take action in every case—or sometimes any case—where people's rights are violated. The experience of the three states that have enacted biometric privacy laws is instructive. In Illinois, where the law includes a private right of action, state residents have been able to sue technology companies like Clearview AI, Facebook, and Google for collecting and using their biometric identifiers without consent, and this has led to those companies changing their practices. In Texas and Washington State, on the other hand, where there is no private right of action, there are *no* documented enforcement actions by those states' attorneys general against companies that violated their laws. State regulators simply have not kept up with companies' practices. A biometric privacy law that is never enforced is unlikely to deter companies from committing violations.

A private right of action both conserves state resources, and ensures that state residents can vindicate their own rights. As the California Attorney General put it when supporting a private right of action in a recently enacted consumer privacy law, "The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the [Attorney General's Office's] need for new enforcement resources. I urge you to provide consumers with a private right of action."[25]

Also critical is HB 259's statutory damages provisions, which permits individuals who prevail in their lawsuits to recover reasonable money damages without needing to document tangible damages. Because nonconsensual capture of biometric identifiers often happens in secret, the resulting harms can be extraordinarily hard to quantify and trace. Statutory damages provide a way to meaningfully enforce the law. Numerous privacy and consumer protection statutes at the state and federal level include statutory damages provisions.[26]

* * *

For the foregoing reasons, the ACLU and ACLU of Maryland support HB 259 and urge a favorable vote.

---

[25] Letter from Xavier Becerra, California Attorney General, to Ed Chau, California Assemblymember, and Robert Hertzberg, Senator (Aug. 22, 2018) available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical.

[26] *See, e.g.*, Md. Code Ann., Com. Law § 14-3003; Md. Code Ann., Com. Law § 14-3807; Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/20; Fair Debt Collection Practices Act, 15 U.S.C. § 1692k; Right to Financial Privacy Act, 12 U.S.C. § 3417; Electronic Communications Privacy Act, 18 U.S.C. § 2707.