

FoxNewsArticleSB335.pdf

Uploaded by: Brian Feldman

Position: FAV

Black teen kicked out of skating rink after facial recognition camera misidentified her

By Randy Wimbley and David Komer online producer | Published July 14, 2021 | Updated July 16, 2021 | Crime and Public Safety | FOX 2 Detroit

FOX 2 - A local roller skating rink is coming under fire for its use of facial recognition software after a teenager was banned for allegedly getting into a brawl there.

"To me, it's basically racial profiling," said the girl's mother Juliea Robinson. "You're just saying every young Black, brown girl with glasses fits the profile and that's not right."

Family says daughter was kicked out of skating rink after facial recognition camera misidentified her

A local roller skating rink is coming under fire for its use of facial recognition software, after a teenager was banned for allegedly getting into a brawl there.

Juliea and her husband Derrick are considering legal action against a Livonia skating rink after their daughter Lamya was misidentified by the business's facial recognition technology.

"I was like, that is not me. who is that?" said Lamya Robinson.

Lamya's mom dropped her off at Riverside Arena skating rink last Saturday to hang out with friends, but staffers barred her entry saying she was banned after her face was scanned - saying Lamya was involved in a brawl at the skating rink back in March.

But there was one problem.

"I was so confused because I've never been there," said Lamya.

The Robinsons' beef with Riverside comes as facial recognition technology undergoes more scrutiny. Robert Williams, one of the first in the country to be misidentified and wrongfully arrested over the technology, testified on Capitol Hill Tuesday.

"I just don't think it's right, that my picture was used in some type of lineup, and I never been in trouble," Williams said.

Tawana Petty heads up Data 4 Black Lives, one of 35 organizations signing onto a campaign calling for retailers to not use facial recognition on customers or workers in their stores.

According to campaign organizers, Lowes and Macy's are among those using the technology.

Walmart, Kroger, Home Depot, and Target are among those that are not.

"Facial recognition does not accurately recognize darker skin tones," Petty said. "So, I don't want to go to Walmart and be tackled by an officer or security guard, because they misidentified me for something I didn't do."

The Robinsons say they are thankful the situation did not lead to an unnecessary interaction with police.

Riverside made Lamya leave the building after misidentifying her, putting her safety, the Robinsons say, at risk.

"You all put my daughter out of the establishment by herself, not knowing what could have happened," said Derrick Robinson. "It just happened to be a blessing that she was calling in frustration to talk to her cousin, but at the

same time he pretty much said I'm not that far, let me go see what's wrong with her."

We have a statement from the skating rink which reads in part:

"One of our managers asked Ms. Robinson (Lamya's mother) to call back sometime during the week. He explained to her, this our usual process, as sometimes the line is quite long and it's a hard look into things when the system is running.

"The software had her daughter at a 97 percent match. This is what we looked at, not the thumbnail photos Ms. Robinson took a picture of, if there was a mistake, we apologize for that."

While Lowe's has been sued for its alleged use of facial recognition technology, a spokeswoman says, "Lowe's does not collect biometric or facial recognition data in our stores."

For more information about stores using facial recognition, go to [**www.banfacialrecognition.com/stores/**](http://www.banfacialrecognition.com/stores/)

PostArticleSB335.pdf

Uploaded by: Brian Feldman

Position: FAV

The Washington Post

Contract lawyers face a growing invasion of surveillance programs that monitor their work

The attorneys worry that if law firms, traditionally the defenders of workers' rights, are turning to the programs, why wouldn't every other business?

(Sébastien Thibault for The Washington Post)

By Drew Harwell

November 11, 2021 at 8:00 a.m. EST

Camille Anidi, an attorney on Long Island, quickly understood the flaws of the facial recognition software her employers demanded she use when working from home. The system often failed to recognize her face or mistook the Bantu knots in her hair as unauthorized recording devices, forcing her to log back in sometimes more than 25 times a day.

When she complained, she said, her bosses brushed it off as a minor technical issue, though some of her lighter-skinned colleagues told her they didn't have the same problem — a common failing for some facial recognition systems, which have been shown to perform worse for people of color.

So after each logout, Anidi gritted her teeth and did what she had to do: Re-scan her face from three angles so she could get back to a job where she was often expected to review 70 documents an hour.

"I want to be able to do the work and would love the money, but it's just that strain: I can't look left for too long, I can't look down, my dog can't walk by, or I get logged out," she said. "Then the company is looking at me like I'm the one delaying!"

Facial recognition systems have become an increasingly common element of the rapid rise in work-from-home surveillance during the coronavirus pandemic. Employers argue that they offer a simple and secure way to monitor a scattered workforce.

But for Anidi and other lawyers, they serve as a dehumanizing reminder that every second of their workday is rigorously probed and analyzed: After verifying their identity, the software judges their level of attention or distraction and kicks them out of their work networks if the system thinks they're not focused enough.

Contract attorneys such as Anidi have become some of America's first test subjects for this enhanced monitoring, and many are reporting frustrating results, saying the glitchy systems make them feel like a disposable cog with little workday privacy.

But the software has also become a flash point for broader questions about how companies treat their remote workforces, especially those, like contract attorneys, whose short-term gigs limit their ability to push for change. The attorneys also worry that it could become the new norm as more jobs are automated and analyzed: If the same kinds of law firms that have litigated worker protections and labor standards are doing it, why wouldn't everyone else?

"There's always going to be a desire to control more of the workplace, just because you can ... and because the cost of all the heavy-handedness comes down on the employee," said Amy Aykut, a contract attorney in the D.C. area.

The monitoring is a symptom of "these pervasive employer attitudes that take advantage of these technologies to continue these really vicious cycles ... that treat employees as commodities," she said. "The irony in this situation is that it's attorneys, who traditionally advocate for employee rights or justice when they're made aware of intrusions like these."

Keystroke tracking, screenshots, and facial recognition: The boss may be watching long after the pandemic ends

Contract attorneys sift through thousands of documents entered as potential evidence during a lawsuit, redacting sensitive information and highlighting relevant details lawyers may need while arguing a case, and they have become a backbone of the legal economy: Law firms hire them on an as-needed basis — such as when a complicated lawsuit involves lots of internal records or emails — and ditch them when they are no longer necessary.

Legal recruiters say the job's flexible schedules and outsourced contracts have opened more opportunities for work in the saturated legal profession. But contract attorneys say their short-term contracts ensure they work without benefits, at reduced hourly rates, and with no expectations of job security after the work is complete. Many said they pursued the job only because firms weren't hiring for the kinds of full-time work they'd need to pay off law school debt.

"An underclass had been created to perform the mundane tasks without the incentive of being mentored and trained for more sophisticated legal work," one contract attorney in Texas said. "And the members of this class could be discarded as soon as a litigation was over — sometimes literally on a moment's notice."

The Washington Post spoke with 27 contract attorneys across the United States who had been asked to use facial recognition software while working remotely. The pandemic pushed many of them out of secure document-review offices and into remote work, and

many expected some additional security, since they look at sensitive files for legal cases with strict confidentiality rules.

But most of them hadn't expected anything like the facial recognition monitoring they've been asked to consent to. The software uses a worker's webcam to record their facial movements and surroundings and will send an alert if the attorney takes photos of confidential documents, stops paying attention to the screen or allows unauthorized people into the room. The attorneys are expected to scan their face every morning so their identity can be reverified minute by minute to reduce potential fraud.

Here are all the ways your boss can legally monitor you

Some attorneys welcomed the monitoring, arguing that they liked trying out cutting-edge software, that the bugs weren't all that bad, or that the hassle was worth it if they could keep working from home. But many others said the systems were finicky, error-prone and imprecise thanks to general weaknesses in facial recognition systems, which can show wild swings in accuracy based on factors such as a room's lighting, a person's skin color or the quality of their webcam.

Lawyers said they had been booted out of their work if they shifted slightly in their chairs, looked away for a moment or adjusted their glasses or hair. The systems, they said, also chastised them for harmless behaviors: holding a coffee mug mistaken for an unauthorized camera or listening to a podcast or the TV.

The constant interruptions have become a major annoyance in a job requiring long-term concentration and attention to detail, some lawyers said. But the errors also undercut how much work they could do, leaving some fearful it could affect their pay or their ability to secure work from the same firms later on.

Several contract attorneys said they worried that their performance ratings, and potential future employability, could suffer solely based on the color of their skin. Loetitia McMillion, a contract attorney in Brooklyn who is Black, said she'd started wearing her hair down or pushing her face closer to the screen in hopes the system would stop forcing her offline.

"It crashes all the time and says it doesn't recognize me," she said, "and I want to just tell it: Actually, no, it's the same Black face I've had for a few decades now."

Some contract attorneys said they felt the burden weighed especially heavily on people of color, who fill an outsize portion of the short-term legal roles. People of color make up about 15 percent of all lawyers in the United States but about 25 percent of the "non-traditional track/staff attorney" jobs, which include contract attorneys, according to recent statistics from the American Bar Association and the National Association for Law Placement.

Cheating-detection companies made millions during the pandemic. Now students are fighting back.

Attorneys of color also worried that the facial recognition systems' varying performance on different skin tones left them disadvantaged from the start. One attorney said he filed a complaint with New York City's Human Rights Commission last year, arguing that he was being denied the right to work by refusing to consent to being monitored. He worries that the facial recognition scans could threaten his legal license or livelihood if it falsely led to accusations that he had compromised client data.

"As a black male in America I am constantly under surveillance the moment I step outside," he wrote in July to one of the agencies in an email he shared with The Post. "I will not subject myself to this indignity and the invasion of my privacy in my own home."

Contract attorneys are far from the only American occupation to undergo enhanced monitoring. Delivery workers, call-center representatives and Uber drivers are increasingly assessed by face- or voice-analyzing software, which their employers say can help the companies verify worker identity, performance or productivity.

Those fields have faced their own frustrations: A former Uber driver has filed a legal claim in the United Kingdom alleging that the company's facial recognition software was racially discriminatory against him and other Black drivers because it worked less effectively on darker skin.

Privacy Reset: A guide to the important settings you should change now

Verificent Technologies, one of the companies selling such work-monitoring software, also offers a similar "online proctoring" service that colleges are increasingly using to monitor students during exams. The systems have led some test-takers to urinate in their seats for fear of being punished or flagged as cheaters if they stepped away and have sparked a backlash on campuses nationwide.

The company's "on-demand monitoring" software, RemoteDesk, can track workers' "idle" and "active" time; record their screens and web-browser history; patrol their background noise for unauthorized music or phone calls; and use the webcam to scan a worker's face or room for company rule-breaking activity, such as eating and drinking or "suspicious expressions, gestures, or behavior."

Nada Awad, the company's chief sales officer, said suspicious behaviors include working for too long without a break or looking away from the monitor for extended periods of time. In an online guide on "the ethical complexity of remote workforce monitoring," the company wrote that its software identifies "various levels of deceit and misconduct based on the guidelines defined by the corporation."

An example screenshot of the RemoteDesk interface for employers, which the company shared with The Post, logged every online activity a worker had done during the workday, with each classified as "productive" and "unproductive," as well as an overall "productivity score." It also showed data on total hours worked and a "webcam feed"

that included snapshots of violations, such as when a worker opened a social media website, used their phone or blocked the camera's view.

Rahul Siddharth, Verificient's co-founder and operations chief, said the company has seen rapid growth during the pandemic from companies worried about "being hosed" by deceptive or unproductive employees who might be working half-mindedly, slacking off or working two jobs at once.

"Abuse happens, and that's a fact of nature — not for everyone, but a significant enough amount that companies and employers want to manage it as best they can," Siddharth said. "It's not for Big Brother to watch them. It's to say you cannot be compensated for a two-hour break."

Workers are putting on pants to return to the office only to be on Zoom all day

Attorneys' document-review work had almost always been an in-person job, and the offices they worked in had strict rules around security. But Cathy Fetgatter, the senior vice president of analytics and managed review services for Innovative Discovery, a legal recruiting agency based in Arlington, Va., said the pandemic changed everything: Every office closed in March 2020, shifting all of the agency's document-review jobs to remote work.

Their law firm clients were given the option to remotely monitor and verify the identities of those attorneys with facial recognition software, Fetgatter said, and about 5 percent of the agency's clients have chosen to do so in the past year.

That number is growing. Other firms have opted for even more "robust monitoring," in which the webcam software looks for other rule-breaking behavior, such as whether anyone else can be heard or seen near the computer screen.

The agency, Fetgatter said, has a database of 10,000 contract attorneys who are assessed based on "performance indicators" that track their demeanor and productivity. She declined to say which facial recognition software attorneys working with Innovative Discovery were expected to use.

The technology isn't perfect, Fetgatter said: One law firm client recently complained that the number of false positives made it "honestly more of a nuisance than it was worth." But much of the attorney feedback about the system so far, she said, has "been positive because of how much attention we put on keeping the team engaged." Attorneys who are uncomfortable with that level of monitoring, she added, can decline the job.

Some attorneys, however, feel like it's not a real choice. While jobs with the facial recognition requirement are still the exception, many attorneys said they expect that more law firms will grow interested as the technology becomes cheaper and easier to deploy, forcing workers to tolerate the monitoring or lose out on jobs.

Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home

Hope Weiner, a contract attorney in New York, said she has embraced the technology, technical quirks and all. Because the software requires the worker to keep their head within a limited space in view of their webcam, she said, “you do find yourself swishing your face around like a tetherball so that the computer does not shut down on you.” But other lawyers said they felt infantilized or distrusted by monitoring software that gave no weight to their experience or careers. One attorney said the software treated “people who have taken oaths as if they are common criminals.” Said another: “Didn’t my work record speak for itself that I had integrity?”

One 10-year contract attorney in Arlington, whose contract required that he use the security software SessionGuardian, said the minute-to-minute need to be constantly looking at his computer made him feel “treated like a robot.” Another said he felt exhausted after 10 hours of sitting like a “gargoyle,” knowing any shift in position might log him out.

Jordan Ellington, SessionGuardian’s founder and chief executive, said that companies can set their own rules — employee facial scans, for instance, can be as frequent as once a second — and that the enhanced at-home security can be worth it for those frustrated by office work.

“That contract attorney would have otherwise spent time commuting to a location that has cameras and people walking around, looking at screens, to maintain their security,” Ellington said. “Wouldn’t you prefer to save on that commute?”

Some attorneys said they worry that this is only the beginning for work-from-home surveillance. Call center workers in Colombia told NBC News in August that they had been asked to consent to in-home camera monitoring. Google and Microsoft already offer tools that employers can use to automatically gauge their workers’ productivity. And some companies, including Amazon, have considered monitoring workers’ mouse movements and keyboard strokes as a way to detect impostors.

But some attorneys said they see a silver lining in this oversight. Anne Ditmore, a freelance document-review attorney in Dallas, said that at first having her face scanned “felt like I was giving away such a unique identifier, and so impersonal. I felt untrusted.” But she now says she feels a “sense of pride” in contributing to the early days of a technology reshaping how people work.

The boom in facial recognition scans and other productivity software “now makes me work harder and longer than when I worked in an office,” she said. “There is no live human interaction, aside from scheduled video meetings, as there once was between co-workers in an office environment. That saved time is spent working.”

PostEditorial.pdf

Uploaded by: Brian Feldman

Position: FAV

Opinion: The IRS should not make you scan your face to see your tax returns

The Internal Revenue Service headquarters in D.C. (Samuel Corum/Bloomberg)

By Editorial Board

February 6, 2022 at 9:00 a.m. EST

The Internal Revenue Service might soon force every American who wants to access their taxes online to record a selfie of themselves and submit to facial recognition to verify their identity. The IRS wants to start this extra verification procedure [this summer](#). That would be a mistake. This cannot be the only way to access an account online, as [90 percent](#) of tax filers currently do.

Requiring facial recognition could prevent a substantial number of people from accessing their accounts. Low-income Americans often lack the necessary technology, and research shows people of color are [more likely to be misidentified](#). There are equally serious concerns about privacy and what will happen to the potentially more than 100 million selfies the IRS will collect.

Cutting down on fraud is a worthy goal, but facial recognition should not be introduced so swiftly without clear guardrails around the data. The IRS hired a private company, ID.me, to handle the facial verification system, and it is currently required to store data [for at least seven years](#) due to IRS auditing requirements. While the company promises not to do anything with the data beyond share taxpayers' selfies with authorities if a fraud issue comes up, there is no federal law regulating how this sensitive information can be used. And let's not forget that [hackers exposed](#) the personal information of more than 140 million Americans when they broke into Equifax — itself once an [IRS verification company](#). If hackers were able to obtain the ID.me selfie records, it could be especially damaging, with potential uses ranging from committing fraud and identity theft to blackmailing people — or the company.

Some try to compare what the IRS wants to do to people using Face ID to unlock their cellphone. But there's a big difference between the two. First, it is not a requirement to use facial recognition to unlock an Apple iPhone. People get to opt in, and there are clear and easy alternatives, such as using a passcode. Second, Apple is very clear that your facial image "[doesn't leave your device](#)." Apple is not storing it anywhere, nor is Apple checking it against a bigger database of images in the way ID.me [describes](#) (a process known as "[one to many](#)" matching).

It's true that someone could still file a paper return or mail in a letter about their tax account. But the reality is more than 152 million tax returns were [filed online](#) last year. The IRS has been urging people not only to file online but also to use the IRS website to check the status of their return, their refund, their child tax credit and more due to a

massive backlog in processing paper returns. IRS call centers have been equally useless, answering only [1 in 10 calls](#) last tax season.

There have been encouraging reports that the IRS is [reconsidering](#) its sole reliance on ID.me for online verification for website access. At a minimum, the IRS must offer other verification options and clearly articulate guidelines on what happens to all facial data. The government is already warning of “[enormous challenges](#)” this tax filing season. Rushing into facial recognition is likely to make them worse.

The Post’s View | About the Washington Post Editorial Board

SB335_Amendment133820-01

Uploaded by: Brian Feldman

Position: FAV



SB0335/133820/1

AMENDMENTS
PREPARED
BY THE
DEPT. OF LEGISLATIVE
SERVICES

08 FEB 22
12:34:19

BY: Senator Feldman
(To be offered in the Finance Committee)

AMENDMENT TO SENATE BILL 335
(First Reading File Bill)

On page 2, in line 22, strike “OR”; in line 28, after “MAMMOGRAPHY” insert “;
OR

(IX) INFORMATION COLLECTED, USED, OR DISCLOSED IN THE
CONTEXT OF RESEARCH CONDUCTED IN ACCORDANCE WITH:

1. THE FEDERAL POLICY FOR THE PROTECTION OF
HUMAN SUBJECTS UNDER 45 C.F.R. PART 46;

2. THE GOOD CLINICAL PRACTICE GUIDELINES
ISSUED BY THE INTERNATIONAL COUNCIL FOR HARMONISATION; OR

3. THE U.S. FOOD AND DRUG ADMINISTRATION
PROTECTION OF HUMAN SUBJECTS UNDER 21 C.F.R. PARTS 50 AND 56”;

and in line 29, after “(C)” insert ““BIOMETRIC INFORMATION” DOES NOT INCLUDE
ANY INFORMATION DERIVED FROM AN ITEM LISTED IN SUBSECTION (B)(2) OF
THIS SECTION.

(D)”.

On page 3, in lines 9, 18, and 28, strike “(D)”, “(E)”, and “(F)”, respectively, and
substitute “(E)”, “(F)”, and “(G)”, respectively.

(Over)

SB0335/133820/1
Amendments to SB 335
Page 2 of 2

Feldman

On page 4, in line 1, strike “**(G)**” and substitute “**(H)**”.

SB 335_ ACLU + Coalition_fav.pdf

Uploaded by: Daniel Marks

Position: FAV

February 9, 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, the undersigned civil rights, civil liberties, and community-based organizations, write to ask for your favorable support of SB335, *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-cast-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 Facebook¹⁵ 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=AQAAAEBrHbxKPyHPswRRR0DSB6DKI2M9R0EBZOxNcySbBlwamvYP6BIU1BLI3H0pxpUJbN2WxW5dnBHep21MFvJZDMkhBQUJQWydNycnJJXGXR0BB9Nz2TLKGT60aE_knpKS9h81g_wUGH-GZNO7-9IzibAkpYKMcwB3HDqK2nXCbhMh

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 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

The Surveillance Technology Oversight Project (S.T.O.P.)

CPD Written Testimony SB 335.pdf

Uploaded by: Hanna Abrams

Position: FAV

BRIAN E. FROSH
Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General



STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

February 9, 2022

TO: The Honorable Delores Kelley, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 335 – Biometric Identifiers Privacy – SUPPORT

The Office of the Attorney General supports Senate Bill 335 (“SB 335”), sponsored by Senators Feldman, Augustine, Benson, Elfreth, Hayes, Jackson, Kagan, King, Kramer, Klausmeier, Lam, Lee, Patterson, and Watson. SB 335 provides Marylanders with privacy protections for biometric data to ensure that businesses do not keep this sensitive data longer than necessary and do not sell it without consumer consent. SB 335 complements Maryland’s Personal Information Protection Act which ensures that businesses that collect personal information maintain it securely¹ by creating timelines for the destruction of biometric data and restrictions on its transfer.

Biometric technologies measure and analyze people’s unique physical and behavioral characteristics, such as fingerprints, iris scans, voiceprints, and facial recognition. Businesses currently use this information to, among other things, verify identity, customize the consumer experience, and for security purposes. For example, the broad applications of facial recognition systems include supplanting time clocks at job sites,² replacing keys for housing units,³ aiding security at stadiums,⁴ and expediting check-in at hotels.⁵ But it is important to recognize that

¹ The Maryland Personal Information Act covers biometric data, but it simply requires companies that collect or store consumers’ personal information to: (1) reasonably protect it, and (2) notify consumers and the Attorney General’s Office if there is a data breach that exposes that information. Md. Code Ann., Com. Law §§ 14-3503; 14-3504.

² *4 Reasons to Use Time Clocks With Facial Recognition*, Buddy Punch (Jun. 19, 2018), available at <https://buddypunch.com/blog/time-clocks-facial-recognition>.

³ Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times (Mar. 28, 2019), available at <https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html>.

⁴ Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times (Mar. 13, 2018), available at <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>.

⁵ *Facial recognition is coming to hotels to make check-in easier—and much creepier*, Fast Company (April 1, 2019), available at <https://www.fastcompany.com/90327875/facial-recognition-is-coming-to-hotels-to-make-check-in-easier-and-muchcreepier>.

biometric technology is not just used when a consumer knowingly provides the information such as when they use a fingerprint or facial scan to unlock their phones. In many cases, the general public is unknowingly surveilled and has little control over the application of this technology.

SB 335 establishes reasonable limits on the collection, use, and storage of biometric data. It prohibits businesses from collecting biometric data without consumer consent. It also prohibits businesses from selling or sharing consumer biometric data.⁶ In addition, SB 335 requires that biometric information be destroyed when it is no longer in use.⁷ Several other states have already enacted laws to protect consumers' biometric information, including California⁸, Illinois⁹, Texas¹⁰, and Washington.¹¹ These protections are particularly important given the uniqueness of biometric identifiers. Unlike account numbers, once biometric data has been breached, it is compromised forever—you cannot change your fingerprint or iris if it gets stolen.¹² Data thieves have already begun to target biometric data; in 2019, data thieves breached an international database and gained access to more than a million fingerprints and other sensitive data, including photographs of people and facial recognition data.¹³

Like the laws already in effect in Illinois and California, SB 335 provides for a private right of action. Given the high cost when an individual's biometrics are compromised, businesses must be held accountable if they sell or misuse an individual's biometric data. A private right of action supplements the limited resources of the Attorney General's office and is necessary to ensure that accountability.

The Office of the Attorney General urges a favorable report.

Cc: Members, Finance Committee
The Honorable Brian Feldman
The Honorable Malcolm Augustine
The Honorable Joanne Benson
The Honorable Sarah Elfreth
The Honorable Antonio Hayes
The Honorable Michael Jackson
The Honorable Cheryl Kagan
The Honorable Nancy King

⁶ Section 14-4404(a)

⁷ Section 14-4402(a).

⁸ Cal. Civ. Code § 1798.100 *et seq.*

⁹ 740 ILCS 14.

¹⁰ Tex. Bus. & Com. § 503.001.

¹¹ Wash. Rev. Code § 19.35.

¹²Data thieves have already begun to target biometric data; in 2019, data thieves breached an international database and gained access to more than a million fingerprints and other sensitive data, including photographs of people and facial recognition data. Scott Ikeda, *Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data*, CPO Magazine (Aug. 27, 2019), available at <https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/>.

¹³ Scott Ikeda, *Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data*, CPO Magazine (Aug. 27, 2019), available at <https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/>.

The Honorable Delores Kelley

February 9, 2022

Page **3** of **3**

The Honorable Benjamin Kramer

The Honorable Katherine Klausmeier

The Honorable Clarence Lam

The Honorable Susan Lee

The Honorable Obie Patterson

The Honorable Ron Watson

2022-02-07-MDBIPA-EFF.pdf

Uploaded by: Hayley Tsukayama

Position: FAV



February 7, 2022

Re: S.B. 335 - Biometric Identifiers and Biometric Information Privacy

Dear Honorable Members of the Senate Finance Committee,

I write today on behalf of the Electronic Frontier Foundation, a non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 35,000 active donors and members, including many in Maryland. We are writing to ask you to advance S.B. 335, Senator Feldman’s bill regarding Biometric Identifiers and Biometric Information Privacy.

It is critically important that lawmakers stand up to protect their constituents from the abuse of biometric information, through strong laws with strong enforcement. Biometric information is unique in many ways. For one, our biometrics are easy to capture. Once captured, we generally cannot change our biometrics, unlike our credit card numbers, or even our names. Databases of biometric information are [ripe targets for data thieves](#). That’s why EFF has worked to defend and enforce the Illinois Biometric Information Privacy Act (BIPA)—on which S.B. 335 is based—as a necessary means to protect our biometric privacy from intrusion by private entities. It is also why we have encouraged other states and the federal government to follow this model of legislation.

Since it was passed in 2008, Illinois’ BIPA has prevented one of the worst corporate uses of face recognition: dragnet faceprinting of the public at large. Some companies do this to all people entering a store, or all people appearing in photos on social media. This practice violates BIPA because some of these people have not previously consented to faceprinting.

We are encouraged to see Maryland recognize the harms that overbroad collection can inflict on people as they go about their daily lives. And we strongly encourage you not to weaken SB 335 by eliminating perhaps the most important piece of Illinois’ BIPA: the private right of action.

Laws are often only as good as their penalties. This is why it is a top priority for the Electronic Frontier Foundation to include private rights of action in privacy laws, including those that protect biometric privacy. Consumer enforcement is part of EFF’s “bottom-up” approach to public policy. Ordinary technology users should have the power to decide for themselves whether to bring a lawsuit to enforce their statutory privacy rights.

Since Illinois’ BIPA was passed in 2008, those seeking to weaken its protections have repeatedly attacked the private right of action, calling it unnecessary. Including a private right of action, in fact, is how legislators normally approach privacy laws. Many privacy statutes contain a private right of action, including federal laws on [wiretaps](#), [stored electronic communications](#), [video rentals](#), [driver’s licenses](#), [credit reporting](#), and [cable](#)

EFF letter re: S.B. 335
February 7, 2022
Page 2 of 2

[subscriptions](#). So do many other kinds of laws that protect the public, including federal laws on [clean water](#), [employment discrimination](#), and [access to public records](#).

We have already seen how ineffective laws become when they are passed without this important enforcement mechanism. Texas, for example, has a [2009 law very similar to Illinois' BIPA](#) except for the fact that only the state attorney general has the right to sue under the law. As a result, it has never been enforced.

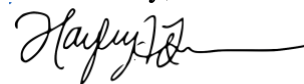
Laws like BIPA that allow private citizens to sue are necessary for several reasons. First, biometric surveillance is a growing menace to our privacy. Our biometric information can be harvested at a distance and without our knowledge, and we often have no ability as individuals to effectively shield ourselves from this grave privacy intrusion. Second, BIPA follows in the footsteps of a host of other privacy laws that prohibit the capture of private information absent informed opt-in consent, and that define data capture without notice and consent as an injury in and of itself. Third, allowing private lawsuits is a necessary means to ensure effective enforcement of privacy laws.

Illinois' BIPA has been on the books for fourteen years and has proven itself one of the most effective laws at holding companies accountable for privacy violations in the country. For example, in 2021, Facebook settled a lawsuit with its Illinois users for [\\$650 million](#) after it collected faceprints from its users without their consent in violation of [BIPA](#).

People should be able to choose which companies they trust with their information, especially information as sensitive and unique as biometrics. Companies, no matter their size, should recognize the responsibilities inherent to the collection of biometric information. They also must be held accountable for actions that break that trust.

We thank you for considering this important issue, and we thank Senator Feldman for his leadership on this issue. If you have any further questions, please reach out to me, legislative activist Hayley Tsukayama, at hayleyt@eff.org. Thank you.

Sincerely,



Hayley Tsukayama
Legislative Activist
Electronic Frontier Foundation
(415) 436-9333 x 161

SB 335_AARPMD_fav.pdf

Uploaded by: Karen Morgan

Position: FAV



One Park Place | Suite 475 | Annapolis, MD 21401-3475
1-866-542-8163 | Fax: 410-837-0269
aarp.org/md | md@aarp.org | twitter: @aarpm
facebook.com/aarpm

SB 335-Commercial Law – Consumer Protection – Biometric Identifiers Privacy
FAVORABLE
Senate Finance Committee
February 9, 2022

As you may know, AARP Maryland is one of the largest membership-based organizations in the Free State, encompassing almost 850,000 members. **AARP MD supports SB 335-Commercial Law-Consumer Protection-Biometric Identifiers Privacy.** We thank Senator Feldman and the other Senate cosponsors for introducing this legislation.

AARP is a nonpartisan, nonprofit, nationwide organization that helps people turn their goals and dreams into real possibilities, strengthens communities, and fights for the issues that matter most to families such as healthcare, employment and income security, retirement planning, affordable utilities, and protection from financial abuse.

AARP MD supports SB 335 because it requires private entities to establish reasonable and necessary standards to protect the use of an individual's biometric data. Biometric data needs to be treated with exceptional care because of its sensitivity, is generally regarded as unchangeable, and its misuse can expose individuals to significant harm from increased risks for fraud, scams, and identity theft.

In the Information Age, data collection has become an extremely useful way to verify who people are and to track their activities. In recent years, the amount of personal information that is collected, used, shared, and sold has skyrocketed. Nearly everyone is affected by this trend, including those in the age 50 and older community that AARP MD represents. Many, if not most, private entities collect some form of personally identifiable information. This trend is expected to continue in the future and will likely accelerate. At AARP MD, we welcome the promise of significant innovation and the more tailored products and services that could benefit individuals and groups, but only with the proper safeguards in place.

SB 335 helps to establish these safeguards. As specified, it requires private entities to develop written policies that set forth clear retention policies and guidelines for the collection, storage, and destruction of biometric data. Including this requirement in a bill that applies statewide means that Maryland citizens have a clearer idea of what to expect when they consent to the use of their biometric data. Biometric data is so sensitive that requiring private entities to adhere to retention and collection standards as a matter of law is long overdue. Because this biometric data is, for all intents and purposes, permanently connected to, and identified with an individual, that individual should be able to control how that data is used, what it is used for, and how long it is subject to use. Individuals should be able to limit or stop its use easily and quickly, using procedures that are transparent. Just because private entities choose to collect biometric data does not mean that they

should have unlimited control of it. Individuals should still be able to find out quickly and easily what has been done with their data, especially if the private entity has been sharing that information with other parties.

Opponents of this common sense legislation will likely complain that adequate regulation already exists and that the high cost of doing business in Maryland will increase. They will also likely complain that the transparency and data security requirements under this bill are unduly burdensome.

To those businesses that oppose SB 335, we say: if you are in the *data collection business*, you are in the *data protection business*. This applies exponentially more to biometric data because of its unique sensitivity and the potential for dire consequences to individuals if the data is mismanaged or exposed in an unauthorized manner. Biometric data is the gold standard when it comes to identity authentication. As a result, this data is deserving of a gold standard when it comes to its management and protection. The costs and requirements that come with data collection and protection are ones that the entities that want to use the data should be willing to undertake. If the costs are too high, then we respectfully suggest that these entities choose a less sensitive, risky, and costly method for identification authentication.

We support the bill's general prohibition on the selling and trading of biometric data, including the prohibitions on providing incentives for the use of this data conditioned on less than rigorous, standardized protections. The use of biometric data should be limited to identification authentication, not used as a profit center.

The private right of action, as set forth in this bill, is a powerful hurdle for those entities that either negligently or willfully fail to comply with the reasonable protections required in the bill. If the prospect of hundreds of civil lawsuits over shoddy collection and management of biometric data is a chilling prospect, then we at AARP MD say that is all to the good. Considering the consequences of violating the sanctity of this data should give everyone pause. The critical need for secure management of this sensitive data cannot be overstated. The stakes are extraordinarily high for individuals who consent to the use of their biometric data. The sanctions for mismanagement of this data should be equally high.

AARP MD supports SB 335 and respectfully requests that the Senate Finance Committee issue a favorable report. For questions, please contact Tammy Bresnahan, Director of Advocacy for AARP Maryland at tbresnahan@aarp.org or by calling 410-302-8451.

SB0335_CMKrisBurnett.pdf

Uploaded by: Kristerfer Burnett

Position: FAV



COUNCILMEMBER KRISTERFER BURNETT
Baltimore City, District 8

Maryland Senate- The Finance Committee
SB0335: Commercial Law – Consumer Protection – Biometric Identifiers Privacy
-Favorable Report-

My name is Kristerfer Burnett and I am a member of the Baltimore City Council representing the 8th City Council District. **I urge a favorable report for Senate Bill 335, Commercial Law – Consumer Protection – Biometric Identifiers Privacy** which will regulate the use of biometric identifiers by private entities, including by requiring certain private entities in possession of biometric identifiers to develop a policy, made available to the public, establishing a retention schedule and destruction guidelines for biometric identifiers; and authorizing an individual alleging a violation of the Act to bring a civil action against the offending private entity.

In 2021, I served as the primary sponsor of Council Bill 21-0001 “Surveillance Technology in Baltimore”, which with the support of my colleagues, placed a moratorium on the sale and heavily restricted the use of facial technology in Baltimore City. We took this critical step after important questions were raised about the technology deployed by both the public & private sectors. We did this to ensure we had adequate time to establish oversight to its uses, promote transparency on how it is deployed, and protect the rights and civil liberties of the citizens of Baltimore.

Our office conducted extensive analysis of the latest research on the development and deployment of facial recognition, related biometric technology, and its use in the community. What we learned is that many of these tools have technical limitations that can and have amplified the harm of Black people and nearly all people of color, indigenous people, the elderly, gender non-conforming people, people living with disabilities, and our youth. Research conducted by the Massachusetts Institute of Technology (MIT) found deeply embedded racial and gender bias encoded in the algorithms used by leading technology companies – including Amazon, Microsoft, and IBM. The algorithms were found to have an inability to identify people of color – particularly in identifying Black and Brown women with the least accuracy.

Subsequent studies, including by the National Institute of Standards and Technology, confirmed these findings. Members of Congress experienced this disproportionate error

rate firsthand when an ACLU of Northern California test of FRT falsely matched 28 members with a mug-shot database. The implicit bias, found throughout this technology, is why I am asking this body to join jurisdictions, across the country, in regulating the use of biometric technology to protect communities of color from unjust actions from law enforcement and private companies.

Lastly, I wanted to lift up concerns that have been raised by subject matter experts and privacy advocates about the capturing, storage, and the potential sale and distribution of biometric data collected by businesses in the private sector and governmental agencies. I was deeply disturbed to learn from industry representatives in the private sector that personal biometric data collected by companies was being shared with law enforcement agencies, and in several industries, being sold. This collected data was being sold, for a profit, to national and transnational marketing companies to build customer profiles – and potentially undisclosed uses without the knowledge of the people the data was collected from. Thus – the passage of the “Biometric Identifiers Privacy” bill is critically important to close these loopholes and better protect the privacy and security of the citizens we represent.

I'll close with a quote from the CEO of IBM in 2020, "IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values..." This was stated in a letter sent to Congress, alongside public statements from Amazon, Microsoft, and several other large technology companies announcing they were ceasing the sale of facial recognition technology to law enforcement agencies across the United States due to racial bias in the algorithms used in the technology.

For the reasons stated above, I urge a favorable report for Senate Bill 335, Commercial Law – Consumer Protection – Biometric Identifiers Privacy.

Sincerely,



Councilmember Krister Burnett
Baltimore City- District 8
kristerfer.burnett@baltimorecity.gov
(410) 396-4818

From the Office of Councilmember Kristerfer Burnett
Baltimore City Council- 8th District
100 N. Holliday Street, Baltimore, MD 21202 - Room 552

SB 335_ACLU & ACLU of MD_fav.pdf

Uploaded by: Nathan Wessler

Position: FAV



**Testimony for the Senate Finance Committee
February 9, 2022**

SB 335 – Commercial Law – Consumer Protection – Biometric Identifiers Privacy

SUPPORT

The ACLU and ACLU of Maryland support SB 335, 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.

SB 335 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 SB 335, 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 SB 335 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 SB 335 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

SB 335'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 SB 335 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 SB 335’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 SB 335 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.

SB 335_Grant_FAV.pdf

Uploaded by: Rachel Weintraub

Position: FAV



Consumer Federation of America

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

February 7, 2022

The Honorable Chair Delores G. Kelley
Senate Finance Committee
Maryland General Assembly
Miller Senate Office Building,
11 Bladen St., Annapolis, Maryland 21401

RE: Support Biometric Identifiers Privacy Act, SB 335

Dear Chair Kelley 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 SB 335, 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 SB 335 with a favorable report. Thank you for considering our views on this important issue.

Sincerely,

A handwritten signature in black ink that reads "Susan Grant". The signature is written in a cursive, flowing style.

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/>.

SB 335 _Access Now_ FAV.docx.pdf

Uploaded by: Willmary Escoto

Position: FAV



Testimony of Willmary Escoto, U.S. Policy Analyst at Access Now to the Maryland Senate Finance Committee In Support of SB335 (Biometric Identifiers Privacy Act) February 7, 2022

Dear Chair Kelley, and Members of the Committee:

Thank you for holding this week's hearing on bills related to consumer protection. I am writing on behalf of Access Now in support of SB 335, An Act establishing the Biometric Identifiers Privacy Act Information Privacy Act, which provides critical protections.

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission, we operate a global helpline for at-risk populations to mitigate online threats. Additionally, we work directly with lawmakers at local, national, and international levels to ensure policy decisions are focused on the rights of people, particularly underrepresented populations. As an organization, we have focused extensively on data protection and connectivity issues.¹

Access Now Supports SB 335

SB 335 provides strong privacy protections and this committee should move it forward. States should be enacting privacy protections given the failure of Congress to pass a federal comprehensive privacy law. Below, I argue that privacy is a fundamental human right and of critical importance in today's society. Then, I describe specific aspects of SB 335 that empower online autonomy and choice, and increase overall privacy protection.

Privacy Is a Fundamental Right and Is Important to People in Maryland

Privacy is a fundamental human right, but most people do not understand how their data is mined and used by companies all over the world, and similarly have minimal control over those practices.² Companies discreetly collect, process, store, and disclose unprecedented quantities of private, personal information about every one of us. Such extensive and granular data collection reveals a lot about a person, and this is especially dangerous for historically marginalized individuals and communities. While data minimization (the concept that a

¹ See <https://www.accessnow.org/issue/privacy> and <https://www.accessnow.org/issue/net-discrimination>.

² Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

company shall collect only as much data as is necessary to provide its service) has been a core privacy principle for decades, very few companies take it seriously.³

The public dislikes these data practices and wants the government to do something about it, and rightfully so.⁴ “Nearly three-quarters of Americans want the federal government to establish national privacy standards.”⁵ According to a poll released last year, nearly 60 percent of people believe their social media activity and location information is not safe.⁶

Private information is susceptible to breaches and leaks, more than ever before, and can cause irreparable harm to people, especially communities of color. For example, one study revealed that women, black people, indigenous people, and people of color are more likely to be victims of cybercrimes, particularly identity theft.⁷ A few years prior, the Federal Trade Commission found similarly that “African American and Latino consumers were more likely to be fraud victims than non-Hispanic whites.”⁸

Over twenty states have already introduced their own privacy bills while Congress has not found common ground to pass a national privacy framework.⁹ A survey of Republicans and Democrats showed people of both parties want state legislatures and Congress to prioritize privacy legislation, with 75% of respondents placing responsibility on state legislatures to act, and 72% saying Congress should act.¹⁰

Major hacks of social media platforms are becoming more and more common and affecting millions of people, necessitating stronger privacy protections to help avoid such exposure. In

³ See generally Eric Null, Isedua Oribhabor, and Willmary Escoto, *Data Minimization: Key to Protecting Privacy and Reducing Harm*, Access Now (May 2021),

<https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf>.

⁴ Emily A. Vogels, *56% of Americans support more regulation of major technology companies*, Pew Research Center (July 20, 2021),

<https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/>;

⁵ Chris Mills Rodrigo, *Majority of Americans support national data privacy standards: poll*, The Hill (Sept. 16, 2021),

<https://thehill.com/policy/technology/572607-majority-of-americans-support-national-data-privacy-standards-poll>. According to the Pew Research Center, 56% of Americans think major technology companies should be regulated more than they are now, which is a 9-point increase year over year, and 68% believe these firms have too much power and influence in the economy. Vogels, *supra*.

⁶ Rodrigo, *supra*.

⁷ Tonya Riley, *Cybercrime is hitting communities of color at higher rates, study finds*, Cyberscoop (Sept. 27, 2021),

<https://www.cyberscoop.com/cybercrime-demographics-bipoc-malwarebytes/>.

⁸ *Combating Fraud In African American & Latino Communities: The FTC's Comprehensive Strategic Plan: A Federal Trade Commission Report To Congress*, FTC (June 15, 2016),

<https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftc-s-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf> at i.

⁹ Sam Sabin, *States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data*, Morning Consult (Apr. 27, 2021),

<https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/>.

¹⁰ *Id.*

January 2021, a Chinese social media management company called Socialarks exposed information gathered from 214 million Facebook, Instagram, and LinkedIn profiles—information like full names, subscriber data, country of residence, phone numbers, and other contact information.¹¹ In April 2021, the credit reporting agency Experian got hacked, compromising the private credit reports of millions of people.¹² In August 2021, T-Mobile learned that a bad actor illegally accessed and acquired personal data and compromised over 50 million customers, former customers, and prospective customers, including SSN, name, address, date of birth, and driver’s license.¹³

Maryland residents cannot control their own digital identity without a modern data protection law. SB 335 can help lead the way and set an example for other states to follow.

SB 335 Includes Several Provisions that Empower Choice and Protect Privacy

Maryland should enact strong data protection legislation for its people to remedy the shortcomings in U.S. law. SB 335 provides a comprehensive privacy framework that would significantly change the privacy landscape in the state, particularly on protections for biometric data, consumer rights, and civil remedies. Below, I focus on three important provisions in SB 335 that should be retained.

SB 335 gives users more power over their data. SB 335 gives people the right to know, access and delete their personal information. Currently, people who use online services generally must fully agree with the company’s data practices, or they cannot use the service. There is no in-between. SB 335 would at least give people more control over the data companies collect about them, allowing them to better control their online identities. Specifically, SB 335 would allow people to access the biometric data a company has collected about them, and if that person wants that data deleted, they are entitled to take those actions. SB 335 requires businesses to delete Marylanders’ biometric identifiers after a fixed length of time and specifies how consumers’ data will be collected, stored, and used. These provisions offer important rights that are often missing, or difficult to take advantage of, online.

¹¹ Chinese start-up leaked 400GB of scraped data exposing 200+ million Facebook, Instagram and LinkedIn users, Safety Detectives (Jan. 11, 2021), <https://www.safetydetectives.com/blog/socialarks-leak-report/>.

¹² Becky Bracken, *Experian API Leaks Most Americans’ Credit Scores*, Threatpost (Apr. 29, 2021), <https://threatpost.com/experian-api-leaks-american-credit-scores/165731/>; see also Scott Kieda, *Another Data Leak for Experian; Credit Scores of Americans Were Available to Anyone Due to API Security Issue*, CPO Magazine (May 3, 2021), <https://www.cpomagazine.com/cyber-security/another-data-leak-for-experian-credit-scores-of-americans-were-available-to-anyone-due-to-api-security-issue/>.

¹³ Mike Sievert, *The Cyberattack Against T-Mobile and Our Customers: What Happened, and What We Are Doing About It*, T-Mobile (Aug. 27, 2021), <https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers>.

SB 335 heightens protections for biometric data. SB 335 would require covered entities to inform in writing and obtain handwritten consent by individuals when collecting and processing biometric data.

Covered entities would also be required to establish a retention schedule and guidelines for permanently destroying biometric data, and the bill places limits on the data's monetization. Covered entities would be banned from collecting, trading, or selling a person's biometric identifiers without affirmative consent.

The collection and use of biometric data, particularly face data, poses significant risks to individuals.¹⁴ Processing biometric data can lead to error and present extreme risks to privacy and civil rights. Data collection and processing can “reduce opportunities for Black, Hispanic, Indigenous, and other communities of color, or actively target them for discriminatory campaigns and deception.”¹⁵

Companies are working hard to develop biometric and artificial intelligence systems based on biometric data, and they are doing it with essentially no safeguards.¹⁶ Without reasonable limits, biometric technologies threaten to enable companies (and by extension, law enforcement) to pervasively track people's movements and activities in public and private spaces and risk exposing people to forms of identity theft that are particularly hard to remedy. SB 335 places reasonable limits on the processing of biometric information.

SB 335 ensures robust enforcement with a private right of action. SB 335 creates a private right of action that will allow aggrieved people to hold the violator directly accountable in state court. A privacy law is only as effective as its enforcement, and allowing individuals to bring lawsuits will help ensure companies comply with the law.

Other private rights of action have been successful. For example, Illinois's biometric privacy law allows users whose biometric data is illegally collected or handled to sue the companies responsible.¹⁷ The private right has been used to take action against Clearview AI for scraping the facial data of millions of people online.¹⁸ It has also been used to take action against Facebook's practice of tagging people in pictures with facial recognition software without

¹⁴ Access Now and over 175 civil society organizations, activists, and researchers from across the globe are calling for a ban on uses of facial recognition and remote biometric recognition that enable mass and discriminatory targeted surveillance, <https://www.accessnow.org/civil-society-ban-biometric-surveillance/>.

¹⁵ Null et al., *Data Minimization: Key to Protecting Privacy and Reducing Harm*, supra; see also Cameron F. Kerry, *Federal privacy legislation should protect civil rights*, Brookings Institute (July 16, 2020), <https://www.brookings.edu/blog/techtank/2020/07/16/federal-privacy-legislation-should-protect-civil-rights>.

¹⁶ For this and other reasons, the UN human rights chief recently called for a ban and moratorium on certain uses of AI. *Urgent Action Needed over Artificial Intelligence Risks to Human Rights*, United Nations (Sept. 15, 2021), <https://news.un.org/en/story/2021/09/1099972>.

¹⁷ 740 Ill. Comp. Stat. Ann. 14/20, <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004>.

¹⁸ *Illinois Court Rejects Clearview's Attempt to Halt Lawsuit against Privacy-Destroying Surveillance*, ACLU-IL (Aug. 27, 2021), <https://www.aclu-il.org/en/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying>.

consent.¹⁹ Without a private right of action, individuals have to rely on federal or state enforcers, like the FTC, to protect their privacy. However, “[m]arginalized communities historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their own rights.”²⁰ Thus, SB 335 should include a private right of action.

SB 335 is a positive framework for privacy protection and will place the burden of protecting against harmful practices on the companies that collect and use the data rather than the people, and will help users take back control of their personal information. For these reasons and others, Access Now supports SB 335 and hopes the legislature will act on it.

Conclusion

Access Now supports SB 335 and the legislature should move the bill forward. Maryland will protect its residents and be a leader in biometric privacy and racial justice by enacting SB 335. Thank you for your time and attention to these important issues. I look forward to continuing to work with you.

¹⁹ Taylor Hatmaker, *Facebook Will Pay \$650 Million to Settle Class Action Suit Centered on Illinois Privacy Law*, TechCrunch (Mar. 1, 2021), <https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/>.

²⁰ Letter to Roger Wicker *et al.*, from Access Now *et al.*, Apr. 19, 2019, https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf, at 3.

Biometric Identifiers Privacy Act.pdf

Uploaded by: David Edelstein

Position: FWA

**SB 335: Commercial Law – Consumer Protection – Biometric Identifiers Privacy
Position: FAVORABLE WITH AMENDMENTS**

SB 335, the Biometric Identifiers Privacy Act, is a good start for protecting the privacy of Marylanders' biometric data. However, there are some points where it falls short in its privacy protections, and a few places where the burden of compliance may have unintended effects. Therefore, I support it with the changes described below.

SB 335 is clearly modeled after Illinois's similarly-named Biometric Information Privacy Act (BIPA). In the years since BIPA was passed, we've had a chance to see how businesses and courts treat its protections. BIPA provides a private right of action, which deputizes aggrieved citizens to enforce the law, rather than having the state itself do so. Although unusual, it has not interfered with successful pursuit of claims under the act, and indeed courts have ruled that claimants do not need to show an injury to be considered "aggrieved."

However, SB 335 fails to remedy certain flaws with BIPA. BIPA does not establish a statute of limitations for claims, leading to a [muddled decision](#) by the Illinois Appellate Court in *Tims v. Black Horse Carriers, Inc.*, in which they held that different safeguards of the law had different statutes of limitation. **Maryland could explicitly set a statute of limitations for claims under SB 335.** Additionally, both BIPA and SB 335 classify genetic markers not as a "biometric identifier," but as "confidential and sensitive information," which is not afforded any special protections by this law. One's DNA is absolutely a biometric identifier, and **SB 335 should classify it as such.**

SB 335 differs from the Illinois law in several important ways. Some of these aim to confer additional protections to Marylanders. For instance, SB 335 explicitly constrains not just the party that collected biometric information but also any processors they use. Likely inspired by the non-discrimination requirement of the California Consumer Privacy Act (CCPA), SB 335 forbids offering reduced services or higher prices to users who decline to provide biometric identifiers or exercise their rights under SB 335. However, unlike CCPA, SB 335 does not allow businesses to adjust prices or services commensurate to the value provided by biometric identifiers, only to refuse service altogether. **SB 335 should offer a similar middle-ground option to CCPA.**

BIPA sets a time limit for the destruction of biometric identifiers: 3 years after collection or after fulfilling the purpose for which they were collected, whichever comes first. SB 335 shortens the maximum retention time to 1 year, and requires that companies also destroy the data within 1 month of receiving a verified request to do so from the person who provided it. This last addition is commendable, but **shortening the maximum**

holding period to 1 year is a mistake, because any added protection from data minimization isn't worth the cross-jurisdictional inconsistency in data destruction requirements.

Unlike BIPA, SB 335 does not apply to uses of employee biometric data for operational purposes. This is a significant shortcoming, as much of the case for biometric privacy — concerns about intrusiveness and the security of private and unchangeable data — apply equally to employee biometrics as to customer ones. Many of the cases brought under BIPA concern employees seeking to assert their privacy rights against their employers, and SB 335 would not offer Maryland workers similar protections. Moreover, SB 335 does not apply to financial service providers. **SB 335 should not have these expansive carve-outs.**

SB 335 improves on BIPA by allowing persons to request copies of their biometric information from entities holding it, as well as information on the purpose of the biometric information and with whom it might be shared. However, unlike BIPA, it fails to require private entities to share, before the biometric data is first collected, information about the purpose of the collection and the term for which the data may be held. **SB 335 should require proactive disclosure prior to collection** to ensure that consent required by SB 335 is informed.

I support a favorable report on SB 335 if the bill is amended as recommended above.

— David W. Edelstein, IAPP Certified Information Privacy Technologist

NetChoice Opposition to MD SB 335.pdf

Uploaded by: Carl Szabo

Position: UNF

Maryland SB 335

Opposition to SB 335 and the overregulation of biometric technology

February 9, 2022

Chair Kelley, Vice Chair Feldman, and members of the Finance Committee:

We ask you **to not advance SB 335** because it will deny Marylanders the benefits of many emerging services. While privacy is a concern for many Marylanders, the unintended consequences of this legislation could put Maryland and Marylanders at a real disadvantage.

While biometrics may seem like an exotic or scary term, many of us are using biometric technologies every day in ways that make our lives easier and more secure. This includes using facial recognition technology to identify friends and family in Shutterfly albums, and Nest doorbells that can provide a sense of security in seeing what is happening outside our homes. In addition, voice authentication offered by anti-fraud companies like Pindrop is used routinely in call centers to help keep fraudsters and scammers from stealing Marylanders' personal information.

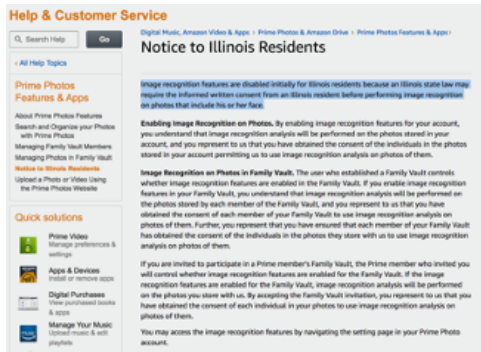
More evolving technologies that make our lives easier and safer using biometrics are increasingly available. Pindrop is developing voice authentication solutions that will enable Marylanders to securely access their accounts with just their own voice, avoiding the need to remember long passwords or master use of a password manager.

But SB 335 would make these uses of biometric technology that clearly benefit consumers much more difficult for Marylanders to access *when Marylanders freely choose to use them*.

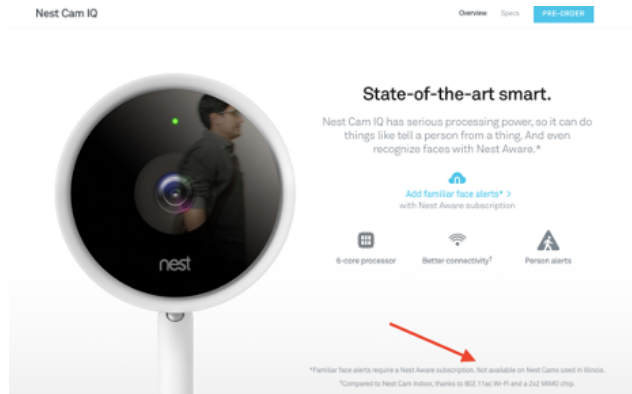
But SB 335 could curtail these beneficial uses of biometric technology.

The real consequences of overregulation of biometric technology can be readily seen in Illinois today. The Illinois's Biometric Information Privacy Act (BIPA) has enabled astounding lawsuits against Shutterfly, Amazon, Google, Apple, Six Flags, and nursing homes. Illinois voters have lost out on the ability to use tech innovations such as Google Art Selfie Match that allowed residents to find their fine art lookalike.

As the images below show BIPA's restrictions and the risks of litigation have resulted in Amazon Photos disabling facial recognition to sort photos a user has uploaded, prevented Nest from offering security matching for friends and family, and stopped an innovative ordering solution at local restaurants that would have allowed customer to place their favorite order with just their face.



Because of BIPA, Amazon Photos does not allow searching photos by face for Illinois residents



Because of BIPA, Nest does not allow Illinois residents the ability to identify friends and family members



Because of BIPA, restaurant kiosks allowing quick reorder of meals at Wao Bao via customer recognition are no longer available in Illinois

In many of these cases, there was not a definable harm that occurred, but the mere existence of a violation was sufficient for class-action litigation. As a result, such bills are not “pro-consumer” or even “pro-privacy,” but better understood as “pro-lawsuit”.

Longer term, this legislation may prevent new secure biometric benefits from being available to Maryland residents.

When it comes to concerns about privacy, a variety of state and federal laws already address many of the concerns that animate this legislation. These include the Children’s Online Privacy Protection Act (COPPA), the Electronic Communications Privacy Act (ECPA), industry specific regulations in healthcare, banking, and education, and the state’s own data breach law. In the case of concerns such as data breaches of sensitive information, existing laws already empower the Maryland Attorney General to bring cases to protect consumers.

In addition to these specific national laws, the Federal Trade Commission (FTC) actively enforces against privacy and security issues across the country, including those involving biometric information.

Under its Section 5 authority regarding “unfair or deceptive practices, the FTC is using an adjustable enforcement approach that evolves with technology and industry best practices. This framework is the ideal way to address concerns related to technologies with a wide-range of applications like the biometrics and has proven an effective way to ensure companies implement strong data security and privacy protections without stifling innovation.

We appreciate your consideration and ask that you not advance SB 335. We welcome the opportunity to work with this committee more as it considers the ideal approach to privacy for the citizens of Maryland.

Thank you again for the opportunity to testify.

Sincerely,

Carl Szabo
Vice President & General Counsel
NetChoice

NetChoice is a trade association that works to make the internet safe for free enterprise and free expression.

MD_TechNet_SB355 Biometrics_2.8.22.pdf

Uploaded by: Christopher Gilrein

Position: UNF



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Northeast | Telephone 774.233.1111
One Beacon Street, Suite 16300, Boston, MA 02116
www.technet.org | @TechNetNortheast

February 7, 2022

The Honorable Senator Delores Kelley, Chair
Senate Standing Finance Committee
Senate Office Building
Annapolis, MD 21401

Re: TechNet Opposition to SB 335 – Biometric Identifiers

Dear Chair Kelley and members of the Committee,

On behalf of TechNet's member companies, I respectfully submit this letter of opposition to SB 335. TechNet's members place a high priority on consumer privacy, however, as drafted, this bill would create significant hardships for Maryland employers and could actually result in stifling important advances in safety and security for consumers.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than three and a half million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet believes that privacy laws should provide strong safeguards for consumers, while allowing the industry to continue to innovate. We understand the Legislature's interest in protecting the data of its constituents, but SB 335 relies on a flawed model. The bill before the Committee today adopts language from the Illinois Biometric Information Privacy Act (BIPA) - a law passed in 2008, which fails to account for over a decade of innovation in technology and business practices. It does not identify and protect against specific privacy harms, instead utilizing a definition of "Biometric identifier" that is overbroad and difficult to implement, which, paired with a private right of action, will open Maryland businesses to costly litigation.

In addition to imposing significant and ongoing compliance costs, this legislation would further burden local businesses with the threat of frivolous class action litigation. In Illinois, BIPA has been used as a cudgel by class-action law firms seeking large payouts from companies leveraging this technology to benefit consumers, or in many cases from providers of support systems that never even interact with consumers. The net effect of BIPA in IL has been to create a cottage industry of class action law firms and to prevent companies and consumers from developing or

accessing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, fraud prevention, and more.

Maryland residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation, security, and job creation. We would welcome the opportunity to work with your office to address issues of privacy protection without unintended consequences. Please consider TechNet's members a resource in this effort.

Thank you for your consideration of this testimony. Please do not hesitate to contact me if I can provide any additional information.

Sincerely,



Christopher Gilrein
Executive Director, Massachusetts and the Northeast
TechNet
cgilrein@technet.org

SIA Letter of Concerns_MD SB 335 BIPA .pdf

Uploaded by: Drake Jamali

Position: UNF



February 9, 2022

Chair, Senator Kelley
Senate Finance Committee on Economic Matters
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chair Kelley and members of the committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with MD SB 335, which establishes requirements & restrictions on private entities use, collection, & maintenance of biometric identifiers & biometric information, while creating a private cause of action for relief on violations of the act.

The Security Industry Association (SIA), which is based in Silver Spring, is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users in the U.S., including businesses headquartered in Maryland and many more with employees and significant business operations in the state. Our members include many of the leading manufacturers of biometric technologies, as well as those who are integrating these technologies into a wide variety of building security and life-safety systems.

At the outset, I want to stress that our members intend their technology products only be used for purposes that are lawful, ethical and non-discriminatory. While we generally support the data policies outlined in H.B. 335 as good practice, careful consideration should be given to whether biometric information should be singled out for regulation separate from other personal data it is often associated with, including biographic information like date of birth, physical characteristics, Social Security number, address, employment, health and education history – the type of information that so far has proven to be more vulnerable to compromise and misuse.

Biometric authentication enhances identity protections while increasing the effectiveness of security systems developed by our industry. Many sectors of the business community stand to benefit from technologically advanced equipment that utilizes biometric identifiers for security purposes, such as authentication, for employee access to buildings or computer networks, and security systems that protect buildings, their occupants and the assets contained therein.

At a minimum, an exemption to a notification and consent requirement for safety and security uses is essential. A good example is the security provision included in Washington State's current biometric data law enacted in 2017. This law generally requires notice and consent of an individual before their biometric information is enrolled in a database for commercial use, but provides an express exception where the collection, capture or enrollment and storage of a biometric identifier is in furtherance of a security purpose (RCW 19.375.020, §7). Such an exemption is necessary, because requiring written

consent would be unworkable for building systems intended for safety or security applications, as an individual with malicious intent would likely not consent to having their information captured.

An increasingly important benefit of biometric data is that it gives employers the ability to alert staff and other building occupants of immediate threats to the safety of a building's occupants, such as where a disgruntled former employee attempts to enter the workplace. Requiring consent or automatic deletion of data after employment would run contrary to ensuring public safety in this case.

Additionally, a consent requirement makes participation optional, thus limiting the ability to effectively deploy safety and security systems that utilize biometric technologies throughout a building, due to the presence of a mixed population of consenting and non-consenting individuals. Without an exception, a consent requirement would essentially preclude using these technologies for the enhancement of access control, intrusion detection, anti-theft, fire alarm, active shooter and other safety and security purposes throughout a building.

The private right of action in the bill should be replaced with enforcement by the attorney general. This mechanism would preserve the protective intent without the potential catastrophic consequences for businesses subjected to unwarranted lawsuits. This is the approach Washington and Texas have taken with their biometrics laws.

In conclusion, due to the wide-ranging negative consequences for Marylanders and Maryland businesses from implementing a Biometric Information Privacy Act (BIPA)-type approach to regulating use of biometric data, we urge the Committee not to advance H.B. 335 in its current form. Instead, we ask that the issue be thoroughly and thoughtfully studied before any legislation or regulations restricting its use are passed.

SIA and our members welcome the opportunity to work with you to identify the best ways to achieve the objective of safeguarding biometric and other personal data, ensuring it is captured, stored and utilized in a responsible manner than benefits Maryland's citizens.

Sincerely,



Don Erickson

Chief Executive Officer

Security Industry Association

Staff contact: Drake Jamali, djamali@securirtyindustry.org

Ext. Comm. - Letter - 2022 - Maryland SB 335 - Bio

Uploaded by: Joshua Fisher

Position: UNF



January 31, 2022

The Honorable Delores Kelley
Chair, Senate Finance Committee
3 East, Miller Senate Office Building
Annapolis, Maryland 21401

RE: SB 335 - Biometric Identifiers Privacy Position: Unfavorable

Chair Kelley:

The Alliance for Automotive Innovation (Auto Innovators) is writing to inform you of **our opposition to SB 335**, which will negatively impact important safety-related vehicle technologies. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents automakers producing nearly 99 percent of cars and light trucks sold in the U.S., major Tier 1 suppliers, as well as other automotive technology companies.

Maintaining Consumer Privacy and Cybersecurity

The protection of consumer personal information is a priority for the automotive industry. Through the development of the “Consumer Privacy Protection Principles for Vehicle Technologies and Services,” Auto Innovators’ members committed to take steps to protect the personal data generated by their vehicles. These Privacy Principles are enforceable by the Federal Trade Commission and provide heightened protection for certain types of sensitive data, including biometric data.¹ Consumer trust is essential to the success of vehicle technologies and services. Auto Innovators and our members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy. Our members are committed to providing all their customers with a high level of protection of their personal data and maintaining their trust.

Practical Concerns

We have concerns about this legislation and recommend an unfavorable report from the committee. Our concerns are outlined below:

First, privacy requirements of this nature require a standardized, nationwide approach so there is not a dizzying array of varied state requirements. Privacy protections regarding biometrics are being enforced by the Federal Trade Commission (FTC). The FTC has been the chief regulator for privacy and data security for decades, and its approach has been to use its authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security

¹ The complete Principles document can be found at www.automotiveprivacy.com

practices. The auto industries "Privacy Principles" are enforceable under Section 5 of the FTC Act.

Second, the current definition of "biometric identifier" is extremely broad and could capture several important safety-related technologies that are not used or intended to be used for the unique personal identification of an individual. For example, external-facing vehicle sensors that are integral to an Advanced Driver Assistance Systems or automated driving systems may be used to recognize that an object in the path of the vehicle is a pedestrian. In addition, internal-facing cameras may be used on some lower-level automated vehicle systems to detect driver misuse or disengagement. While these "images" are not used by an auto company to identify individuals, they are potentially captured by the definition of "biometric identifier."

This issue could be remedied by modifying the definition of "biometric identifier" so that it explicitly excludes images obtained by vehicle safety technologies. It could also be remedied by striking the references to "biometric identifiers" throughout and limiting the applicability of these provisions to "biometric information." Since "biometric information" is defined as information that is used to identify an individual (as opposed to information that can be used to identify an individual), it would presumably exclude the images captured by these vehicle safety technologies.

Third, while the requirement to have a written policy that lays out a retention schedule conforms with the industry's existing Privacy Principles, the requirement to destroy the information no later than one year after the company's last interaction seems somewhat arbitrary. A requirement to provide clear disclosure to consumers about how long such information will be maintained should be sufficient. Moreover, in practice, this requirement may prove challenging because, in the automotive case, manufacturers do not generally have visibility into who is driving or using a particular vehicle at a particular time and using vehicle technologies that may utilize biometric technology. In addition, manufacturers may not always know when a vehicle has been sold to another owner.

Finally, the bill creates a private right of action. Businesses may very well find themselves in a position of facing severe penalties for even very minor and inadvertent infractions and where there are no actual damages.

Thank you for your consideration of the Auto Innovators' position. For more information, please contact our local representative, Bill Kress, at (410) 375-8548.

Sincerely,



Josh Fisher
Director, State Affairs

SB 335_MDCC_Commercial Law–Biometric Identifiers_U

Uploaded by: Maddy Voytek

Position: UNF



LEGISLATIVE POSITION:

Unfavorable

Senate Bill 335

Commercial Law – Consumer Protection – Biometric Identifiers Privacy

Senate Finance Committee

Wednesday, February 9, 2022

Dear Chairwoman Kelley and Members of the Committee:

Founded in 1968, the Maryland Chamber of Commerce is the leading voice for business in Maryland. We are a statewide coalition of more than 5,500 members and federated partners working to develop and promote strong public policy that ensures sustained economic recovery and growth for Maryland businesses, employees, and families.

Maryland Chamber of Commerce members place a high priority on consumer privacy, however, as drafted, SB 335 would create significant hardships for Maryland employers and could result in stifling important advances in safety and security.

Chamber members believe that privacy laws should provide strong safeguards for consumers, while allowing the industry to continue to innovate. However, SB 335 adopts language from an Illinois law passed in 2008 that would further burden local businesses with the threat of frivolous class action litigation. As has been demonstrated in Illinois, the threat of liability will prevent Maryland companies from developing or utilizing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, and fraud prevention.

In addition to the private right of action outlined in SB 335, Chamber members remain concerned about the impacts on the use of biometric technology for security, identification and authentication purposes to help prevent and detect fraud. Concerns include:

- The retention policy outlined in the bill is mandating the destruction of biometrics that are fundamental to businesses preventing fraud and keeping their customers safe. This hampers a businesses ability to identify bad actors potentially increasing the amount of fraudulent activity.
- The language in the bill leaves open the possibility that a private company would be forced to make the mandated written policy public. This would mean making

public the protocols and methods used to combat fraud and ensure security, which is the information of most interest to bad actors.

- The bill sets forth a right to know policy for sensitive information but does not include an ability for the private entity to engage in appropriate and commercially reasonable authentication of the individual making the request (which could result in biometric information being disclosed to bad actors).
- The “do not sell” provision seems to prevent an entity from being able to profit from biometric identifiers beyond a direct sell or trade of the information. The language could be taken to prevent the use of biometric information for security, research and product development. Would the use of biometrics to improve a network security product constitute profiting off the biometrics? Deleting the “or otherwise profit” portion of 14-4404 may take care of this issue.
- The limitation that a private entity cannot condition a service on the collection and use of biometrics unless it is strictly necessary for the service undermines the use of biometrics in fraud prevention and security. Again, this will serve bad actors and could incentivize unlawful behavior.

Maryland residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation and job creation. The Maryland Chamber of Commerce continues to urge the bill sponsors to work alongside industry partners in addressing the issues surrounding the safety and security of personal data.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **unfavorable report** on SB 335.



SB0335_UNF_MTC_Commercial Law - Consumer Protectio

Uploaded by: Pam Kasemeyer

Position: UNF



MARYLAND TECH COUNCIL

TO: The Honorable Delores G. Kelley, Chair
Members, Senate Finance Committee
The Honorable Brian J. Feldman

FROM: Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
Christine K. Krone

DATE: February 9, 2022

RE: **OPPOSE** – Senate Bill 335 – *Commercial Law – Consumer Protection – Biometric Identifiers Privacy*

The Maryland Tech Council (MTC) is a collaborative community, actively engaged in building stronger life science and technology companies by supporting the efforts of our individual members who are saving and improving lives through innovation. We support our member companies who are driving innovation through advocacy, education, workforce development, cost savings programs, and connecting entrepreneurial minds. The valuable resources we provide to our members help them reach their full potential making Maryland a global leader in the life sciences and technology industries. On behalf of MTC, we submit this letter of **opposition** for Senate Bill 335.

MTC members place a high priority on consumer privacy, however, as drafted, the legislation would create significant hardships for Maryland employers and could actually result in stifling important advances in safety and security as well as exposing member businesses and customer data to greater degrees of fraud and cybercrime. For example, Senate Bill 335 has no exception for fraud prevention. Biometric data is used today for security, authentication, and fraud prevention purposes, such as to secure access to highly sensitive buildings, to detect fraudulent callers, and to improve security on financial accounts. Because the bill does not allow for the use of biometric data for fraud prevention, and does not even have a clear security exception, the bill would put Maryland residents at greater risk of fraud and security threats.

In addition, this legislation would leave Maryland businesses vulnerable to class action lawsuits for even minor violations. This is especially true as the bill also does not distinguish between service providers and consumer-facing entities and therefore every business is liable for failing to provide consumers with consent, even when consumers never interact directly with the product. The threat of liability will prevent Maryland companies from developing or utilizing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, and fraud prevention and may dissuade startups and other companies from choosing to do business in the state. Experience with an existing Illinois law upon which these provisions seem to be based bears this out.

MTC recognizes the importance of protecting consumer information, including biometric identifiers and information, and the matters that Senate Bill 335 address should and must be resolved on the federal level. Meaningful consistent compliance by industry would be more reliably satisfied with a uniform nationwide solution. This bill would have the effect of imposing millions of dollars of compliance costs on tech businesses and would harm the State's economy more than it would protect consumer privacy. MTC respectfully requests an unfavorable report.

For more information call:

Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
Christine K. Krone
410-244-7000