Sara N. Love
Legislative District 16
Montgomery County

Environment and Transportation Committee

The Maryland House of Delegates
6 Bladen Street, Room 210
Annapolis, Maryland 21401
410-841-3454 · 301-858-3454
800-492-7122 *Ext.* 3454
Sara.Love@house.state.md.us

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

February 2, 2022

Sponsor Testimony for HB 259 –
Commercial Law – Consumer Protection – Biometric Identifiers and Biometric Information Privacy

HB 259, a bill you have seen before, will put in place guardrails for our biometric identifiers. Biometric identifiers are things like fingerprints, retina or iris scans, or scans of our hand or face geometry. Currently, companies can collect our biometric identifiers without our consent, and there are no rules regarding how long they can keep them or what they can do with them. To be clear, this bill does not ban the use of biometric identifiers. It simply puts in guardrails regarding their collection and use.

In light of complaints made by companies during the 2021 session, we have updated the definition of biometrics and distinguished between front-facing entities and processors.

Collecting biometric identifiers is an area of exploding technological advances and many, many businesses use this technology. Here are a few examples:

- Employers are using facial recognition software to determine whether an employee is working or not.[1]
- Car manufacturers are looking into using facial recognition as a way to determine who is driving a car, or who is walking up to the car to adjust the seat or mirrors;[2]
- Make-up companies are using facial recognition to let consumers try on make-up virtually;[3]
- Macy's uses facial recognition in its stores;[4]
- Apple uses fingerprint scans for unlocking our phones. Their FaceID program allows someone to not only unlock their phone, but also to log into their online banking account.

While there are many beneficial uses for biometric identifiers, there are also myriad concerns with the collection of our biometric identifiers. First, is the privacy concern. These are unique, physical identifiers for individuals. Companies should not be able to collect them without an

[1] https://www.washingtonpost.com/technology/2021/11/11/lawyer-facial-recognition-monitoring/; https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/
[2] https://www.cbinsights.com/research/facial-recognition-technology-us-corporations/
[3] https://www.cbinsights.com/research/facial-recognition-technology-us-corporations/
[4] https://www.axios.com/facial-recognition-retail-surge-c13fff8d-72c6-400f-b680-6ae2679955d4.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

individual's knowledge and consent. Second, is the security concern. Once these identifiers are gone, there is no getting them back. They are not like passwords that can be changed. PayByTouch had 3.7 million fingerprints and when they went bankrupt, those fingerprints – linked to financial accounts – were considered assets that could be sold.[5] In 2015, hackers stole 5.6 million fingerprints from the federal government.[6]

In addition, there is the problem of bias in some of the technology. Facial recognition technology is well-known to be less reliable for persons of color than white people.[7]

- Employees of color whose companies use facial recognition to monitor their activity are kicked out of the system more than their white colleagues.
- A 14-year old was kicked out of a skating rink, even though she had never been there, because the facial recognition system matched her to someone else.[8]
- Apple wrongly accused a black teenager of shoplifting in New York, in part based on facial recognition.[9]
- Rite Aid installed more cameras in areas that were less wealthy and less white.[10]

Finally, I would like to address the opponents' argument that regulating the collection and use of biometric identifiers will make us less safe. This is simply not the case. Take, for example, a company that uses fingerprint technology for access. Employees have given their consent, so their fingerprints are on file. If an unauthorized person tries to access the building, their fingerprint will not be on file, so they will not be able to enter. In addition, the bill does not prohibit companies from using security cameras. They will still be able to use them; they just can't use those cameras to collect face prints.

There are few rules governing the use, retention, and destruction of biometric identifiers despite the explosion of technology gathering them. Illinois, Texas, and Washington have laws like HB 259. I urge you to again pass this bill so Marylanders have some protection with respect to this unique and very personal data.

---

[5] https://trustarc.com/blog/2008/04/02/truste-recommends-destruction-of-more-than-37-million-fingerprint-records/
[6] https://money.cnn.com/2015/09/23/technology/opm-fingerprint-hack/index.html?iid=EL
[7] https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/
[8] https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her
[9] https://www.theregister.com/2021/05/29/apple_sis_lawsuit/
[10] https://www.reuters.com/investigates/special-report/usa-riteaid-software/

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/**

The Washington Post *Democracy Dies in Darkness*

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?

Listen to article 13 min

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

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."

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.

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.

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.

Verificient 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.”

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.

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."

MORE TOP STORIES HAND CURATED

Nearly 50,000 Facebook users may have been targets of private surveillance, company says

News • December 16, 2021

A QAnon con: How the viral Wayfair sex trafficking lie hurt real kids

News • December 16, 2021

Trailblazing Black feminist and social critic bell hooks dies at 69

News • December 15, 2021

View 3 more stories