

**FoxNewsArticleSB169.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/)

**PostArticleSB169.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.”

**PostArticleSB169TSA.pdf**

Uploaded by: Brian Feldman

Position: FAV

Washington Post  
December 2, 2022

YOUR DATA AND PRIVACY

## TSA now wants to scan your face at security. Here are your rights.

16 major domestic airports are testing facial recognition tech to verify IDs — and it could go nationwide in 2023



By Geoffrey A. Fowler  
Share

Next time you're at airport security, get ready to look straight into a camera. The TSA wants to analyze your face.

The Transportation Security Administration has been quietly testing controversial facial recognition technology for passenger screening at 16 major domestic airports — from Washington to Los Angeles — and hopes to expand it across the United States as soon as next year. Kiosks with cameras are doing a job that used to be completed by humans: checking the photos on travelers' IDs to make sure they're not impostors.

The TSA says facial recognition, which has been banned by cities such as San Francisco, helps improve security and possibly also efficiency. But it's also bringing an unproven tech, with civil rights ramifications we still just don't understand, to one of the most stressful parts of travel.

After hearing concerns from Washington Post readers who encountered face scans while traveling, I wanted to know how the TSA is using the tech and what our rights are. Everybody wants better safety, but is this really safer — and what are its real costs? So I quizzed the TSA's Jason Lim, who helps run the program formally known as Credential Authentication Technology with Camera (CAT-2). And I also called Albert Fox Cahn, the founder of the Surveillance Technology Oversight Project, or STOP, and one of the biggest critics of facial recognition.

I learned the TSA has put some important constraints on its use of facial recognition — but its current programs are just the beginning.

No, you don't have to participate in facial recognition at the airport. Whether you'll feel like you have a real choice is a separate question.

### How TSA facial recognition works

American airports have been experimenting with so-called biometric technology for years, following the 9/11 attacks. You might have seen Customs collecting biometric information from passengers entering the United States. In 2019, I tested some of the ways airlines

were using face scans to replace boarding passes for international flights. The TSA's facial recognition pilot began at Ronald Reagan Washington National Airport (DCA) amid concerns about covid transmission through contact in August 2020.

This system is for general passenger security screening. You step up to the travel document checker kiosk and stick your ID into a machine. Then you look into a camera for up to five seconds and the machine compares your live photo to the one it sees on your ID. They call this a "one to one" verification system, comparing one face to one ID. Even though the software is judging if you're an impostor, there's still a human agent there to make the final call (at least for now).

So how accurate is it? The TSA says it's been better at verifying IDs than the manual process. "This technology is definitely a security enhancement," Lim said. "We are so far very satisfied with the performance of the machine's ability to conduct facial recognition accurately."

A TSA security checkpoint at Los Angeles International Airport uses facial recognition technology to verify passenger identities. (Monique Woo/The Washington Post)

What about people who don't exactly look like their driver's license photo? Minor variations in appearance over time — such as changing your hairstyle — have negligible negative impact on identity verification, the TSA says.

But the TSA hasn't actually released hard data about how often its system falsely identifies people, through incorrect positive or negative matches. Some of that might come to light next year when the TSA has to make its case to the Department of Homeland Security to convert airports all over the United States into facial recognition systems.

"I am worried that the TSA will give a green light to technology that is more likely to falsely accuse Black and Brown and nonbinary travelers and other groups that have historically faced more facial recognition errors," said Cahn of STOP.

Research has shown facial recognition algorithms can be less accurate at identifying people of color. [A study published by the federal National Institute of Standards and Technology in 2019](#) found that Asian and African American people were up to 100 times more likely to be misidentified than White men, depending on the particular algorithm and type of search. [Federal study confirms racial bias of many facial recognition systems, casts doubt on their expanding use](#)

Should travelers be concerned? "No one should worry about being misidentified. That is not happening, and we work diligently to ensure the technology is performing according to the highest scientific standards," Lim told me. "Demographic equitability is a serious issue for us, and it represents a significant element in our testing."

That doesn't satisfy critics such as Cahn. "I don't trust the TSA to evaluate the efficacy of its own facial recognition systems," he said.

### **What about your privacy?**

When some people hear about governments using facial recognition, they rightly picture the situation in China, where broad use of the technology makes it extremely difficult for citizens to evade surveillance. Does going through airport security now mean Homeland Security has a face ID that can identify you at a protest?

The TSA says it doesn't use facial recognition for law-enforcement purposes. It also says it minimizes holding on to our face data, so it isn't using the scans to build out a new national database of face IDs.

“The scanning and match is made and immediately overwritten at the Travel Document Checker podium. We keep neither the live photo nor the photo of the ID,” said Lim. But the TSA did acknowledge there are cases in which it holds on to the data for up to 24 months so its science and technology office can evaluate the system’s effectiveness.

*Tiny toiletries forever? The future of TSA, from liquids to shoes.*

What’s more, the TSA already has a plan to expand the scope of how it’s using the tech. It’s running a pilot of a second system at a few airports where you don’t even have to present your physical ID for inspection. Your face *is* your ID.

In tests with Delta, machines compare passengers’ live faces to a database of photos the government already has, typically from passports. For now, this system only works for passengers with PreCheck or Global Entry and passengers also have to request it from Delta. A colleague recently tried it in Atlanta and reported it was like an extra-fast version of PreCheck that probably saved him five minutes on his trip.

Just remember: Any time data gets collected somewhere, it could also be stolen — and you only get one face. The TSA says all its databases are encrypted to reduce hacking risk. But in 2019, the Department of Homeland Security disclosed that photos of travelers were taken in a data breach, accessed through the network of one of its subcontractors.

### **Your rights**

So do you have to participate?

“None of this facial recognition technology is mandated,” said Lim. “Those who do not feel comfortable will still have to present their ID — but they can tell the officer that they do not want their photo taken, and the officer will turn off the live camera.” There are also supposed to be signs around informing you of your rights.

But does it mean you’ll get moved to a slow line, get an extra pat down, or a mark on your record? “You should have no derogatory experience based on you exercising your right,” said Lim. If you suspect that has happened, the TSA says you should ask to speak to a manager.

*How to prevent customs agents from copying your phone’s content*

“What we often see with these biometric programs is they are only optional in the introductory phases — and over time we see them becoming standardized and nationalized and eventually compulsory,” said Cahn. “There is no place more coercive to ask people for their consent than an airport.”

Even people who care a lot about privacy often find their limits when it comes to airline travel. People gravitate to options that help them get through the airport faster — and it’s not hard to imagine ending up with a bifurcated airport experience, said Cahn.

Those who have the privilege of not having to worry their face will be misread can zip right through — whereas people who don’t consent to it pay a tax with their time. At that point, how voluntary is it, really?

# **PostEditorialSB169.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**

**SunOp-Ed\_SB169.pdf**

Uploaded by: Brian Feldman

Position: FAV

# Legislators: Maryland must set limits on biometric identifiers | READER COMMENTARY

The Baltimore Sun  
Feb 10, 2022

We use our faces to open our phones. We pay for things with our fingerprints. Our kids record themselves performing on [TikTok](#). And companies [install](#) facial recognition software on employees' computers to monitor their every move. We are already living in a reality in which facial recognition and other forms of biometric surveillance pervade our daily lives.

But right now, in Maryland, there are essentially no restrictions on the ways corporations can collect, use and even sell our personal, unchangeable biological characteristics like fingerprints and faceprints. That is why we are sponsoring a bill in the Maryland legislature that would protect all Marylanders' right to privacy by establishing guardrails around when and how companies can collect our biometric identifiers.

These technologies can pose a danger to all of our core constitutional rights. They've made it [easier for](#) abusers to stalk their victims, caused [wrongful arrests](#), and led to [arbitrary exclusion from businesses](#) — like the 14-year old Black girl who was denied entry to a roller skating rink because its facial recognition system [misidentified her](#) as someone else who'd gotten into a fight. A [2019 federal study](#) of facial recognition systems found that Asian and Black people were up to 100 times more likely to be misidentified than white men depending on the particular algorithm and type of search. Native Americans had the highest false-positive rate of all ethnicities. Women were also more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups.

The Biometric Identifiers' Privacy Act — or BIPA — is common sense. Think about how terrifying it is when you get a notification alerting you someone stole your password or bank information. With biometric identifiers, the consequences are even more permanent. Unlike a credit card or even a Social Security number, our biometric data can't be revoked or reissued. Once we lose control, as [happened recently](#) when the fingerprints and facial recognition markers of over 1 million people were found accessible on a public database, we are identifiable forever.

While we believe there can be beneficial uses of biometric identifiers, we also believe there should be rules. Our bill would require that companies get consent before taking our biometric identifiers; that they tell consumers what is being taken, stored and for how long; that there are rules on when they delete the identifiers; that they cannot profit off of them; and that there are consequences when they don't follow the law.

It's not enough for us to just pass laws that theoretically protect us from corporations capturing and monetizing our personal information without our knowledge or consent. These laws must make it impossible for companies to ignore these protections. The best way to hold powerful

companies accountable is by empowering ordinary people, like you and me, to bring our own lawsuits against businesses that violate our privacy rights.

Only one other state has a law like this — Illinois. And the difference it's made is clear: A Reuters review of lawsuits filed in Illinois since 2015 found widespread evidence that private companies, like Clearview AI, Facebook and TikTok had secretly collected, tagged and categorized biometric data gleaned from millions of unsuspecting Americans. With BIPA, Illinoisians were able to actually hold these companies accountable. Marylanders deserve the same protection.

*Brian Feldman and Sara Love, Annapolis*

*The writers, both Montgomery County Democrats, are members of the Maryland General Assembly*

# **OAG Written Testimony SB 169.pdf**

Uploaded by: Hanna Abrams

Position: FAV

**ANTHONY G. BROWN**  
*Attorney General*

**CANDACE MCLAREN LANHAM**  
*Chief of Staff*

**CAROLYN QUATTROCKI**  
*Deputy Attorney General*



**WILLIAM D. GRUHN**  
*Chief*  
Consumer Protection Division

**STATE OF MARYLAND**  
**OFFICE OF THE ATTORNEY GENERAL**  
**CONSUMER PROTECTION DIVISION**

February 8, 2023

**TO:** The Honorable Melony Griffith, Chair  
Finance Committee

**FROM:** Hanna Abrams, Assistant Attorney General

**RE:** Senate Bill 169 – Biometric Data Privacy – SUPPORT

The Office of the Attorney General supports Senate Bill 169 (“SB 169”), sponsored by Senators Feldman, Augustine, Brooks, Elfreth, Jackson, Jennings, King, Kramer, McCray, Rosapepe, Salling, Washington, and West. Senate Bill 169 provides Marylanders with privacy protections for biometric data to ensure that businesses do not keep this sensitive data longer than necessary, do not sell it, and obtain consumer consent before sharing it. Senate Bill 169 complements Maryland’s Personal Information Protection Act which ensures that businesses that collect personal information maintain it securely<sup>1</sup> by creating timelines for the destruction of biometric data and restrictions on its transfer which, in turn, will reduce the number of breaches involving biometric data.

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 enhance security. For example, the broad applications of facial recognition systems include supplanting time clocks at job sites,<sup>2</sup> replacing keys for housing units,<sup>3</sup> and aiding security at stadiums.<sup>4</sup> But it is important to recognize that biometric technology is not just

---

<sup>1</sup> The Maryland Personal Information Act covers biometric data, but it generally 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. Senate Bill 169 adds provisions specific to the unique nature of biometric data.

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

<sup>3</sup> 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>.

<sup>4</sup> Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y.

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. For example, recently the owner of Madison Square Gardens Entertainment used facial recognition to identify and bar attorneys involved in disputes against the company from entering its venues.<sup>5</sup>

Senate Bill 169 establishes reasonable limits on the collection, use, and storage of biometric data. It prohibits businesses from collecting biometric data without consumer consent.<sup>6</sup> It also prohibits businesses from selling or sharing consumer biometric data.<sup>7</sup> In addition, SB 169 requires that biometric information be destroyed when it is no longer in use.<sup>8</sup> Several other states have already enacted laws to protect consumers' biometric information, including California<sup>9</sup>, Illinois<sup>10</sup>, Texas<sup>11</sup>, and Washington.<sup>12</sup> And New York City, a city with a population larger than the entire State of Maryland, enacted a biometric ordinance that went into effect 18 months ago.<sup>13</sup> 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. Data thieves have already begun to target biometric data.<sup>14</sup>

Senate Bill 169 provides for an extremely limited remedy for individuals. Unlike the laws already in effect in Illinois and California, there is no broad private right of action. Instead, SB 169, like the New York City biometric law, provides for a private right of action only where a company violates the law by *selling* biometric data. And SB 169 further limits the scope of relief because an individual must suffer actual damages in order to recover. The scope of relief is thus very narrowly tailored and only provides for a remedy when a company profits off of violating the law and causes harm to an individual. 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.

---

Times (Mar. 13, 2018), available at

<https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>.

<sup>5</sup> <https://www.rollingstone.com/music/music-news/madison-square-garden-face-scan-1234650989/>.

<sup>6</sup> Section 14-4504(a)(1).

<sup>7</sup> Section 14-4503.

<sup>8</sup> Section 14-4502(a).

<sup>9</sup> Cal. Civ. Code § 1798.100 *et seq.*

<sup>10</sup> 740 ILCS 14.

<sup>11</sup> Tex. Bus. & Com. § 503.001.

<sup>12</sup> Wash. Rev. Code § 19.35.

<sup>13</sup> 2021 NYC Local Law No. 3, NYC Admin. Code §§ 22-1201–22-1205.

<sup>14</sup> Data thieves have already begun to target biometric data. In 2021, Nevada Restaurant Services, Inc. disclosed a privacy breach that exposed, among other personal information, customers' biometrics.

<https://www.prnewswire.com/news-releases/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event-301369180.html>. And 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/>.



Cc: Members, Finance Committee  
The Honorable Brian Feldman  
The Honorable Malcolm Augustine  
The Honorable Benjamin Brooks  
The Honorable Sarah Elfreth  
The Honorable Michael Jackson  
The Honorable J.B. Jennings  
The Honorable Nancy King  
The Honorable Benjamin Kramer  
The Honorable Cory McCray  
The Honorable Jim Rosapepe  
The Honorable Johnny Salling  
The Honorable Mary Washington  
The Honorable Chris West

**SB 169\_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 169-Commercial Law – Consumer Protection – Biometric Data Privacy**  
**FAVORABLE**  
**Senate Finance Committee**  
**February 8, 2023**

Good afternoon, Chair Griffiths and members of the Senate Finance Committee. I am Karen Morgan, a member of the Executive Council for AARP Maryland. 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 169-Commercial Law-Consumer Protection-Biometric Data 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 169 because it requires that private entities 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, because it is generally regarded as unchangeable, and because 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 ages 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 169 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 169, 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 penalty for violation of the bill's provisions is a powerful hurdle for those entities that either negligently or willfully fail to comply with the reasonable protections required in the bill. A violation is justifiably classified as an unfair, abusive, or deceptive trade practice, subject to enforcement by the Office of Attorney General. At the same time, the bill still preserves a private right of action for losses or injuries suffered due to actions prohibited under the bill. The reach of this provision is fair and balanced, as it limits an award to compensation for damages suffered. The bill also specifies that a person may not frivolously bring an action or act in bad faith.

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 169 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](mailto:tbresnahan@aarp.org) or by calling 410-302-8451.

**SB 169 Economic Action Maryland Letterhead (1).pd**

Uploaded by: Marceline White

Position: FAV



Testimony to the House Economic Matters Committee  
SB 169: Commercial Law-Consumer Protection-Biometric Identifiers  
Privacy

Position: Favorable

February 9, 2022

The Honorable Melony Griffith, Chair  
Senate Finance Committee  
Third Floor, Miller Senate Office Building  
Annapolis, Maryland 21401  
Cc: Members, Senate Finance Committee

Honorable Chair Griffith and Members of the Committee:

Economic Action Maryland (formerly the Maryland Consumer Rights Coalition) is a people-centered movement to expand economic rights, housing justice, and community reinvestment for working families, low-income communities, and communities of color. Economic Action Maryland provides direct assistance today while passing legislation and regulations to create systemic change in the future.

We are here today in strong support of SB 169. SB 169 provides common-sense guardrails to protect Marylanders biometric privacy. Many of these protections in SB 169 are enshrined in law for other types of data to protect consumers-SB 169 extends these protections to address modern technological advances.

Biometric identifiers (palm, fingerprint, iris, voice, face) are increasingly being used by law enforcement, airports, property management firms, and employers. Currently there are no restrictions on how companies collect, analyze, store, share, or sell our personal biometric identifiers. Unlike a credit card, we can't get new biomarkers.

Although use of biometric identifiers is becoming more widespread, these markers, particularly use of facial recognition tools have been found to be racially biased and inaccurate. A 2018 Gender Shades study found that facial recognition tools performed the worst on darker-skinned females, with error rates up to 34% higher than for lighter-skinned males.

2209 Maryland Ave · Baltimore, MD · 21218 · 410-220-0494

[info@econaction.org](mailto:info@econaction.org) · [www.econaction.org](http://www.econaction.org) · Tax

ID 52-2266235

Economic Action Maryland is a 501(c)(3) nonprofit organization and your contributions are tax deductible to the extent allowed by law.

SB 169 requires individuals affirmative consent before a company can collect or use their biometric information, limits the disclosure and sharing of biometric information, allows a private right of action, and creates clarity around how this information may be collected, used, and stored.

For all of these reasons, we support SB 169 and urge a favorable report.

Best,

Marceline White  
Executive Director

2209 Maryland Ave · Baltimore, MD · 21218 · 410-220-0494

[info@econaction.org](mailto:info@econaction.org) · [www.econaction.org](http://www.econaction.org) · Tax

ID 52-2266235

Economic Action Maryland is a 501(c)(3) nonprofit organization and your contributions are tax deductible to the extent allowed by law.

# **EPIC-Testimony-MD-BiometricPrivacy-Feb2023.pdf**

Uploaded by: Jake Wiener

Position: FWA



February 7, 2023

The Honorable Melony Griffith, Chair  
Senate Finance Committee  
Maryland General Assembly  
3 East  
Miller Senate Office Building  
Annapolis, MD 21401

Dear Chair Griffith and Members of the Committee:

EPIC writes in support of SB169/ HB33 regarding biometric identifiers and biometric information privacy. Biometric data is highly sensitive. A person's biometric data is linked to that person's dignity, autonomy, safety, and identity.<sup>1</sup> Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. SB169 would protect Marylanders by requiring that the use and retention of biometric data is minimized and that data is kept secure.

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.<sup>2</sup> EPIC has long advocated for strict limits on the collection and use of biometric data.<sup>3</sup>

Late last year, the owner of Madison Square Garden and Radio City Music Hall began using facial recognition to deny all lawyers working for law firms engaged in litigation against MSG access to concerts and sporting events.<sup>4</sup> Radio City Music Hall refused entry to the chaperone of a Girl Scout troop going to see the annual "Christmas Spectacular" show because of who she works for. Facial recognition makes it possible to gate entry to otherwise public spaces. Despite public outcry, MSG owner James Dolan recently "doubled down" on using facial recognition to exclude his personal enemies.<sup>5</sup> A business owner could just as easily use facial recognition deny services to

---

<sup>1</sup> Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

<sup>2</sup> EPIC, *About EPIC*, <https://epic.org/epic/about.html>.

<sup>3</sup> See e.g. Brief for EPIC as Amici Curiae, *Patel v. Facebook.*, 932 F.3d 1264 (9th Cir. 2019), <https://epic.org/amicus/bipa/patel-v-facebook/>;

Brief for EPIC as Amici Curiae, *Rosenbach v. Six Flags Entm't Corp.*, 2017 Ill. App. 2d 170317 (Ill. 2019), <https://epic.org/amicus/bipa/rosenbach/>; Comments of EPIC to the Dept. of Homeland Security, *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 F.R. 56338, 4 (Oct. 13, 2020), <https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf>.

<sup>4</sup> Kashmir Hill and Cory Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. Times (Jan. 3, 2023), <https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html>.

<sup>5</sup> Aaron McDade, *James Dolan defends use of facial-recognition technology to ban entry into Madison Square Garden and Radio City Music Hall*, Insider (Jan. 28, 2023), <https://www.businessinsider.com/james-dolan-stands-behind-msg-facial-recognition-ban-entry-2023-1?op=1>.

members of this Committee who voted against the owner's interests. A biometric privacy bill like SB169 would prevent this and many other harms.

SB169 is modeled after the Illinois Biometric Information Privacy Act (BIPA).<sup>6</sup> Passed in 2008, BIPA has been referred to as one of the most effective and important privacy laws in America.<sup>7</sup> BIPA and SB169 set out a simple privacy framework: businesses may not sell, lease, trade, or otherwise profit from a person's biometric information; businesses must comply with specific retention and deletion guidelines; and companies must use a reasonable standard of care in transmitting, storing, and protecting biometric information that is as protective or more protective than the company uses for other confidential and sensitive information.

BIPA and SB169 also include a requirement that a business obtains informed, written consent before collecting or otherwise obtaining a person's biometric information. Though "notice-and-choice" regimes are not sufficient to protect privacy, the consent provision has proven to be effective in Illinois because it is easy to enforce. It is much easier for an individual to discover and prove that a company collected their biometric data without the requisite consent than it is to prove a violation of the retention and deletion rules that are implemented by businesses after the data is collected. We encourage the Committee to retain this provision.

As this bill moved through the House last year, the private right of action was weakened to require individuals to prove injury or loss sustained as a result of a violation of the law, rather than simply a violation of the law qualifying as an injury-in-fact, as it does in Illinois. Unfortunately, SB169 mirrors this change, which renders the private right of action almost meaningless. Although the impact of improper collection and use of an individual's biometric data is very serious, the ability for an individual to prove harm is particularly difficult.<sup>8</sup> Unlike physical crimes, harms arising from improper data collection or inadequate data protection are often concealed. In addition, the harms caused by such privacy violations are not easily quantified, though the consequences of a lost job, denial of entry to public spaces, or breach of one's biometric information are very real.

If Maryland passes this law to enshrine a right for Marylanders to avoid the improper collection of their biometric data, that right should be enforceable. EPIC recommends reverting to the private right of action provisions from the bill as introduced last session.

The inclusion of a private right of action in SB169 is the most important tool the Legislature can give to Marylanders to protect their privacy. Modeled after BIPA's private right of action, the bills would impose enforceable legal obligations on companies that choose to collect and store individuals' biometric data. As EPIC Advisory Board member Professor Woody Hartzog has written:

---

<sup>6</sup> 740 Ill. Comp. State. Ann. 14/15.

<sup>7</sup> Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>.

<sup>8</sup> See e.g. Brief for EPIC as Amici Curiae, *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), <https://epic.org/wp-content/uploads/amicus/spokeo/EPIC-Amicus-Brief.pdf>.

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook’s share price actually rose 2 percent after the FTC announced its historic \$5 billion fine for the social media company’s privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. [...] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.<sup>9</sup>

The ACLU’s suit against facial recognition company Clearview AI recently settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.<sup>10</sup> BIPA does not just provide Illinoisans with more privacy than most other states, it has nationwide consumer protection effects that similar laws like SB169 will bolster.

EPIC also recommends that any exceptions to the written consent requirement be narrowly defined to avoid abuse. Under SB169 §14-4505 (b)(1)(I), private entities may “collect, use, disclose, redisclose, or otherwise disseminate” biometric information without an individuals’ consent for “fraud prevention or security purposes”. Although such purposes may be legitimate, overly broad definitions of security purposes invite abuse. EPIC suggests the following language to narrow the definition of security purposes under which the use of biometrics should be allowed:

1. To respond to a security incident. For purposes of this paragraph, security is defined as network security and physical security and life safety.
2. To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services. For purposes of this paragraph, the term “illegal activity” means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm.

These narrower definitions would prevent pretextual uses like the deployment of facial recognition at Madison Square Garden and prevent generalized security concerns from validating broad surveillance practices like Clearview AI.

## **Conclusion**

An individual’s ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security and privacy. The unregulated collection and use of biometrics threatens that right to privacy and puts individuals’ identities at risk. We urge the Committee to give SB169 a favorable report with amendment.

---

<sup>9</sup> Hartzog, *supra* note 7.

<sup>10</sup> Ryan Mac and Kashmir Hill, *Clearview AI settles suit and agrees to limit sales of facial recognition database*, N.Y. Times (May 9, 2022), <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>.

If EPIC can be of any assistance to the Committee, please contact EPIC Deputy Director Caitriona Fitzgerald at [fitzgerald@epic.org](mailto:fitzgerald@epic.org).

Sincerely,

/s/ Caitriona Fitzgerald  
Caitriona Fitzgerald  
EPIC Deputy Director

/s/ Jake Wiener  
Jake Wiener  
EPIC Counsel

**2023 CBAC SB169 HB33 Biometric Bill Amendment.pdf**

Uploaded by: Michael Johansen

Position: FWA

Alan M. Rifkin  
M. Celeste Bruce (MD, DC)  
Stuart A. Cherry  
Michael T. Marr (MD, DC, VA, NC)  
Edgar P. Silver (1923-2014)  
†Of Counsel  
††Retired Emeritus

Arnold M. Weiner  
Charles S. Fax (MD, DC, NY)†  
Brad I. Rifkin  
William A. Castelli  
Michael A. Miller†

Scott A. Livingston (MD, DC)  
Jamie Eisenberg Katz (MD, DC, NY)  
Camille G. Fesche (MD, DC, NY, NJ)  
Geoffrey W. Washington  
Laurence Levitan††

Michael V. Johansen  
Barry L. Gogel  
Michael D. Berman (MD, DC)†  
Devon L. Harman  
Lance W. Billingsley††

Joel D. Rozner (MD, DC)  
Liesel J. Schopler (MD, DC)  
Madelaine Kramer Katz (MD, DC, VA)  
Brian Chorney (MD, DC, FL)  
John C. Reith (Nonlawyer/Consultant)  
Matthew Bohle (Nonlawyer/Consultant)  
Obie L. Chinemere (Nonlawyer/Consultant)

**TESTIMONY OF CBAC GAMING (HORSESHOE CASINO BALTIMORE)  
IN SUPPORT WITH AMENDMENTS  
SB 169 / HB 33 “Commercial Law – Consumer Protection – Biometric Data Privacy”**

CBAC Gaming is the licensee of Horseshoe Casino Baltimore. Horseshoe is one of the state’s six video lottery facilities and offers slots, table games and sports wagering. The Maryland Lottery & Gaming Control Agency has established a comprehensive regulatory framework to protect the state’s interests in commercial gaming and ensure both the casino operator and casino patrons comply with the state’s laws and standards. SB 169 / HB 33 restricts a casino’s use of biometric data and these restrictions could hamper a casino’s efforts to prevent fraud, theft and other illicit activities occurring on the property. The amendment below removes the restrictions for gaming/wagering entities licensed by the state. 14-4502.

(A) (1) EXCEPT AS PROVIDED IN PARAGRAPH (3) OF THIS SUBSECTION AND SUBSECTION (B) OF THIS SECTION, EACH PRIVATE ENTITY IN POSSESSION OF BIOMETRIC DATA SHALL DEVELOP A WRITTEN POLICY, MADE AVAILABLE TO THE PUBLIC, ESTABLISHING A RETENTION SCHEDULE AND GUIDELINES FOR PERMANENTLY DESTROYING BIOMETRIC DATA ON THE EARLIEST OF THE FOLLOWING:

- (I) THE DATE ON WHICH THE INITIAL PURPOSE FOR COLLECTING OR OBTAINING THE BIOMETRIC DATA HAS BEEN SATISFIED;
- (II) WITHIN 3 YEARS AFTER THE INDIVIDUAL’S LAST INTERACTION WITH THE PRIVATE ENTITY IN POSSESSION OF THE BIOMETRIC DATA; OR
- (III) WITHIN 30 DAYS AFTER THE PRIVATE ENTITY RECEIVES A VERIFIED REQUEST TO DELETE THE BIOMETRIC DATA SUBMITTED BY THE INDIVIDUAL OR THE INDIVIDUAL’S REPRESENTATIVE.

(2) ABSENT A VALID WARRANT OR SUBPOENA ISSUED BY A COURT OF COMPETENT JURISDICTION, EACH PRIVATE ENTITY IN POSSESSION OF BIOMETRIC DATA SHALL COMPLY WITH THE RETENTION SCHEDULE AND DESTRUCTION GUIDELINES DEVELOPED UNDER PARAGRAPH (1) OF THIS SUBSECTION.

(3) A PRIVATE ENTITY IN POSSESSION OF BIOMETRIC DATA FOR FRAUD PREVENTION OR SECURITY PURPOSES IS NOT REQUIRED TO DESTROY AN INDIVIDUAL’S BIOMETRIC DATA IN ACCORDANCE WITH PARAGRAPH (1)(II) AND (III) OF THIS SUBSECTION IF THE INDIVIDUAL IS PART OF THE STATE VOLUNTARY EXCLUSION PROGRAM **ENTITY IS LICENSED BY THE MARYLAND STATE LOTTERY AND GAMING CONTROL AGENCY.**

Submitted by: Michael Johansen, RWL for CBAC Gaming  
[mjohansen@rwllaw.com](mailto:mjohansen@rwllaw.com) 410.591.6014

# **Chamber of Progress MD SB 169\_Submitted Testimony.**

Uploaded by: Alain Xiong-Calmes

Position: UNF



February 8, 2023

The Honorable Melony Griffith, Chair  
Senate Finance Committee  
Miller Senate Office Building  
11 Bladen Street  
Annapolis, Maryland 21411

RE: OPPOSE: SB 169 (Feldman): Commercial Law – Consumer Protection –  
Biometric Data Privacy

Dear Chair Griffith and members of the Committee:

Thank you for the opportunity to submit testimony for the record regarding SB 169. On behalf of the Chamber of Progress, a tech industry coalition promoting technology's progressive future, I write to urge you to oppose SB 169, which imposes unworkable hurdles for businesses trying to use biometric technology to increase security for their customers.

Our organization works to ensure that all Americans benefit from technological leaps. Our corporate partners include companies like Amazon, Apple, Pindrop, and CLEAR, but our partners do not have a vote on or veto over our positions.

### **SB 169's Provisions are Ill-Suited for Modern Applications of Biometric Technology**

Biometrics improve the security of important transactions, electronic devices, and online accounts. Biometrics improve security by assigning a value unique to an individual that cannot be lost, forgotten, faked, guessed, written on a Post-It note, or obtained via social engineering. This vastly improves the security of online accounts and phone transactions by eliminating some of the most common ways that hackers and identity thieves access private accounts.



We appreciate your attempts to address the security concerns created by other biometrics privacy bills and include carve-outs for anti-fraud and security features. Unfortunately, **some requirements under SB 169 are ill-suited to the modern environment** and would create hurdles for businesses trying to use biometric technology to increase security for their customers.

The bill's requirement to obtain "affirmative written consent" for use of biometric data makes no provision for, and offers no exceptions for, situations where obtaining such consent would be impossible or impracticable.

For example, augmented reality services can make it significantly easier for those with visual or hearing impairments to navigate the world. It might be possible to collect consent from work colleagues to wear glasses that recognize faces and tell the visually impaired person who entered a room, but it might not be possible when attending large conferences or meeting with external groups.

While the bill provides an exception to the consent requirement for anti-fraud and security features, the requirement of posting "conspicuous written notice" at every point of collection could still be unworkable. The notice requirement would be impractical, for instance, when a customer was attempting to access account information over the phone and was asked to verify their identity through voice recognition.

Additionally, the bill's requirement that companies return data to consumers upon request, while well-intentioned, runs the risk of exposing sensitive information to hackers. SB 169 requires any entity in possession of an individual's biometric data to disclose that data and information about its use upon request. Other state privacy laws, like in California and Colorado, include similar provisions but allow companies to delay their responses in order to address security concerns<sup>1</sup> or merely confirm the data in their possession.<sup>2</sup> These guardrails prevent companies from being forced to turn over data via insecure channels, leaving unique biometric identifiers in email inboxes or cloud accounts, or to turn over sensitive data to fraudsters posing as authorized representatives.

---

<sup>1</sup> [https://leg.colorado.gov/sites/default/files/2021a\\_190\\_signed.pdf](https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf)

<sup>2</sup> [https://leginfo.legislature.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5)

## **Vague Standards in SB 169 Create Compliance and Security Risks**

Additionally, many of the bill's standards are not clearly defined, leaving unanswered questions about how companies should implement consumer protections.

### ***“Strictly necessary” standard creates uncertainty for companies.***

The vague standards under the anti-retaliation provisions could create burdensome requirements for companies implementing biometric technology. SB 169 prevents entities from offering different “levels or quality” of service or charging “different prices” if a consumer declines to consent to use of biometric data. Entities may decline to provide a service to a consumer who withholds consent, but only if the biometric data is “strictly necessary” to the service.

However, how this “strictly necessary” standard would apply remains unclear. For example, if a business takes on additional financial risk when a consumer declines biometric authentication of a transaction, but the consumer still wants to conduct it remotely, would the business allow it?

If biometrics in a product allows speed, convenience, or additional personalization, must businesses re-engineer their products to provide an alternative under the “strictly necessary” standard? Many smart home devices include the option to apply voice recognition to seamlessly switch between settings for different family members. Without more guidance about how the “strictly necessary” standard applies, companies may be forced to develop equivalent features that can identify different individuals for preference setting without using voice recognition in order to avoid accusations of “conditioning” access on the use of biometrics.

### ***“Authorized legal representatives” needs further clarification.***

Additionally, the bill does not provide guidance for companies to authenticate “authorized legal representatives,” increasing the risk of delays to consumer requests or outright fraud. A non-native English speaking customer might want to designate a representative to exercise their rights, but the bill does not lay out the proper forms or authentication required. Even worse, a scammer could pose as an authorized representative to collect vast amounts of sensitive information.

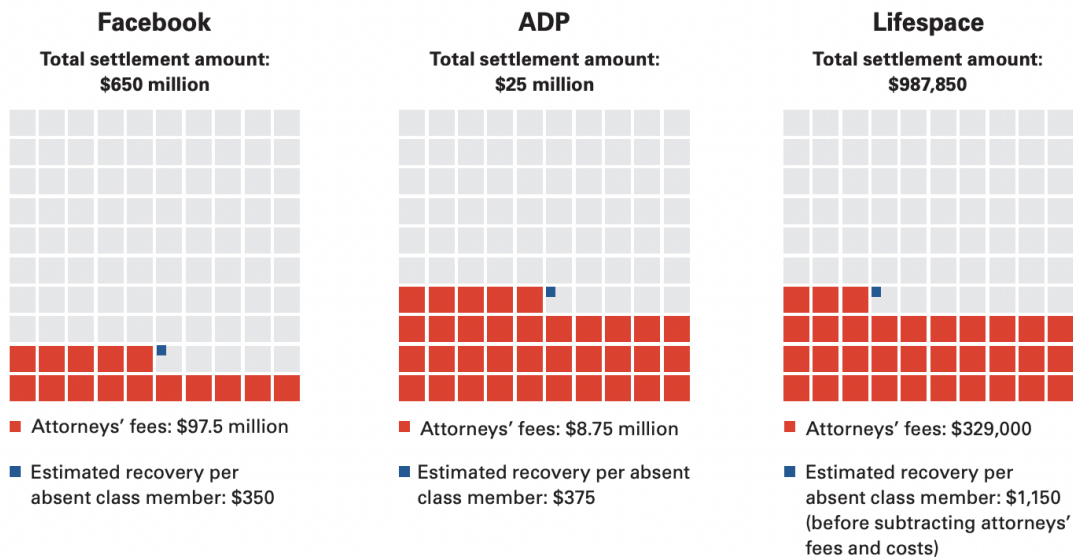
Without more guidance as to how to authenticate authorized representatives, companies could be forced to give up information to bad actors.

### Enforcement Mechanisms Could Reduce Options for Consumers

Coupling these vague standards with a private right of action could result in businesses denying access to Maryland customers altogether for fear of a lawsuit.

SB 169 allows individuals to take private action against companies for violations. This approach is similar to the one followed in Illinois, where class action lawsuits skyrocketed after the passage of the Biometric Information Privacy Act in 2008. Unfortunately, as shown in the graphic below, those lawsuits primarily benefited trial attorneys rather than individual plaintiffs.<sup>3</sup>

**Figure 4: Attorneys' Fees as a Proportion of BIPA Settlements<sup>23</sup>**



These lawsuits had a chilling effect for consumers in Illinois. Augmented reality products, like face filters, were blocked for users in the state,<sup>4</sup> and some companies opted not to sell their products in the state at all.<sup>5</sup> The vague standards in SB 169 could result in companies opting not to offer their products, like the popular Amazon Ring or Google Nest, to Maryland consumers at all, for fear of inadvertent violations resulting in costly lawsuits.

<sup>3</sup> <https://institutelegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf>

<sup>4</sup>

<https://www.chicagotribune.com/business/ct-biz-meta-pulls-augmented-reality-biometrics-cb-20220518-rp7a6bd7afae5djil24yjy6pgy-story.html>

<sup>5</sup> <https://www.sony.com/electronics/support/smart-sports-devices-entertainment-robots/ers-1000/articles/00202844>

We welcome the opportunity to work with the committee to create alternative legislation that will benefit consumers without the consequences described above. For example, allowing a cure period of 30 days would give companies acting in good faith the opportunity to address inadvertent violations without stifling innovation.

Privacy laws and safeguards are crucial to the protection of Maryland consumers. We appreciate the author's attempts to protect security and anti-fraud products, but we believe more work needs to be done to avoid unintended consequences for businesses and consumers.

Thank you,

**Alain Xiong-Calmes**

Director of State and Local Public Policy, Northeast US  
Chamber of Progress

**MCPA-MSA\_SB 169\_Biometric Data Privacy\_OPPOSE.pdf**

Uploaded by: Andrea Mansfield

Position: UNF



# Maryland Chiefs of Police Association

## Maryland Sheriffs' Association



### MEMORANDUM

TO: The Honorable Melanie Griffith, Chair and  
Members of the Finance Committee

FROM: Darren Popkin, Executive Director, MCPA-MSA Joint Legislative Committee  
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee  
Natasha Mehu, Representative, MCPA-MSA Joint Legislative Committee

DATE: February 8, 2023

RE: **SB 169 – Commercial Law – Consumer Protection – Biometric Data Privacy**

POSITION: **OPPOSE**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs' Association (MSA) **OPPOSE SB 169**. This bill sets standards and mandates policies and procedures private entities must follow when handling biometric data but does so in an overly broad and restrictive manner that conflicts with recently established privacy laws under Title 17 of the Criminal Procedure Article and jeopardizes criminal investigations.

The MCPA and MSA are significantly concerned with the impact this bill would have on the ability of law enforcement to use advancements in DNA and ancestry technology to solve difficult criminal cases. In 2021, legislation was passed into law establishing important guardrails and protocols for law enforcement and ancestry databases that govern how biometric data can be used for the investigative process of Forensic Genetic Genealogy. The provisions in Title 17 of the Criminal Procedure Article were carefully worded to balance the need for privacy protections while allowing individuals to voluntarily share the DNA they have provided to ancestry databases with law enforcement to help solve crimes. SB 169 would override all those thoughtful provisions and prevent the effective use of Forensic Genetic Genealogy.

Some of the most concerning aspects of SB 169 are the definition of biometric data in 14-4501, the mandatory destruction protocols in 14-4502, and the various non-disclosure provisions in 14-4503 – 14-4505. Among other things, these provisions require the mandatory destruction of all biometric data in the possession of private entities including DNA profiles that consumers have provided to certain ancestry search companies. The provisions do not reflect or account for the provisions in Title 17 or federal guidelines that were established to specifically deal with the sensitive nature of Forensic Genetic Genealogy.

Forensic Genetic Genealogy has been critical for solving decades-old cold cases. Most notably the technology was used to identify the Golden Gate Killer. It is important to note that DNA from ancestry databases can only be used for law enforcement purposes with the explicit consent of the individual submitting their DNA and that not all databases chose to partner with law enforcement. This process is truly voluntary and ensures that all parties involved are adhering to stringent privacy protections and biometric data management established under both Title 17 and US Department of Justice guidelines.

Local law enforcement is actively working on cases using Forensic Genetic Genealogy. For instance, the Prince George's County Police Department's Cold Case Homicide Unit in partnership with the Prince George's County State's Attorney's Office is currently working on 15 cold cases involving murder or sex offenses. The Prince George's State's Attorney's Office was awarded a \$470,000 grant to support the investigation of unsolved homicides and sex offense cases using recently developed forensic genealogy (FGG) processes. Local agencies across the state are even partnering with the FBI's Investigative Genealogy Unit on some of their cold cases. The passage of SB 169 as written would hinder the ability of the department to work locally or with their federal partners to use this innovative and burgeoning technology to solve these crimes and bring justice to the victims and their families.

DNA and Forensic Genetic Genealogy are extraordinary investigative tools for identifying violent offenders that would be crippled by the passage of this bill. It is critical to ensure that there are exemptions that allow for the continued use of Forensic Genetic Genealogy and the regulatory provisions already established under Title 17. For these reasons, MCPA and MSA **OPPOSE SB 169** and urge an **UNFAVORABLE** report.

# **SB 169\_MDCC\_Commercial Law–Biometric Data Privacy\_**

Uploaded by: Andrew Griffin

Position: UNF





**LEGISLATIVE POSITION:**

**Unfavorable**

**Senate Bill 169**

**Commercial Law – Consumer Protection – Biometric Data Privacy**

**Senate Finance Committee**

**Wednesday, February 8, 2022**

Dear Chairwoman Griffith 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 6,400 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 169 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 169 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 contained in SB 169, Maryland businesses remain concerned about the impacts this legislation could have on the use of biometric technology for security, identification, and authentication purposes to prevent and detect fraud. Concerns include:

- The retention policy outlined in SB 168 mandates the destruction of biometrics that are fundamental to businesses preventing fraud and keeping their customers safe. This hampers a business' 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, methods and information 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 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.
- Recently enacted security laws in California, Colorado, and Virginia all provide a two-year delay in enforcement. SB 169 goes into effect on October 1, 2023. This tight turnaround presents real challenges for compliance, particularly as SB 169 requires sweeping changes to how businesses manage biometric data.

Maryland residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation and job creation. The Maryland Chamber of Commerce is committed to working alongside the bill sponsors and impacted partners to address 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 169**.



**SPSC MD SB 169 FINANCE UNF.pdf**

Uploaded by: Andrew Kingman

Position: UNF

# STATE PRIVACY & SECURITY COALITION

February 8, 2023

Chair Melony Griffith  
Vice Chair Katherine Klausmeier  
3 East  
Miller Senate Office Building  
Annapolis, Maryland 21401

**Re: SB 169 (Biometrics) – Opposition**

Dear Chair Griffith and Vice Chair Klausmeier,

The State Privacy & Security Coalition, a coalition of over 30 companies and five trade associations in the retail, automotive, technology, telecom, and payment card sectors, writes in opposition to SB 169, which would decrease consumer safety and significantly impact the state's economy. The bill is based on an outdated Illinois law, the Biometric Information Privacy Act (BIPA), that was passed in 2008 – less than a year after the smartphone was invented. The abuse of the private right of action (PRA) in the law, as well as the evolution of the online ecosystem, has led to bipartisan efforts in Illinois to reform the statute so as to eliminate the problems that have plagued it since its passage.

SPSC strongly supports consumer protections for personal data that can identify individuals. Effective privacy legislation should appropriately balance increased consumer control over their data and how it is used, while balancing the need for operational workability and cybersecurity.

Fortunately, privacy law has evolved since 2008, and in fact has evolved rapidly in the last two years. States such as Connecticut and Colorado have passed comprehensive privacy laws that cover a broad swath of personal data. These bills provide:

- strong, opt-in protections for consumers with regard to biometrics and other sensitive data;
- a greater number of consumer rights (access, deletion, correction, portability), opt-out of sale, targeted advertising, and profiling;
- strong obligations on businesses to document data processing activities that present a heightened risk of harm; and
- strong contractual requirements for entities that handle personal data – including biometrics – on behalf of the entities that collect the data.

These laws provide stronger protections for biometric data than SB 169, but do so in a way that much more accurately reflects the divided responsibilities of “controllers” and “processors.” We would strongly urge the legislature to consider moving forward with the Colorado or Connecticut model rather than pursue legislation that, in Illinois, has caused startups to avoid offering products in the state and safety products that are diminished due to the omnipresent litigation threat.

# STATE PRIVACY & SECURITY COALITION

## The Private Right of Action Will Make Consumers Less Safe

First, including a private right of action for statutory damages would create massive class action litigation exposure for any *alleged* violations of the law by commercial entities, significantly deterring uses of biometric data including for anti-fraud, authentication and other security purposes that benefit consumers. As in Illinois, the result would be to enrich trial lawyers without striking a balance that allows the use of biometric data for purposes that benefit Maryland residents. Put simply, a private right of action means businesses will be much less likely to offer services that keep Maryland residents' identities safe.

The litigation numbers bear this out: in the last five years, trial lawyers have filed *nearly 1000 class action lawsuits based on BIPA*. 14 years of experience with Illinois' law have shown that this approach leads businesses to decline to offer their full suite of services to state residents, or avoid offering their services in the state at all, due to the overzealous litigation this legislation catalyzed. For this reason, Illinois is considering amending the law in order to address this significant unintended consequence and bring beneficial services back to Illinois consumers.

This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest on the merits of the case, but instead on the opportunity to inflict asymmetrical discovery costs on businesses both small and large – with a cost to defend these frivolous actions averaging \$500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal discovery costs, huge negotiating leverage for nuisance settlements, even if the defendant is compliant with the law. In fact, ***only a single case has ever been brought to trial.***

Furthermore, studies have revealed that private rights of action fail to compensate consumers ***even when a violation has been shown***, and instead primarily benefit the plaintiff's bar by creating a "sue and settle" environment.<sup>1</sup> This is not to say that Maryland lacks effective enforcement options outside the trial bar – to the contrary, it has a strong consumer protection statute that the Attorney General can use *right now* to punish bad actors. On the other hand, the PRA in Illinois has not only failed to meaningfully protect consumers, but actually made them less safe, as anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.

## SB 169 Has Significant Anti-Privacy and Anti-Security Consequences

Additionally, SB 169 provides an access right for consumers with regard to their biometric information and other types of "personal information." We believe that implementing the overbroad provisions related to this right will present real, if unintended, threats of harm to consumers. Additionally, the vast majority of biometric information is hashed, meaning that it is

---

<sup>1</sup> Mark Brennan et al., *Ill-Suited: Private Rights of Action and Privacy Claims*, U.S. Chamber Institute for Legal Reform (July 2019).

# STATE PRIVACY & SECURITY COALITION

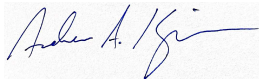
converted to a lengthy numeric value. Consumers will not derive any meaning from this numerical sequence, or any understanding of how their information is used that is not already covered by a business's privacy policy.

Disclosing actual biometric identifiers upon consumer request also poses significant security concerns, as the bill does not allow a private entity to refrain from disclosing biometric identifiers or other sensitive information like Social Security Numbers to an individual if the business cannot reasonably authenticate the request. Even California's privacy law recognizes and accounts for this security concern, making clear that a business "shall not disclose in response to a[n access request] a consumer's...unique biometric data."<sup>2</sup>

SB 169 includes a provision allowing for "authorized representatives" of consumers to request and obtain this very sensitive data, but provides no methods that would allow the business to verify that a) the consumer is who they say they are, and b) the authorized representative has the proper authority to exercise this right. The lack of these types of authentication and security provisions leave consumers extremely vulnerable to being taken advantage of. Vulnerable populations such as the elderly could easily designate their authority to a scammer, believing that the individual is safeguarding their data.

These are just some of the significant issues with SB 169 as drafted. Again, we would urge this committee to consider alternative, more modern, and more expansive data privacy protections for Maryland consumers that are more balanced, work across state lines, and do not create risks of frivolous litigation.

Respectfully,



Andrew A. Kingman  
Counsel, State Privacy & Security Coalition

---

<sup>2</sup> See 11 CCR §999.313(c)(4).

**SB169\_PGCEX\_OPP.pdf**

Uploaded by: Angela Alsobrooks

Position: UNF



# THE PRINCE GEORGE'S COUNTY GOVERNMENT

## OFFICE OF THE COUNTY EXECUTIVE

**BILL:** SB 169 - Commercial Law - Consumer Protection - Biometric Data Privacy

**SPONSOR:** Senator Feldman

**HEARING DATE:** February 08, 2023

**COMMITTEE:** Finance Committee

**CONTACT:** Intergovernmental Affairs Office, 301-261-1735

---

**POSITION:** OPPOSE

---

The Office of the Prince George's County Executive **OPPOSES Senate Bill 169 - Commercial Law – Consumer Protection – Biometric Data Privacy** which sets standards and mandates policies and procedures private entities must follow when handling biometric data but does so in an overly broad and restrictive manner that conflicts with recently established privacy laws under Title 17 of the Criminal Procedure Article and jeopardizes criminal investigations.

Prince George's County State Attorney's Office received a grant from the Department of Justice for the purposes of utilizing Forensic Genetic Genealogy. Forensic Genetic Genealogy has been instrumental in assisting Law Enforcement with decade old cases that were lacking further leads. It is an investigative tool that will continue to produce successful outcomes in criminal investigations that would otherwise remain unsolved.

Prince George's County Police Department has been successful in solving a cold case homicide using Forensic Genetic Genealogy. Matthew Mickens-Murrey was found stabbed to death in his apartment in Cheverly on May 30, 2017. Family members called police after Matthew failed to report for work as a security guard that day. When police responded to his apartment, they found Matthew lying face down in his living room, suffering from stab wounds.

Crime Scene Investigators collected evidence from the scene which included a bloody fingerprint that did not belong to the victim. It was clear the murderer was injured at some point while committing the brutal crime. A DNA profile of the bloody fingerprint was submitted to both the national fingerprint and DNA data bases maintained by the FBI - but no match was obtained.

After an extensive investigation failed to develop any promising leads, the case went cold for several years. Finally, in 2019, the unidentified blood evidence was submitted to a private laboratory to develop a profile for Forensic Genetic



Genealogy. Forensic Genetic Genealogy looks at more than half a million single nucleotide variations to DNA (called single nucleotide polymorphism, or SNP). The SNPs can identify family traits from sections of the DNA recovered at a crime scene sample to distant relatives.

In Matthew's case, the private laboratory developed a profile and then work building the family tree began. This ultimately led to a possible suspect in Charles County, but more police investigation was needed. Further investigation indicated the potential suspect, Brandon Biagas, suffered a serious injury the night of the murder. He sought medical treatment at a hospital in Charles County. When questioned by a deputy sheriff at the hospital, Mr. Biagas gave inconsistent and contradictory versions of how he injured his hand, which he claimed took place during the purchase of marijuana at a park in Waldorf. The deputies collected a knife and bloody clothing from his vehicle pursuant to a court-ordered search and seizure warrant. The evidence the Charles County Sheriff's Office collected was not submitted to CODIS because no qualifying crime was identified to justify a submission. Years after the murder, and thanks to the lead provided by the forensic genetic genealogy process, Brandon Biagas was identified as the donor of the bloody fingerprint found in Matthew's apartment. He ultimately pleaded guilty to second-degree murder and was sentenced to a lengthy prison sentence.

The passage of **SB 169** would hinder what has become an invaluable tool for law enforcement to use to resolve unsolved homicides, sexual assaults as well as identify human remains

For these reasons, the office of the County Executive **OPPOSES Senate Bill 169** and asks for a **UNFAVORABLE** report.

# **SB0169\_UNF\_MTC\_Commercial Law - Consumer Protectio**

Uploaded by: Drew Vetter

Position: UNF



# MARYLAND TECH COUNCIL

TO: The Honorable Melony Griffith, Chair  
Members, Senate Finance Committee  
The Honorable Brian J. Feldman

FROM: Pamela Metz Kasemeyer  
J. Steven Wise  
Danna L. Kauffman  
Andrew G. Vetter  
Christine K. Krone  
410-244-7000

DATE: February 8, 2023

RE: **OPPOSE** – Senate Bill 169 – *Commercial Law – Consumer Protection – Biometric Data Privacy*

---

The Maryland Tech Council (MTC) writes in **opposition** to *Senate Bill 169: Commercial Law – Consumer Protection – Biometric Data Privacy*. We are a community of over 700 Maryland member companies that span the full range of the technology sector. Our vision is to propel Maryland to become the number one innovation economy for life sciences and technology in the nation. We bring our members together and build Maryland's innovation economy through advocacy, networking, and education.

Consumer privacy is of the utmost importance to members of the MTC. Senate Bill 169, however, as drafted, poses some significant challenges for Maryland employers and could jeopardize some important advances in safety and security, as well as contribute to a perception that Maryland is not receptive to innovation. Biometric data has become an essential tool for many industries and is used 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. These technologies are good for the safety and convenience of Maryland residents. Rather than taking this restrictive approach, we believe that strong privacy laws can be paired with policies that allow industries to continue to innovate.

In addition, we are concerned about the private right of action provided for in this legislation. The ability to file individual legal actions under this law risks significant and ongoing burdens and costs for technology companies. 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.

We also believe issues of data privacy are better addressed at the federal level. Many technology companies reach into numerous states, and it can be a significant practical challenge to comply with a patchwork of state policies. These inconsistencies and resulting confusion could deter innovative companies and start-ups from wanting to do business here.

MTC believes there are alternative approaches to ensuring the privacy of residents and creating transparency around data collection and use of biometric data. We would be pleased to engage in discussions about such solutions. In summary, this bill could impose 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.

**LEYDEN--Legislative Testimony--SB 169--2-7-23.pdf**

Uploaded by: Edward Leyden

Position: UNF

**AISHA N. BRAVEBOY**  
STATE'S ATTORNEY



**JASON B. ABBOTT**  
PRINCIPAL DEPUTY STATE'S ATTORNEY

**State's Attorney for Prince George's County**  
14735 Main Street, Suite M3403  
Upper Marlboro, Maryland 20772  
301-952-3500

February 8, 2023

Testimony in **Opposition** of  
SB 169 – Commercial Law – Consumer Protection – Biometric Data Privacy

---

Dear Chairwoman Griffith, Vice Chairwoman Klausmeier, and Members of the Committee:

I am writing to show my opposition to Senate Bill (HB) 169 on behalf of State's Attorney Aisha Braveboy and to urge an unfavorable report. I am an Assistant State's Attorney in the Special Prosecutions Unit in the State's Attorney's Office for Prince George's County.

As a member of the Special Prosecutions Unit, I prosecute, in addition to vehicular homicides and particular murders, financial and property crimes (including arsons and terroristic threats). As a result, I am all too familiar with the very real assistance that evolving facial recognition technologies provide in rapidly identifying subjects for investigation and in helping to dissuade chronic offenders from even entering vulnerable venues, such as banks, hospitals, and casinos.

To be clear, the civil liberty concerns encapsulated in this proposed bill are certainly well-considered and weighty. It must also be borne in mind, however, that the bulk of the individuals that facial technologies have brought to the prosecutorial attention of this office had voluntarily entered the commercial premises where allegedly they committed their crimes – hence, the expectation of privacy such individuals could have reasonably entertained while within such premises was minimal.

In a real, practical sense, facial recognition technologies simply provide the kind of advanced institutional memory that a savvy and experienced premises security officer would command in being able to recognize those individuals who have earlier come into an establishment bent on committing crimes and causing trouble. It is, thus, vital to meeting evolving challenges that law enforcement be availed of these irreplaceable technologies.

For the foregoing reasons, I respectfully urge an unfavorable report, and ultimately rejection, on SB 169.

Sincerely,

/s/

Edward J. Leyden  
Assistant State's Attorney – Special Prosecutions Unit  
State's Attorney's Office for Prince George's County

# **1st sgt. Gregory McDonald Testimony.pdf**

Uploaded by: Gregory McDonald

Position: UNF

---

Madam Chair, Madam Vice Chair, and members of the Senate Finance Committee, I am 1<sup>st</sup> Sergeant Gregory McDonald of the Prince George's County Police Department. On behalf of Chief Malik Aziz, we are grateful for the opportunity to address you today to express our deep concern with the negative impact this bill will have on the field of Forensic Genetic Genealogy in Maryland. I'd also like to publicly thank the family of Matthew Alan Mickens-Murrey whose tragic murder was solved thanks to Forensic Genetic Genealogy. They traveled from out of state to be here today.



---

I have been a police officer for thirty-two years, a criminal investigator for the past twenty-eight years, and assigned to the Homicide Unit for the past twenty-four years. Since 2015, I have been in charge of the Cold Case Homicide Unit. Our team has fully embraced this new investigative tool, particularly in light of a Department of Justice grant that was awarded to the Prince George's County State's Attorney's Office. Forensic Genetic Genealogy is unquestionably one of the most significant advancements to recently impact law enforcement. It is an investigative tool that

---

will continue to produce successful outcomes in criminal investigations that would otherwise remain unsolved. Forensic Genetic Genealogy produces leads which law enforcement can then use to identify unknown suspects. The method can also assist in identifying unidentified human remains and the remains of homicide victims.

Please allow me to now share with you the role Forensic Genetic Genealogy played in solving the murder of Matthew Mickens-Murrey, a young man found stabbed to death in his apartment in Cheverly on May 30, 2017. Family members called police

---

after Matthew failed to report for work as a security guard that day. When police responded to his apartment, they found Matthew lying face down in his living room, suffering from stab wounds.

Crime Scene Investigators collected evidence from the scene which included a bloody fingerprint that did not belong to the victim. It was clear the murderer was injured at some point while committing the brutal crime. A DNA profile of the bloody fingerprint was submitted to both the national fingerprint and DNA data bases maintained by the FBI - but no match was obtained.

---

After an extensive investigation failed to develop any promising leads, the case went cold for several years. Finally, in 2019, the unidentified blood evidence was submitted to a private laboratory to develop a profile for Forensic Genetic Genealogy. Forensic Genetic Genealogy looks at more than half a million single nucleotide variations to DNA (called single nucleotide polymorphism, or SNP). The SNPs can identify family traits from sections of the DNA recovered at a crime scene sample to distant relatives.

---

In Matthew's case, the private laboratory developed a profile and then work building the family tree began. This ultimately led to a possible suspect in Charles County, but more police investigation was needed.

Further investigation indicated the potential suspect, Brandon Biagas, suffered a serious injury the night of the murder. He sought medical treatment at a hospital in Charles County. When questioned by a deputy sheriff at the hospital, Mr. Biagas gave inconsistent and contradictory versions of how he injured his hand, which he claimed took place during the purchase of marijuana at a park in Waldorf. The

---

deputies collected a knife and bloody clothing from his vehicle pursuant to a court-ordered search and seizure warrant. The evidence the Charles County Sheriff's Office collected was not submitted to CODIS because no qualifying crime was identified to justify a submission. Years after the murder, and thanks to the lead provided by the forensic genetic genealogy process, Brandon Biagas was identified as the donor of the bloody fingerprint found in Matthew's apartment. He ultimately pleaded guilty to second-degree murder and was sentenced to a lengthy prison sentence.

---

Were this bill before you today become law as it's now written, it would undoubtedly jeopardize leads developed from Forensic Genetic Genealogy that would aid law enforcement in resolving unsolved homicides in our state. If Forensic Genetic Genealogy is lost, any hopes of resolving unsolved homicides or identifying unidentified human remains will significantly diminish. There are thousands of unidentified DNA profiles from Maryland crime scenes that have been submitted to the national DNA data base (CODIS), and after decades, no suspect match has been developed. If leads developed by Forensic

---

Genetic Genealogy are lost, investigators will have to revert to relying on often unreliable jailhouse snitches, eyewitness identifications, and suspect confessions.

Let me close by saying that law enforcement cannot afford to lose access to this groundbreaking investigative technique, which will only continue to improve and advance criminal investigations. This would be a disservice to crime victims, their families, and the citizens of Maryland.

With the Chair's permission I would like to read a portion of a letter from family members of Matthew Mickens-Murray.



---

I respectfully ask you to join us in our opposition and return an unfavorable report on Senate Bill 169.

# **Matthew Mickens-Murray Family Letter.pdf**

Uploaded by: Gregory McDonald

Position: UNF

February 3, 2023

Dear General Assembly of The State of Maryland Finance Committee of Senate,

I am writing this letter on behalf of my brother Matthew A. Mickens-Murrey, who was the victim of a Brutal Murder. Matthew was 26 years old at the time of his demise. He was born and raised in West Chester PA and relocated to Maryland to reside with his God Sister when he graduated High School. Matthew was outgoing, energetic, and just so full of life until that life was taken by Brandon Biagas. Matthew and I were my parents only living children and now I am alone. My mother took his death the hardest due to their close bond, hence the phrase Mama's Boy cause I'm Daddy's Girl! Not to say that my father wasn't affected as well, being that Matthew was his only son and the baby of the family. I as well have a son that was only 9 years younger than Matthew, so they kind of grew up as brothers rather than Uncle and Nephew so he took it pretty hard as well, and now he has a son of his own that Matthew will never get to meet.

We waited 3 long years and stayed in consistent contact with Detective Kingston to solve this case, I refused to let my brother become a Cold Case File stuffed in a box in the basement. I then suggested to Det. Kingston that he load the suspects DNA into one of those Ancestry.com databases to at least get a lead on his Family Bloodline, and to all our surprise and great relief it actually worked and is called by law Forensic Genetic Genealogy. Without this technique I don't believe we would have ever found, prosecuted, and convicted Brandon Biagas. Although it took 3 years to catch him we consider July 23,2020 Our Justice Day and when he pleaded Guilty on December 7<sup>th</sup> 2021 we consider that Our Day of Peace and Closure.

We as a unit of Family and Friends highly recommend and encourage this technique to be utilized in assisting in solving past/present/ and future crimes in order to bring Justice and Peace to other families as it has done for ours.

Sincerely The Family of Matthew A Mickens-Murrey

Melody Mickens (Mother)	Patricia Murrey (Maternal Grandmother)
Jamy Mickens (Father)	Shelly Hugan (God Mother)
Naja Murrey (Sister)	Shanay Atkins (God Sister)
Zaevahn Murrey (Nephew)	Bonnie Murrey (Aunt)
	Crystal Murrey (Aunt)

\* All the names on the left spoke at the Sentencing Hearing (and My Mom)

**Ext. Comm. - Testimony - 2023 - Maryland SB 169 -**

Uploaded by: Joshua Fisher

Position: UNF



February 6, 2023

The Honorable Melony Griffith  
Chair, Senate Finance Committee  
3 East, Miller Senate Office Building  
Annapolis, Maryland 21401

**RE: SB 169 - Biometric Data  
Position: Unfavorable**

Chair Griffith:

The Alliance for Automotive Innovation (Auto Innovators) is writing to inform you of **our opposition to SB 169**, which establishes requirements & restrictions on private entities use, collection, & maintenance of biometric data.

From the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers – Alliance for Automotive Innovation represents the full auto industry, a sector supporting 10 million American jobs and five percent of the economy.

***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 provide heightened protection for certain types of sensitive data, including biometric data.<sup>1</sup> 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.

***Unique Considerations for Vehicle Safety Technology***

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)<sup>1</sup>. 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

---

<sup>1</sup> [https://autoalliance.org/wp-content/uploads/2017/01/Consumer\\_Privacy\\_Principlesfor\\_VehicleTechnologies\\_Services.pdf](https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf)

practices. As noted above, the auto industries “Privacy Principles” are enforceable under Section 5 of the FTC Act. We prefer this standard approach over individual states enacting disparate and conflicting laws.

SB 169 raises unique challenges for the auto industry. 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 three years after the company’s last interaction are 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 will therefore have no way of knowing when a particular customer last interacted with the vehicle.

Additionally, in the automotive context, a strict deletion requirement may interfere with automakers ability to evaluate the performance of the technology and federal requirements concerning vehicle recalls. Any deletion requirement should be accompanied by reasonable exceptions which recognize these concerns.

As written, SB 169 requires automakers to provide a service dependent on biometric data even if the consumer does not want his or her biometric data collected. It is common sense not to require a company to provide a service if the consumer is not willing to provide the data that is required to utilize said service.

Finally, under the SB 169, businesses may very well find themselves in a position of facing severe penalties for alleged violations and even very minor and inadvertent infractions and where there are no actual damages. We think existing remedies under state law are sufficient to address these issues.

Thank you for your consideration of the Auto Innovators’ position. Please do not hesitate to contact me at [jfisher@autosinnovate.org](mailto:jfisher@autosinnovate.org) or 202-326-5562, should I be able to provide any additional information.

Sincerely,



Josh Fisher  
Director, State Affairs

---

<sup>i</sup> <https://www.ftc.gov/news-events/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers>

**SB 169 SIA Oppose 02.08.23.pdf**

Uploaded by: K. Alexander Wallace

Position: UNF



February 8, 2023

The Honorable Melony Griffith  
Chair  
Senate Finance Committee  
Maryland General Assembly  
Annapolis, Maryland 21401

**RE: SIA Recommended Amendments to SB 169 Concerning Biometric Data**

Dear Chair Griffith, Vice-Chair Klausmeier and Members of the Senate Finance Committee:

On behalf of the Security Industry Association (SIA) and our members, I am writing to express our opposition to SB 169 under consideration by the committee.

SIA is a nonprofit trade association located in Silver Spring, MD that represents companies providing a broad range of safety and security-focused products and services in the U.S and throughout Maryland, including more than 40 companies headquartered in our state. Among other sectors, our members include the leading providers of biometric technologies available in the U.S. Privacy is important to the delivery and operation of many safety and security-enhancing applications of technologies provided by our industry, and our members are committed to protecting personal data, including biometric data.

We are concerned that, at a time when many states have now enacted or are considering broader data privacy measures that include protections for biometric data, and the prospect of a federal law setting nationwide data privacy rules draws nearer, SB 169 is the wrong approach, as it would import an outdated and problematic model from Illinois that is incompatible with the common frameworks that are emerging.

No other state has adopted legislation similar to the Illinois Biometric Information Protection Act (BIPA) of 2008, which has resulted in more harm to consumers and local businesses than any protections. There, businesses have been extorted through abusive “no harm” class actions, and beneficial technologies have been shelved. In fact, many of our member companies that provide products utilizing biometric technologies have chosen not to make these products or specific functions available in Illinois.

Safeguarding biometric information is important, but it should be done in a way that both protects Marylanders and allows development and use of advanced technologies that benefit them. Beyond opening the door to lawsuit abuse with enforcement through a private right of action and the harm that brings, there are also very real consequences to consumers – including their privacy – for imposing unnecessary limits through overregulation.



In several examples, as currently written SB 169 would:

- Prohibit businesses from requiring biometric identity verification to access to accounts or services, over less secure alternatives. Biometric technologies play a key role in protecting privacy during transactions that require identity verification, by preventing exposure of personal information (date of birth, Social Security Number, address, etc.) that is far more vulnerable to compromise and abuse.
- Prevent the use of screening technology to allows “fast-lane” entry at special events, and other opt-in customer services.
- Prevent long term data retention on attempted fraud attempts. Without this, identity fraudsters will have a right to be "forgotten."
- Expose sensitive biometric data to fraud due to overly broad “access rights.”
- Prevent the functionality and availability of biometric user-verification features in consumer electronics.
- Allow local jurisdictions to establish conflicting biometric data requirements.

We continue to believe that protecting biometric data is best addressed within a broader data privacy framework that protects all types of personal information. However, if the committee decides to move SB 169 forward, key changes are critical to preventing negative impact on Maryland businesses and consumers. We urge you not to approve the bill in its current form.

Again, we support the overall goal of safeguarding biometric information, and we stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,



Jake Parker  
Senior Director, Government Relations  
Security Industry Association  
Silver Spring, MD  
[jparker@securityindustry.org](mailto:jparker@securityindustry.org)  
[www.securityindustry.org](http://www.securityindustry.org)

**CCIA\_Written Comments\_MD SB 169 (Oppose).pdf**

Uploaded by: Khara Boender

Position: UNF



February 7, 2023

Senate Finance Committee  
Attn: Tammy Kraft, Committee Manager  
3 East Wing  
Miller Senate Office Building  
11 Bladen Street  
Annapolis, Maryland 21401

## Re: SB 169 - the Biometric Data Privacy Act (Oppose)

Dear Chair Griffith and Members of the Senate Finance Committee:

On behalf of the Computer & Communications Industry Association (CCIA)<sup>1</sup>, I write to respectfully oppose SB 169, the Biometric Data Privacy Act. CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.<sup>2</sup>

CCIA strongly supports the protection of consumer data and understands that Maryland residents are rightfully concerned about the proper safeguarding of their biometric data. However, as currently written SB 169 goes far beyond protecting such data, which could result in degraded consumer services and experience. We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

### 1. Align key definitions with privacy standards to promote regulatory interoperability and mitigate unnecessary compliance burdens.

By introducing a definition and compliance obligations relating to “personal information”, SB 169’s scope extends beyond the subject of “biometric” data, with multiple implications. To meet compliance requirements under a new privacy regime, businesses inevitably face logistical and financial challenges. Given the significant costs associated with developing privacy management systems, even minor statutory divergences between frameworks for

---

<sup>1</sup> CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: <https://www.ccianet.org/about>.

<sup>2</sup> Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), <https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf>

definitions or the scope of compliance obligations, can create significant burdens for covered organizations.<sup>3</sup> SB 169’s definition of personal information includes, *inter alia*, “information that indirectly relates to a device” and therefore goes far beyond what could reasonably be linked to an individual. As such, this definition should be more narrowly tailored to avoid unnecessary regulatory burdens.

## 2. Privacy protections should take a risk-based approach.

Privacy protections should be directed toward managing data collection and processing practices that pose a high risk of harming consumers or are unexpected in the context of a service. Consent mechanisms can be a powerful tool for promoting transparency and consumer control. However, it is important to recognize that the provision of many services, both online and offline, requires the collection and processing of certain user information. Requiring specific user consent for any data collection or processing would be inconsistent with consumer expectations, introduce unnecessary friction resulting in the degradation of user experience, and likely overwhelm consumers, resulting in “consent fatigue” that would lessen the impact of the most important user controls.<sup>4</sup>

As drafted, SB 169’s written consent requirements would uniquely burden consumers and businesses alike without any obvious benefit to privacy interests. SB 169’s provision mandating disclosure of biometric information to individuals or their authorized representatives similarly fails the risk-return calculus. This provision omits any form of authentication, and could therefore put Marylanders at even greater risk. Moreover, by prohibiting the use of biometric information except when “strictly necessary”, and by simultaneously prohibiting different levels of products or services, SB 169 might result in Marylanders being denied innovative products in the marketplace.

## 3. Sufficient time is needed to allow covered entities to understand and comply with newly established requirements.

SB 169 fails to provide covered entities with a sufficient onramp to achieve compliance. A successful privacy framework should ensure that businesses have an appropriate and reasonable opportunity to clarify the measures that need to be taken to fully comply with new requirements. Recently enacted privacy laws in California, Colorado and Virginia included two-year delays in enforcement of those laws. CCIA recommends that any privacy legislation advanced in Maryland include a comparable lead time to allow covered entities to come into

---

<sup>3</sup> A study commissioned by the California Attorney General estimated that in-state companies faced \$55 billion in initial compliance costs for meeting new privacy requirements, with small businesses facing disproportionately higher shares of costs. Berkeley Economic Advising and Research, LLC, “Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations,” (August, 2019), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

<sup>4</sup> See Article 29 Data Protection Working Party, WP 259, *Guidelines on Consent Under Regulation 2016/679*, 17 (Apr. 10, 2018), (“In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.”), <https://ec.europa.eu/newsroom/article29/items/623051>.



compliance and would therefore recommend amending the current October 1, 2023 effective date included in SB 169 to a later date.

#### **4. Investing enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.**

SB 169 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Maryland’s courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state. Further, every state that has established a comprehensive consumer data privacy law – California, Colorado, Connecticut, Utah and Virginia – has opted to invest enforcement authority with their respective state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA recommends that the legislation include a cure period of at least 30 days. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government’s limited resources on enforcing the law’s provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential privacy changes rather than shifting focus to defending against litigation.

\* \* \* \* \*

We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender  
State Policy Director  
Computer & Communications Industry Association

**MD SB 169 biometrics\_final PDF.pdf**

Uploaded by: margaret durkin

Position: UNF



**TECHNET**  
THE VOICE OF THE  
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622  
www.technet.org | @TechNetMidAtla1

February 7, 2023

The Honorable Melony Griffith  
Miller Senate Office Building, 3 East Wing  
11 Bladen Street, Annapolis, MD 21401

**RE: SB 169 Biometric Data Privacy**

Dear Chair Griffith and Members of the Committee,

On behalf of TechNet's member companies, I respectfully submit this letter of opposition to SB 169. TechNet's members place a high priority on consumer privacy; however, as drafted, this bill would create significant hardships for Maryland employers and could 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 over five 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 has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, and Washington, D.C.*

TechNet members recognize the importance of consumer privacy and the sensitivity of biometric data that can identify individuals. TechNet believes that privacy laws should provide strong safeguards for consumers, while allowing companies to innovate, provide security, and create jobs. Consumer trust is a top priority for our members, and that includes transparency on methods used to collect and use personal data. As currently drafted, this bill presents several problems for Maryland employers, consumers, and innovation.

## **Data Security**

Biometrics has a critical role to play in the security and anti-fraud space, as it represents a generational improvement over “knowledge-based” security questions that are easily-answered – favorite foods, colors of first cars, etc. To ensure consumers retain cutting-edge protection, it is critical that laws regulating biometric privacy have an unqualified security and fraud exemption. Modern opt-in consent statutes in Washington, Virginia, and Colorado all recognize the crucial need for robust fraud and security exemptions. Unfortunately, the bill as drafted does not allow businesses that provide anti-fraud services to operate in a way that protects consumers. Using data to prevent and identify fraud, and protect consumers, should not be subject to this bill’s requirements.

## **Processor Limitations and Consent**

TechNet agrees with the spirit of the bill to limit processor uses of data through the contract with the private entity. However, a processor will not know, nor have the means to know, whether the private entity obtained the biometric information lawfully or with consent. For services and products where individuals are acutely aware of the biometric component, this creates unnecessary friction without further protecting consumer privacy.

## **Disclosing Biometric Data Without Confirmation**

The bill still requires the disclosure of actual biometric information, without even confirming that the individual, or the “authorized representative”, are who they say they are. This puts consumer information in danger of criminals and allows criminals to cover their tracks. No other privacy law requires the disclosure of biometric data.

## **Private Right of Action**

TechNet opposes the inclusion of a private right of action because any unintentional or perceived violation could result in damaging liability for companies. The inclusion of a PRA for statutory damages would create massive class action litigation exposure for any alleged violations of the law by commercial entities, significantly deterring uses of biometric data including for anti-fraud, authentication, and other security purposes that benefit consumers. Studies have also revealed that private rights of action fail to compensate consumers even when a violation has been shown.



Well-meaning businesses, small and large, could be subject to frivolous lawsuits with little or no actual value delivered to the consumer. In turn, some businesses may choose to stop doing business in Maryland or be forced to cease operations altogether. The State Attorney General should have exclusive authority over any perceived violations. Every biometrics and omnibus privacy statute enacted, aside from the troublesome Illinois Biometric Information Privacy Act (BIPA), has relied on this exclusive authority.

TechNet joins industry partners and strongly encourages Maryland to look to the protections for consumers included in the Virginia, Colorado, and Connecticut omnibus privacy laws – protections that are, in fact, stronger than those that exist in the California privacy regime – that still require opt-in consent from the consumer but reflect a more modern and widely-accepted approach. We also urge you to consider that every single omnibus privacy bill enacted across the country to date includes biometrics protections. We believe it makes sense to consider how biometrics best fits into a larger consumer privacy conversation to further protect Maryland residents and businesses.

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 time and we look forward to continuing these discussions with you.

*Margaret Durkin*

Margaret Durkin  
Executive Director, Pennsylvania & the Mid-Atlantic  
TechNet  
[mdurkin@technet.org](mailto:mdurkin@technet.org)

# **MD 2023 NAMIC letter SB169 Biometric data privacy.**

Uploaded by: Matt Overturf

Position: UNF

**FINANCE COMMITTEE**

**MARYLAND SB 169: Commercial Law—Consumer Protection—Biometric Data Privacy**

**UNFAVORABLE**

**February 8, 2023**

Chairwoman Griffith and Members of the Senate Finance Committee:

On behalf of the National Association of Mutual Insurance Companies<sup>1</sup> (NAMIC) thank you for the opportunity to submit this statement in opposition to Senate Bill 169.

NAMIC consists of more than 1,500 member companies, including seven of the top 10 property/casualty insurers in the United States. The association supports local and regional mutual insurance companies on main streets across America as well as many of the country's largest national insurers.

The insurance industry takes consumer privacy very seriously and have been subject to numerous laws and regulations for years for the protection of consumer data. Our industry's commitment to appropriate use and safeguarding of consumer information has helped establish what has become a comprehensive federal and state regulatory framework governing the use and disclosure of personal information for the insurance industry.

**Exceptions for GLBA-Subject Financial Institutions**

When considering the broad privacy landscape, NAMIC encourages legislators to fully understand all the existing frameworks of laws and regulations currently in place, which can vary significantly from industry to industry. New provisions would not be enacted in a vacuum. This is especially true for insurance -- each state and the federal government already has robust laws/regulations to address data privacy, security, and other requirements. By recognizing that this is not a blank slate and to forestall confusion and conflicts, NAMIC advocates that new provisions are not a disconnected additional layer of obligations. To avoid unintended consequences, NAMIC encourages policy makers to recognize existing laws and regulations.

Given the vital business purposes for data in the insurance transaction, historically policy makers have recognized the important role information plays in insurance and, with certain protections in place, they have allowed collection, use, and disclose for operational and other reasons.

Title V of the Gramm-Leach-Bliley Act (GLBA)<sup>2</sup> provides a landmark privacy framework for financial services, including insurance. It sets forth notice requirements and standards for the disclosure of nonpublic personal

<sup>1</sup> NAMIC member companies write \$357 billion in annual premiums and represent 69 percent of homeowners, 56 percent of automobile, and 31 percent of the business insurance markets. Through its advocacy programs NAMIC promotes public policy solutions that benefit member companies and the policyholders they serve and fosters greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

<sup>2</sup> See 15 U.S.C. Sec. 6801 et. seq.



financial information – it specifically requires giving customers the opportunity to opt-out of certain disclosures. Under GLBA, functional financial institution regulators implemented the privacy standards. Given concerns with consistency, the National Association of Insurance Commissioners (NAIC) has adopted multiple model laws with regard to data privacy and cybersecurity<sup>3</sup>. And states have moved forward with adopting those models. For insurers, the Maryland Insurance Administration (MIA) regulates privacy matters (including consistent with Md. Code regs. 31.16.08.01 to 31.16.08.24) and provides robust oversight.

When it comes to retaining information, today insurers are already subject to specific record retention requirements. This information is important for several reasons. Insurers need to have information available for claims and litigation and insurance regulators rely on data for market conduct purposes. Again, insurance-related data is subject to numerous existing laws and regulations.

While NAMIC is pleased to see the inclusion of a GLBA exemption in SB 169, the exception should apply to both the data and entity subject to the GLBA as follows:

*Nothing in this Act shall be deemed to apply in any manner to data or to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal "Gramm-Leach-Bliley Act of 1999," 15 U.S.C. s.6801 et seq. and the rules and implementing regulations promulgated thereunder or to Maryland Insurance Code Ann. Sec. 2-109 and the rules and implementing regulations promulgated thereunder.*

Thank you for taking the time to consider our position on Senate Bill 169.

Sincerely,

A handwritten signature in black ink that reads "Matthew Overturf".

Matthew Overturf, Regional Vice President  
Mid-Atlantic Region

<sup>3</sup>See NAIC Model Laws [668](#), [670](#), [672](#), [673](#)

# **SB169-CTIA-UNF**

Uploaded by: Rob Garagiola

Position: UNF



**Testimony of  
JAKE LESTOCK  
CTIA**

**In Opposition to Maryland SB 169**

**Before the Maryland Senate Finance Committee**

**February 8, 2023**

Chair, Vice-Chair, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to SB 169. This bill places businesses under a strong threat of litigation and is not reflective of the current online ecosystem.

SB 169 is modeled after a biometric privacy law in Illinois, enacted in 2008, which has led to myriad lawsuits and little consumer protection. Maryland should not replicate this problematic law. The private right of action contained in SB 169 would subject companies to the risk of expensive litigation that primarily benefits the plaintiffs' bar and offers little relief to consumers. This has shown true in Illinois, where at the end of 2019, nearly 300 lawsuits were filed regarding their law – almost four times the total for 2018, the previous high watermark. Through September of 2021, according to a search of court filings, plaintiffs' lawyers have filed over 900 cases alleging violations under the BIPA law in Illinois.<sup>1</sup>

---

<sup>1</sup> <https://institutelegalreform.com/research/ilr-briefly-a-bad-match-illinois-and-the-biometric-information-privacy-act/>



These lawsuits have targeted businesses both large and small for alleged technical violations linked to collecting, using, and sharing biometric identifiers, like those indicated in SB 169. Rather than protecting consumers, however, these lawsuits have stifled beneficial uses of biometric data, and this legislation would do the same.

Furthermore, the written consent requirement does not reflect the current online ecosystem and is unworkable from a practical sense. This bill would have the negative effect of precluding protection for some consumers such as disabled populations, the elderly, and others, as they would be disadvantaged because they would be unable to use their voice to consent to services that protect themselves and others from cyber threats. This could also impact the use of voice recognition services such as those used in automobiles that help avoid distracted driving.

The right to access biometric information contained in the bill could also expose Maryland consumers to security risks, particularly by allowing a consumer's representative to make a request on her behalf. This creates the risk that biometric identifiers and other sensitive information could land in the hands of bad actors posing as consumers exercising their rights under the law or victims of domestic abuse.

Moreover, for over 20 years, the Federal Trade Commission has developed and enforced an effective privacy framework that applies to all players in the internet ecosystem. The FTC is an active consumer privacy enforcer. It has brought over 500 enforcement actions protecting consumer privacy. Through these enforcement actions, as well as through



extensive policy guidance, the FTC has articulated a consumer privacy framework in which more sensitive personal information including biometric or genetic information, is generally subject to heightened protections, while there is greater flexibility to collect, use, and disclose non-sensitive information. In addition, the Maryland Attorney General already has the authority to address unfair or deceptive acts or practices relating to consumer privacy under state consumer protection laws. Because of these existing federal and state measures, and other privacy laws, biometric data is already protected.

This bill raises complex issues and replicating an outdated and litigious statute, which was passed over a decade ago and has not been enacted in any other state, is not a path that Maryland should follow. As stated, passage of this legislation would expose consumers to new privacy and security risks and open up businesses to the threat of litigation, which would act as a damper on innovation, ultimately harming consumers in Maryland. Accordingly, CTIA respectfully requests that you not move this legislation. Thank you for your consideration.



# **PhRMA - SB 169 - Biometrics - Proposed Amemdments.**

Uploaded by: Josh White

Position: INFO

## Amendments to Biometrics - Maryland SB 169 / HB 033

The requirements of the Maryland SB 169 /HB 033 could jeopardize companies' ability to conduct clinical trials and biomedical research in Maryland. SB 169 /HB 033 would require private entities to delete all biometric data within 1 year of the entity's last interaction with an individual, or when the initial purpose for their collection has been satisfied, or within 30 days of receiving a request to delete an individual's biometric data, whichever is sooner. The current definition of "biometric data" may include information that is used in clinical trials or other biomedical research. The requirement to delete this information—by a specific deadline or upon request—may conflict with researchers' legal obligations to maintain and report information collected for biomedical research. For this reason, we are seeking the proposed amendments that would exclude entities conducting biomedical research in accordance with recognized research standards, exclude information that is collected or used for research in accordance with certain federally or internationally recognized research standards from the definition of "biometric data," and include a definition for "research."

In addition, we are seeking an amendment to define research, as defined under the federal Health Insurance Portability and Accountability Act (HIPAA), that would expressly clarify that research includes clinical trials but also includes critical observational research outside of a clinical setting which can reflect diverse patients in real world practice settings. This type of research can lead to more efficient drug development programs, provide more robust information about the benefits and risks of new medicines, and can ultimately lead to quicker access to innovative, safe, and effective medicines for patients. This type of research also may help to understand how treatments work in a broader patient population – such as those who may not be able to participate in trials because of comorbidities or because they live far from a clinical trial site.

Research involving human subjects already applies to recognized and accepted research standards that incorporate ethics and privacy principles, including an informed consent process. Providing an exemption for entities conducting biomedical research will help to avoid any unintended consequences that may impede the development of critical therapies and medicines by recognizing that biomedical research, conducted in accordance with existing ethical frameworks, already safeguards individuals' decision-making with regard to their information, including biometric data.

### PROPOSED AMENDMENTS

#### **Add to 14-4501(E)(2):**

(V) AN ENTITY, OR AN AFFILIATE OF AN ENTITY, CONDUCTING RESEARCH IN COMPLIANCE WITH THE FEDERAL POLICY FOR THE PROTECTION OF HUMAN SUBJECTS, 45 C.F.R. PART 46, THE GOOD CLINICAL PRACTICE GUIDELINES ISSUED BY THE INTERNATIONAL COUNCIL FOR HARMONISATION, OR THE UNITED STATES FOOD AND DRUG ADMINISTRATION PROTECTION OF HUMAN SUBJECTS UNDER 21 C.F.R. PARTS 50 AND 56.

#### **Add to 14-4501 as new (G):**

"RESEARCH" MEANS A SYSTEMATIC INVESTIGATION, INCLUDING RESEARCH DEVELOPMENT, TESTING, AND EVALUATION, DESIGNED TO DEVELOP OR CONTRIBUTE TO GENERALIZABLE KNOWLEDGE.

#### **Add to 14-4501(B)(2):**

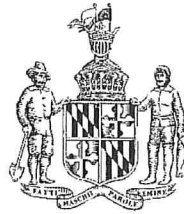
(IV) INFORMATION, HUMAN BIOLOGICAL SAMPLES, IMAGES, OR FILMS COLLECTED, USED, OR DISCLOSED IN THE CONTEXT OF RESEARCH CONDUCTED IN ACCORDANCE WITH THE FEDERAL POLICY FOR THE PROTECTION OF HUMAN SUBJECTS, 45 C.F.R. PART 46, THE GOOD CLINICAL PRACTICE GUIDELINES ISSUED BY THE INTERNATIONAL COUNCIL FOR HARMONISATION, OR THE UNITED STATES FOOD AND DRUG ADMINISTRATION PROTECTION OF HUMAN SUBJECTS UNDER 21 C.F.R. PARTS 50 AND 56.

# **Robert L. Dean Testimony.pdf**

Uploaded by: Robert Dean

Position: INFO

AISHA N. BRAVEBOY  
STATE'S ATTORNEY



JASON B. ABBOTT  
PRINCIPAL DEPUTY STATE'S ATTORNEY

State's Attorney for Prince George's County  
14735 Main Street, Suite M3403  
Upper Marlboro, Maryland 20772  
301-952-3500

February 8, 2023

Informational Testimony

**SB 169 – Commercial Law – Consumer Protection – Biometric Data Privacy**

---

Dear Chairman Griffith and Members of the Committee:

This submission is to provide information on Senate Bill 169 and its impact. This is provided on behalf of Aisha Braveboy, States Attorney for Prince George's County, and the Maryland State's Attorney's Association. I am Robert Dean, Special Assistant State's Attorney for Prince George's County, assigned to work with the Cold Case Homicide Unit of the Prince George's County Police Department.

Our concern is the effect that the effect of SB169 may have on important law enforcement activity should it become law as is – specifically the effect on the forensic genetic genealogical investigative process. We urge you to consider ways to accomplish your purpose in protecting biometric data privacy yet at the same time preserving Maryland's ability to utilize the forensic genetic genealogy investigative process, which has become an essential tool in solving cold cases of homicide and sex offenses. As the bill stands now, it is flawed, but we believe it can be fixed.

One and a half years ago, our office was awarded a \$470,000 grant from the Department of Justice to support the investigation of unsolved homicides and sex offenses using forensic genetic genealogy. Working with the police crime lab, we have identified at least 640 cases of unsolved homicides and sex offenses in Prince George's County where forensic genetic genealogy investigation may be useful. (This process is also valuable in identifying human remains.) We currently have 15 active cases utilizing the forensic genetic genealogy process and we anticipate increasing that number up to about 20 by the end of this year.

In 2021, the General Assembly enacted a comprehensive regulatory scheme covering some of this field in *Title 17 of the Criminal Procedure Code*. This comprehensive effort, the only one in the nation so far, governs in considerable detail how investigations utilizing forensic genetic genealogy are to proceed.

Title 17 establishes regulatory criteria, including judicial oversight of the investigative process, and rules governing the composition of the data bases available to law enforcement for this investigative purpose. There are rules requiring confidentiality and destruction protocols, as well as the establishment of regulatory criteria for those involved in the process.

Without getting into all the details of the Title 17 requirements, our unit must follow the requirements of Title 17, as well as the *Department of Justice Interim Guidelines on Forensic Genetic Genealogy (2019)*. We currently have obtained judicial approval to proceed in approximately 15 cases that occurred from 1972 to 2006.

An initial step in developing leads for investigative purposes is to submit biological samples from the crime scene that are likely to originate from the offender. This sample must have already been submitted to the national CODIS data base to see if there is a match from samples of known offenders that have already been provided into the data base.

Once it is determined that there is no match, the Forensic Genetic Genealogy process involves sending the biological sample of a purported unidentified offender to a private laboratory that performs a SNP extraction (Single Nucleotide Polymorphism), which is then uploaded into a database of DNA samples that have been voluntarily submitted by consumers to determine their ancestry. The donors to this data base have consciously opted into the database and agreed that their DNA sample could be made available to law enforcement.

Based upon the SNP upload of the suspect sample, a distant relative of the possible suspect may be identified based upon a calculation of familial DNA characteristics. At this point, a genealogist will construct a family tree based upon open-source information.

This process can be very time consuming. But it may provide leads for investigators to follow. In building the family tree, persons of interest may be revealed. Any leads that arise through this process will, of course, need further investigation based on the specifics of the crime being investigated.

Our concern with SB 169 (as well as cross-filed HB 33) is that those private entities that develop the SNPs and those that maintain the essential databases of DNA profiles voluntarily submitted will likely avoid accepting Maryland cases because of the potential reach of this bill.

A reading of the bill as it defines and regulates biometric data by private entities, and the destruction protocols imposed, as well as the cause of action it affords individuals has the very real potential of ending the forensic genetic genealogy investigative process in Maryland.

This is not an unlikely result. I have spoken to representatives of Othram and BODE technologies who have expressed concern over the potential negative impacts this legislation may have.

In light of the already existing regulatory scheme of *Criminal Procedure Title 17*, and the chilling effect that SB 169 would have to the availability of this crime solving technique in Maryland, we urge this committee to consider amending this proposed legislation to exclude from the coverage of this bill those entities that have laboratories developing the appropriate

DNA profiles necessary in the forensic genetic genealogy process, as well as those entities that maintain those data bases essential to the forensic genetic genealogy process.

Title 17 section 17-101 (c) and (g) provides a statutory definition for those entities that provide the services necessary to the forensic genetic genealogy process. The operative definitions are: (c) Direct to Consumer genetic genealogy services; and (g) publicly available open-data personal genomics database.

Therefore, we urge that these two types of private entities be excluded from the definition of private entities for purposes of SB 169 found in 14-4501 (E) (2) of SB 169. In addition to this amendment, the purpose clause should be amended to explain that nothing in this law should affect the investigative processes regulated in *Title 17 of the Criminal Procedure Article*.

I will be happy to answer any questions.

**Robert Dean**  
Special Assistant State's Attorney  
Prince George's County  
[rldean@co.pg.md.us](mailto:rldean@co.pg.md.us)

**FPF Written Tetsimony - MD HB33 .docx.pdf**

Uploaded by: Tatiana Rice

Position: INFO

## **FPF Written/Verbal Testimony for 2/8/23 Hearing**

Good Afternoon,

My name is Tatiana Rice, and I serve as Senior Counsel at the Future of Privacy Forum, a non-profit dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.

In the absence of comprehensive privacy legislation, I appreciate this legislature's efforts to establish new rights and protections for consumers biometric information. Today, I'm here to recommend to this Committee the three following points should it consider advancing this legislation:

- 1. The carve-out for physical and digital photographs, and video or audio recording should be limited to identification**

As currently drafted, the definition of "biometric data" which "does not include a physical or digital photograph, or a video or audio recording" may unintentionally create loopholes for technologies that pose the highest privacy risks. For example, when developing a facial recognition system, photos of individuals are used to train the system by extracting certain unique features and vectors from the photograph and associating them with a known identity in a database. If the raw sources of data used to create biometric systems such as photos are excluded, it is possible an entity could escape liability due to this carve-out. Instead, the legislature should consider adopting the language used in the Connecticut Data Privacy Act, which excludes these sources, and any data generated therefrom, **unless it is used to identify a specific individual.**

- 2. Consumer rights of access and deletion should be verifiable and required of all processing entities.**

SB 169 Section 14-4505 and Section 14-4502(A)(1)(III) provides consumers with important rights of access and deletion. If passed, this would be the first time a specific biometric data privacy bill in the US provides these rights to consumers, it also highlights the need to ensure these provisions are carefully drafted. While these rights are important, it is equally important to ensure that businesses are not required to process fraudulent requests from bad actors that could also risk consumers' information. As written, the "right to deletion" provision does not specify what a "verified" request means, it also does not instruct any service providers or third-parties to which a business may be using for its software to also delete the data, and it does not require notice to the individual if there is reason to believe someone is fraudulently attempting to access or delete their biometric data. Comprehensive data privacy laws that provide consumer privacy rights such as the California Privacy Protection Act (CCPA) can provide a useful framework, where the California AG specified in their implementing regulations that a "verifiable consumer request" could be determined by matching identifying information provided by the consumer to the personal information already maintained by the business.



### **3. Lastly, the Bill should make the Fraud and Security exemptions consistent**

Decades of research has demonstrated that biometric authentication is one of the most important security measures for many companies to prevent against fraud. It is used, for example, to secure access to buildings or databases, or confirm the identity of a known consumer before providing access to financial information. Fingerprinting, is also a common requirement for employee background checks pursuant to state or federal laws.

Unlike other biometric data privacy laws in the US, this bill provides compliance exemptions for biometric data used for fraud prevention or security purposes as it relates to consent and deletion requirements. Section 14-4504 exempts entities from getting individual consent to process biometric information if it is required by federal, state, or local law, or if it used for fraud prevention or security purposes (so long as there is still conspicuous notice). However, Section 14-4502 only exempts entities from complying with deletion requests if the individual is “part of the state voluntary exclusion program” which appears to be a program for individuals who wish to ban themselves from Maryland casinos. As a result, if any non-casino entity received a verifiable deletion request, they must delete the data which would terminate the entity’s ability to continue using the biometric authentication system for that individual. The entity, therefore, must choose between recommended security practices or compliance by federal or state law, or compliance with this Act, even if they were initially able to collect the individual information without consent. Given that the bill’s consent fraud exemptions are broader than the fraud exemptions for deletion, the legislature may consider better aligning these provisions for consistency of compliance.

Should the legislature have any additional questions or seek additional information, I would be more than happy to assist in whatever way I can.



**Tatiana Rice**

Senior Counsel for U.S. Legislation and Biometrics

[trice@fpf.org](mailto:trice@fpf.org) | [www.fpf.org](http://www.fpf.org)

[1350 Eye Street NW, Suite 350](#)

[Washington, DC 20005](#)