SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

AB 1814 (Ting)
Version: June 12, 2024
Hearing Date: July 2, 2024
Fiscal: No
Urgency: No
CK

SUBJECT

Law enforcement agencies: facial recognition technology

DIGEST

This bill prohibits a finding of probable cause or justification for a warrant based solely on a facial recognition technology (FRT) match.

EXECUTIVE SUMMARY

FRT identifies or confirms a person's identity using their facial features in an image or video. It can automate face detection by running an image against digital photos from various sources, including public and private databases. The technology has been growing in use, especially among law enforcement, where supporters tout its ability to facilitate solving crimes and identifying perpetrators.

However, much of this use is largely unregulated. And there are growing concerns about its invasive approach and inaccuracies in identifying people of color. More alarming are concerns that use by law enforcement will begin to automate their discretion and undermine the constitutional rights of Californians. Many call for an outright ban to what is considered a dangerous and socially corrosive technology. Others believe that at the very least there needs to be strong safeguards put in place to mitigate the more problematic implications of integrating this technology into law enforcement.

Instead, this bill simply provides that an FRT match cannot form the sole basis for probable cause for an arrest or search, or the sole basis for issuing a warrant. It further encourages officers to "examine results with care" and to "consider the possibility that matches could be inaccurate."

The bill is author-sponsored. It is supported by various groups, including the California Police Chiefs Association and the Protection of the Educational Rights of Kids

Advocacy. It is opposed by dozens of organizations, including the University of California, Irvine Faculty Association, the National Immigration Law Center, and Black Lives Matter California. This bill passed out of the Senate Public Safety Committee on a 5 to 0 vote.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Provides, pursuant to the Unruh Civil Rights Act, that all persons within the jurisdiction of this state are free and equal, and no matter what their sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status are entitled to the full and equal accommodations, advantages, facilities, privileges, or services in all business establishments of every kind whatsoever. (Civ. Code § 51.)

3) Provides, pursuant to the Tom Bane Civil Rights Act, a cause of action for intentional interference with a person's civil rights through violence, coercion, or intimidation. (Civ. Code § 52.1.)

4) Provides that no person in the State of California shall, on the basis of sex, race, color, religion, ancestry, national origin, ethnic group identification, age, mental disability, physical disability, medical condition, genetic information, marital status, or sexual orientation, be unlawfully denied full and equal access to the benefits of, or be unlawfully subjected to discrimination under, any program or activity that is conducted, operated, or administered by the state or by any state agency, is funded directly by the state, or receives any financial assistance from the state. (Gov. Code §§ 11135 et. seq.)

5) Defines "false imprisonment" as the unlawful violation of the personal liberty of another. (Pen. Code § 236.)

6) Excludes from government immunity provisions false arrest or false imprisonment. (Gov. Code § 820.4.)

7) Declares that it is the intent of the Legislature to establish policies and procedures to address issues related to the downloading and storage of data recorded by a body-worn camera worn by a peace officer; these policies and procedures shall be based on best practices. (Pen. Code § 832.18(a).)

8) Encourages agencies to consider best practices in developing policies related to the use of body-worn cameras and the storage of the data obtained from these cameras. (Pen. Code § 832.18.)

9) Instructs law enforcement agencies to work with legal counsel to determine a retention schedule to ensure that storage policies and practices are in compliance with all relevant laws and adequately preserve evidentiary chains of custody. (Pen. Code § 832.18(b)(5)(D).)

This bill:

1) Prohibits a law enforcement agency or peace officer from using an FRT match as the sole basis for probable cause for an arrest or search.

2) Prohibits a judge from granting an application for a warrant based solely on an FRT match.

3) Requires a peace officer using information obtained from the use of FRT to examine results with care and consider the possibility that matches could be inaccurate.

4) Defines the following terms:
   a) "Facial recognition technology" or "FRT" means a system that compares a probe image of an unidentified human face against a reference photograph database, and, based on biometric data, generates possible matches to aid in identifying the person in the probe image.
   b) "Probe image" means an image of a person that is searched against a database of known, identified persons or an unsolved photograph file.
   c) "Reference photograph database" means a database populated with photographs of individuals that have been identified, including databases composed of driver's licenses or other documents made or issued by or under the authority of the state, a political subdivision thereof, any other state, or a federal agency, databases operated by third parties, and arrest photograph databases. This paragraph shall not be deemed to abrogate the provisions of Section 12800.7 of the Vehicle Code or any other provision of law limiting the use of databases populated with photographs of individuals.

5) Provides that a violation constitutes false arrest for which damages of up to $25,000 may be awarded to an individual who is subjected to the false arrest. A court shall award reasonable attorney's fees to a prevailing party. All other remedies available under other applicable laws continue to be available.

6) Provides that a "false arrest" occurs when an individual is detained, arrested, or otherwise placed in custody without legal justification.

COMMENTS

1. Concerns with use of facial recognition technology

In recent years, there have been growing concerns about how biometric surveillance, and particularly FRT, has been deployed. FRT is being used in our electronic devices and smart home products. However, the widespread collection of data through this technology is troubling. A study found that there is more than a 50 percent chance that any adult is already included in a law enforcement facial recognition database.[1] A researcher at the Center for a New American Security has described the privacy concerns with such ubiquitous and powerful technology:

> If you just walk down the street in Boston, in New York, in London, you are going to be recorded by many security cameras. Some of them [in] the possession of the local police force, most of them in possession of private companies who just have a security camera. So in society, we have really gotten used to the idea of being photographed constantly. What's new in facial recognition technology is that we're losing the anonymity that used to be associated with being recorded. So it's not just that you walk past a 7-Eleven, and the security camera notes that you're there. There's the possibility that the 7-Eleven will know that you specifically, as an individual, are there, and they know how many times you have passed by in the past few weeks. That's what's really changing in recent years is the ability to analyze this data and correlate it and draw insights from it. It really does raise a whole host of new privacy concerns.[2]

The use of FRT by private businesses has also exploded in recent years:

> Facial-recognition software, which has been in development since the 1960s and has been gaining popularity with police for more than a decade, has taken off with retailers and event spaces during the last couple of years, consultants say. It's marketed to them as an unparalleled tool for cutting down on shoplifting, and sold to the public as a security tool — helping identify would-be terrorists at sports games, for instance, or protecting consumers against identity theft by

[1] Shannon Van Sant, S*an Francisco Approves Ban On Government's Use Of Facial Recognition Technology* (May 14, 2019) NPR, https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology. All internet citations are current as of June 24, 2024.

[2] Peter O'Dowd, *As Facial Recognition Technology Booms, So Do Privacy Concerns* (Dec. 21, 2018) WBUR, https://www.wbur.org/hereandnow/2018/12/21/facial-recognition-privacy-concerns.

> making sure that they are who they say they are. It's also almost completely unregulated.[3]

In addition to the troubling privacy concerns posed by the technology, there has been research showing that the technology frequently results in misidentification, especially with persons with darker skin tones. A test of the technology highlighted accuracy concerns when matched with federal lawmakers:

> The errors emerged as part of a larger test in which the [ACLU] used Amazon's facial software to compare the photos of all federal lawmakers against a database of 25,000 publicly available mug shots. In the test, the Amazon technology incorrectly matched 28 members of Congress with people who had been arrested, amounting to a 5 percent error rate among legislators.
>
> The test disproportionally misidentified African-American and Latino members of Congress as the people in mug shots.[4]

A similar test was conducted with members of the California Legislature, resulting in 1 in 5 legislators being erroneously matched to a person who had been arrested when their pictures were screened against a database of 25,000 publicly available booking photos.[5]

One recent research study has supported these concerns, finding that FRT "can worsen racial inequities in policing" and that "law enforcement agencies that use automated facial recognition disproportionately arrest Black people."[6] The research asserts that this can result from "factors that include the lack of Black faces in the algorithms' training data sets, a belief that these programs are infallible and a tendency of officers' own biases to magnify these issues." The researchers conclude:

> Amid the growing staffing shortages facing police nationwide, some champion FRT as a much-needed police coverage amplifier that helps

[3] Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores* (Oct. 20, 2018) New York Magazine, http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html.

[4] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says* (Jul. 26, 2018) New York Times, https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

[5] Anita Chabria, *Facial recognition software mistook 1 in 5 California lawmakers for criminals, says ACLU* (August 13, 2019) Los Angeles Times, https://www.latimes.com/california/story/2019-08-12/facial-recognition-software-mistook-1-in-5-california-lawmakers-for-criminals-says-aclu.

[6] Thaddeus L. Johnson & Natasha N. Johnson, *Police Facial Recognition Technology Can't Tell Black People Apart* (May 18, 2023) Scientific American, https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/; Thaddeus L. Johnson, *Facial recognition systems in policing and racial disparities in arrests*, Government Information Quarterly, Volume 39, Issue 4, 2022, https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892?via%3Dihub.

> agencies do more with fewer officers. Such sentiments likely explain why more than one quarter of local and state police forces and almost half of federal law enforcement agencies regularly access facial recognition systems, despite their faults.
>
> This widespread adoption poses a grave threat to our constitutional right against unlawful searches and seizures.

2. FRT

According to the author:

> I authored AB 1215 in 2019 which banned the use of biometric surveillance through police body cameras. The bill only passed with a three year moratorium that expired January 1, 2023. Consequently, current law has absolutely no parameters set regarding law enforcement's use of facial recognition technology. It is critical that we ensure there are safeguards in place in order to avoid another year of unregulated use. California can't go another year with no protections. AB 1814 is a modest step to setting safeguards in California law by prohibiting law enforcement agencies and peace officers from using facial recognition technology as the sole basis for probable cause for an arrest, search, or affidavit for a warrant. Most importantly, this bill does not prohibit nor deter local governments from choosing to ban the use of facial recognition technology.

This bill provides that an FRT match shall not serve as the sole basis for probable cause for a search or seizure, or the sole basis for issuance of a warrant. However, the Constitution likely already requires as much, as in most cases an FRT match likely does not support a finding of probable cause on its own.[7] In fact, stakeholders have argued that the bill merely codifies the use of FRT by law enforcement rather than provide any meaningful guardrails. A coalition in opposition, including the Western Center on Law and Policy and the California Immigrant Policy Center, write:

> Rather than ensuring that face surveillance cannot be used to threaten the lives, rights, and safety of Californians, AB 1814 proposes a woefully inadequate band-aid that emboldens police to expand dangerous face recognition and just writes into law the same failed rules that have already played a role in the wrongful arrests of innocent people—particularly

[7] In most cases of FRT misidentification, law enforcement use the FRT match to create a photo lineup that is already influenced by the faulty FRT match. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm* (June 24 2020) The New York Times, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

> Black men. If AB 1814 is passed, it would effectively greenlight a surveillance technology that is racist, unreliable, and anti-democratic.

A recent opinion piece in the Sacramento Bee calls attention to this issue:

> To date, we know of seven wrongful arrests in the United States caused by incorrect face recognition results — and those are only the cases that have become public. In six out of the seven cases, the wrongfully accused individuals were Black, a figure that corresponds to numerous studies showing that facial recognition technology misidentifies Black people and other people of color at higher rates than white people. This is due, in part, to biases in the photo databases used to train the algorithms.
>
> Despite these failures, however, police departments across the state and the country are increasingly using facial recognition technology to try to match pictures of suspects with driver's license photos, mugshots and images from other databases.
>
> A technology this biased and error-prone should not be used by the police. Unfortunately, California has responded with Assembly Bill 1814, authored by Phil Ting, D-San Francisco. The bill is a misguided attempt to regulate — rather than prohibit — police use of facial recognition by merely declaring that officers shouldn't rely on this technology as the sole basis to obtain an arrest warrant. While this might sound sensible, it will not stop wrongful arrests. In fact, bills like AB 1814 will make the problem worse.
>
> Even a short time in jail can turn a person's life upside down. Wrongful arrests caused by facial recognition have set people back thousands of dollars, costing them their job and their home and inflicting lasting psychological and emotional harm on their families.[8]

Writing in support, the California Police Chiefs Association points out the benefits of the technology:

> Across the country, real-world examples of law enforcement using FRT to solve major crimes showcases just how important this new technology can be towards protecting our communities. In North America alone, FRT has been used in 40,000 human trafficking cases, helping rescue 15,000 children and identify 17,000 traffickers. In Detroit, law enforcement was successful in identifying a gunman who targeted and murdered three

[8] Nate Freed Wessler, *Why aren't California lawmakers banning police from using facial recognition technology?* (April 25, 2024) Sacramento Bee.

> LGBTQ victims. In 2018, another gunman who killed five employees at a newspaper headquarters in Maryland was identified using FRT. And in New York, FRT was used to identify a perpetrator within 24-hrs of kidnapping and raping a young woman; and in a separate instance, a suspected subway bomber was identified through FRT.
>
> As California looks to host the 2026 World Cup and the 2028 Winter Olympics in Los Angeles, we must ensure our agencies have all the best possible tools necessary – including FRT – to defend against threats to the safety of the public at these worldwide events.

However, such successes are weighed against tragic outcomes of false FRT matches, primarily impacting communities of color. There are myriad examples, including Porcha Woodruff:

> Porcha Woodruff was getting her two daughters ready for school when six police officers showed up at her door in Detroit. They asked her to step outside because she was under arrest for robbery and carjacking.
>
> "Are you kidding?" she recalled saying to the officers. Ms. Woodruff, 32, said she gestured at her stomach to indicate how ill-equipped she was to commit such a crime: She was eight months pregnant.
>
> Handcuffed in front of her home on a Thursday morning last February, leaving her crying children with her fiancé, Ms. Woodruff was taken to the Detroit Detention Center. She said she was held for 11 hours, questioned about a crime she said she had no knowledge of, and had her iPhone seized to be searched for evidence.
>
> "I was having contractions in the holding cell. My back was sending me sharp pains. I was having spasms. I think I was probably having a panic attack," said Ms. Woodruff, a licensed aesthetician and nursing school student. "I was hurting, sitting on those concrete benches."
>
> After being charged in court with robbery and carjacking, Ms. Woodruff was released that evening on a $100,000 personal bond. In an interview, she said she went straight to the hospital where she was diagnosed with dehydration and given two bags of intravenous fluids. A month later, the Wayne County prosecutor dismissed the case against her.
>
> The ordeal started with an automated facial recognition search, according to an investigator's report from the Detroit Police Department. Ms. Woodruff is the sixth person to report being falsely accused of a crime as a result of facial recognition technology used by police to match an

> unknown offender's face to a photo in a database. All six people have been Black; Ms. Woodruff is the first woman to report it happening to her.
>
> It is the third case involving the Detroit Police Department, which runs, on average, 125 facial recognition searches a year, almost entirely on Black men, according to weekly reports about the technology's use provided by the police to Detroit's Board of Police Commissioners, a civilian oversight group. Critics of the technology say the cases expose its weaknesses and the dangers posed to innocent people.[9]

The particulars of this case make the danger clear – that such technology will likely exacerbate racial bias issues in policing. However, this bill does not require any reporting or that logs be kept, so identifying patterns in the deployment of FRT will be nearly impossible. This prompts concerns that there should be some form of transparency in law enforcement use and that at the very least there should be internal logging of FRT use or reporting to an entity with oversight. Bolstering the need for such provisions is a recent report from the Los Angeles Times detailing FRT use, and denial, by the Los Angeles Police Department:

> The Los Angeles Police Department has used facial recognition software nearly 30,000 times since 2009, with hundreds of officers running images of suspects from surveillance cameras and other sources against a massive database of mug shots taken by law enforcement.
>
> The new figures, released to The Times, reveal for the first time how commonly facial recognition is used in the department, which for years has provided vague and contradictory information about how and whether it uses the technology.
>
> The LAPD has consistently denied having records related to facial recognition, and at times denied using the technology at all.
> . . .
> LAPD Assistant Chief Horace Frank said "it is no secret" that the LAPD uses facial recognition, that he personally testified to that fact before the Police Commission a couple years ago, and that the more recent denials — including two since last year, one to The Times — were just mistakes.
>
> "We aren't trying to hide anything," he said.
>
> Civil liberties advocates disagree. They said the recent denials — only corrected after The Times questioned their accuracy — are part of a long

[9] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match* (August 6, 2023) The New York Times, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

> pattern of deception in which the LAPD has systematically avoided discussing facial recognition by denying it has records related to the technology or by claiming, erroneously, that it doesn't use it.
>
> As such technology improves and becomes more pervasive, transparency around the government's use of it becomes all the more important — and the LAPD's actions all the more concerning — given the potential for privacy and civil rights infringements, advocates say.[10]

The author may wish to consider whether some sort of transparency measures should be added before codifying the ability of law enforcement to use FRT. At the very least, any codification of FRT use by law enforcement should require that a suspect searched, detained, or arrested based on an FRT match be notified that FRT was used, otherwise there is little chance they would even now that a violation of this bill has occurred.

FRT is defined to mean a system that compares a probe image of an unidentified human face against a reference photograph database, and, based on biometric data, generates possible matches to aid in identifying the person in the probe image.

Concerns have been raised with the bill's definition of "reference photograph database," which means a "database populated with photographs of individuals that have been identified." This is an extremely broad definition. It provides examples, which include not only arrest photograph databases but also any databases operated by third parties. This means that law enforcement could run a photo against private databases like those compiled by Clearview AI, which boasts having a database of over 50 billion facial images, with more on the way:

> The facial recognition company Clearview AI is telling investors it is on track to have 100 billion facial photos in its database within a year, enough to ensure "almost everyone in the world will be identifiable," according to a financial presentation from December obtained by The Washington Post.
>
> Those images — equivalent to 14 photos for each of the 7 billion people on Earth — would help power a surveillance system that has been used for arrests and criminal investigations by thousands of law enforcement and government agencies around the world.
>
> And the company wants to expand beyond scanning faces for the police, saying in the presentation that it could monitor "gig economy" workers and is researching a number of new technologies that could identify

[10] Kevin Rector & Richard Winton, *Despite past denials, LAPD has used facial recognition software 30,000 times in last decade, records show* (September 21, 2020) Los Angeles Times, https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software.

> someone based on how they walk, detect their location from a photo or scan their fingerprints from afar.[11]

A lawsuit against Clearview AI, filed by two immigrants' rights groups in California, Mijente and NorCal Resist, sought to stop the company's surveillance technology from proliferating in the state.[12] The complaint alleged that the company's software is still used by state and federal law enforcement to identify individuals despite the various official bans. The suit alleges Clearview AI's database of images violates the privacy rights of people in California broadly and that the company's "mass surveillance technology disproportionately harms immigrants and communities of color." The tactics used to amass the company's massive stockpile have also drawn widespread backlash and legal action:

> Clearview has built its database by taking images from social networks and other online sources without the consent of the websites or the people who were photographed. Facebook, Google, Twitter and YouTube have demanded the company stop taking photos from their sites and delete any that were previously taken. Clearview has argued its data collection is protected by the First Amendment.
>
> Facebook, which forbids the automated copying, or "scraping," of data from its platform and has an External Data Misuse team, has banned Clearview's founder, Hoan Ton-That, from its site and has sent the company a cease-and-desist order, but Clearview has refused to provide any information about the extent to which Facebook and Instagram users' photos remain in Clearview's database, an official with Facebook's parent company, Meta, told The Post. The official declined to comment on any steps Meta may be considering in response.
>
> Clearview's cavalier approach to data harvesting has alarmed privacy advocates, its peers in the facial recognition industry and some members of Congress, who this month urged federal agencies to stop working with the company, because its "technology could eliminate public anonymity in the United States." Sens. Ron Wyden (D-Ore.) and Rand Paul (R-Ky.) last year introduced a bill that would block public money from going to Clearview on the basis that its data was "illegitimately obtained."
>
> Clearview is battling a wave of legal action in state and federal courts, including lawsuits in California, Illinois, New York, Vermont and

[11] Drew Harwell, *Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement* (February 16, 2022) The Washington Post, https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

[12] Rachel Metz, *Clearview AI sued in California by immigrant rights groups, activists* (March 9, 2021) CNN, https://www.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html.

> Virginia. New Jersey's attorney general has ordered police not to use it. In Sweden, authorities fined a local police agency for using it last year. The company is also facing a class-action suit in a Canadian federal court, government investigations in Canada, Sweden and the United Kingdom and complaints from privacy groups alleging data protection violations in France, Greece, Italy and the U.K.
>
> The governments of Australia and France have ordered Clearview to delete their citizens' data, with Australia saying the company had covertly monetized people's faces for a purpose "outside reasonable expectations." "The indiscriminate scraping of people's facial images, only a fraction of whom would ever be connected with law enforcement investigations, may adversely impact the personal freedoms of all Australians who perceive themselves to be under surveillance," Australia's information and privacy commissioner, Angelene Falk, said in November.[13]

The author may wish to consider whether amendments limiting the scope of databases used by law enforcement to run FRT to only specified law enforcement databases is warranted and whether the bill should require FRT searches to be run by law enforcement themselves.

A number of jurisdictions have already responded to the risks by severely restricting the use of FRT by law enforcement and other government entities. Multiple California cities have already banned its use outright. San Francisco has banned its use by police and government agencies.[14] Oakland followed suit, and according to the then Oakland City Council President, "the ban was instituted on the basis that facial recognition is often inaccurate, lacks established ethical standards, is invasive in nature, and has a high potential for government abuse."[15] Alameda also banned the use of such systems in 2019, asserting "its potential abuse could undermine civil liberties and the technology was unreliable."[16] Berkeley's city council banned its use by its police department and other public agencies.[17]

[13] *Ibid.*

[14] Sarah Emerson, *San Francisco Bans Facial Recognition Use by Police and the Government* (May 14, 2019) Vice, https://www.vice.com/en/article/wjvxxb/san-francisco-bans-facial-recognition-use-by-police-and-the-government.

[15] Caroline Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition* (July 17, 2019) Vice, https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

[16] Peter Hegarty, *East Bay police used facial recognition technology despite ban* (April 9, 2021) East Bay Times, https://www.eastbaytimes.com/2021/04/09/east-bay-police-used-facial-recognition-technology-despite-ban/.

[17] Levi Sumagaysay, *Berkeley bans facial recognition* (October, 16, 2019) The Mercury News, https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.

At the federal level, multiple pieces of legislation have been aimed at reining in the use of FRT in law enforcement. In March of last year, a bill imposing a moratorium was introduced by a coalition of Senators and Representatives:

> Senators Edward J. Markey (D-Mass.), Jeff Merkley (D-Ore.), Bernie Sanders (I-Vt.), Elizabeth Warren (D-Mass.), and Ron Wyden (D-Ore.) and Representatives Pramila Jayapal (WA-07), Ayanna Pressley (MA-07), Rashida Tlaib (MI-12), Earl Blumenauer (OR-03), Cori Bush (MO-01), Greg Casar (TX-35), Adriano Espaillat (NY-13), Barbara Lee (CA-12), Eleanor Holmes Norton (DC), Jamaal Bowman (NY-16), and Jan Schakowsky (IL-09) today reintroduced the *Facial Recognition and Biometric Technology Moratorium Act*, legislation to prevent the government from using facial recognition and other biometric technologies, which pose significant privacy and civil liberties issues and disproportionately harm marginalized communities. The legislation responds to reports that hundreds of local, state and federal agencies, including law enforcement, have expanded their use of facial recognition technologies while multiple Black men have been wrongfully arrested based on a false facial recognition match, including a recent case in Maryland. Research shows nearly half of U.S. adults' faces exist in facial recognition databases and that the faces of Black, Brown, and Asian individuals are up to 100 times more likely to be misidentified than white male faces.
>
> "The year is 2023, but we are living through 1984. The continued proliferation of surveillance tools like facial recognition technologies in our society is deeply disturbing," said Senator Markey. "Biometric data collection poses serious risks of privacy invasion and discrimination, and Americans know they should not have to forgo personal privacy for safety. As we work to make our country more equitable, we cannot ignore the technologies that stand in the way of progress and perpetuate injustice."[18]

In addition, last October, Congressman Ted Lieu, and others, introduced the *Facial Recognition Act*, which "places strong limits on law enforcement use of FRT, provides transparency, and requires annual assessments and reporting on the deployment of the technology to protect individuals' rights. Specifically, the bill requires that a warrant be obtained that shows probable cause an individual committed a serious violent felony **before** FRT is deployed."[19]

[18] Press release, *Markey, Merkley, Jayapal Lead Colleagues on Legislation to Ban Government Use of Facial Recognition and other Biometric Technology* (March 7, 2023) website of Senator Ed Markey, https://www.markey.senate.gov/news/press-releases/markey-merkley-jayapal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology.

[19] Press release, *Reps Lieu, Jackson Lee, Clarke, Gomez, Ivey, and Veasey Introduce Bill to Regulate Law Enforcement's Use of Facial Recognition Technology* (October 27, 2023) website of Congressman Ted Lieu,

However, even when banned, law enforcement agencies have attempted to get around the laws. As reported in the Washington Post:

> As cities and states push to restrict the use of facial recognition technologies, some police departments have quietly found a way to keep using the controversial tools: asking for help from other law enforcement agencies that still have access.
>
> Officers in Austin and San Francisco — two of the largest cities where police are banned from using the technology — have repeatedly asked police in neighboring towns to run photos of criminal suspects through their facial recognition programs, according to a Washington Post review of police documents.
>
> . . .
>
> SFPD spokesman Evan Sernoffsky said these requests violated the city ordinance and were not authorized by the department, but the agency faced no consequences from the city. He declined to say whether any officers were disciplined because those would be personnel matters.[20]

This emphasizes the importance of enforcement. This bill provides that a violation constitutes "false arrest" for which damages of up to $25,000 may be awarded to an individual who is subjected to the false arrest. First, without proper oversight and auditing, it is difficult to determine whether an FRT match alone was the basis for a search or arrest. Second, the bill provides that the match cannot form the "sole basis" for probable cause for a search or arrest. It is unclear how much more is required. For instance, an FRT match plus a minor similarity between the matched individual and a description could be enough. Finally, while the bill makes a violation a "false arrest," it goes on to define "false arrest" to mean when an individual is detained, arrested, or otherwise placed in custody without legal justification. It is unclear how the two provisions interact; is a violation enough to meet this definition? The author may wish to clarify the enforcement mechanism.

An opposition letter submitted by dozens of organizations, including Chispa and Black Lives Matter California, highlights concerns with the enforcement:

> Rather than recognizing and addressing the widely understood harms of face surveillance, AB 1814 does nothing to prevent law enforcement from using face surveillance to identify and track people across the state. Further, even the limited restriction this bill imposes to not use face

https://lieu.house.gov/media-center/press-releases/reps-lieu-jackson-lee-clarke-gomez-ivey-and-veasey-introduce-bill.

[20] Douglas MacMillan, *These cities bar facial recognition tech. Police still found ways to access it.* (May 18, 2024) The Washington Post, https://www.washingtonpost.com/business/2024/05/18/facial-recognition-law-enforcement-austin-san-francisco/.

> recognition as the sole basis for probable cause is itself unworkable and difficult to enforce. There is no way for people to find out if facial recognition is used against them and no mechanism to make sure the police comply with the law.

3. <u>Additional stakeholder positions</u>

The City of Visalia explains its support:

> Facial recognition technology is one of many tools utilized in identifying an individual by comparing a digital image of the person's face to a database of known faces, typically by measuring distinct facial features and characteristics. This technology does not, by itself, result in ultimate identification, but it may generate investigative leads necessary for combatting crime within our communities. Technology assists our law enforcement partners in doing their jobs more efficiently and ultimately improves public safety.
>
> The City of Visalia supports accountability on the part of law enforcement agencies concerning police surveillance technology and policies, as well as related oversight by local governing bodies. However, we do not support policies that restrict law enforcement agencies from utilizing technologies that would otherwise enhance their ability to prevent criminal activity in the communities they serve.

A large coalition in opposition, include ACLU California Action and the Asian Law Alliance, writes:

> Face recognition use by law enforcement is among the most invasive surveillance technology that exists. It is already well-understood how this dangerous surveillance technology has been improperly used to wrongfully accuse people of crimes, target immigrants, intimidate activists, and can also threaten the safety of people seeking reproductive rights and gender-affirming care.
>
> Face recognition supercharges the government's power to surveil people of color and other marginalized groups and threatens our rights to privacy and free expression. We cannot freely organize, seek reproductive health care, or attend a place of worship if we fear that our faces, who we are, where we go, and what we do can be recorded by the police.
>
> The fact that face recognition is simply too dangerous and corrosive to our rights and safety to be used by law enforcement is why companies like companies like Amazon, Microsoft, and IBM do not sell it to police. It is

> why 20 U.S. communities across the country have already banned the government's use of face recognition technology. It is why progressive leadership in the United States Congress recently introduced a bill that would prohibit government use of facial recognition and also conditions funding to localities on adopting similar prohibitions. The only responsible standard for face recognition is to prohibit its use by governments. Prohibitions on government use of facial recognition protect our civil rights, reduce dangerous encounters and wrongful detentions, and impede the creation of dangerous biometric databases that would further threaten already vulnerable communities in California.

SUPPORT

California Faculty Association
California Police Chiefs Association
City of Visalia
League of California Cities
Perk Advocacy

OPPOSITION

Access Reproductive Justice
Access Support Network
ACLU California Action
Advocacy for Principled Action in Government
All Family Legal
Alliance San Diego
American Atheists
Asian Americans Advancing Justice - Asian Law Caucus
Asian Law Alliance
Asian Solidarity Collective
Bienestar Human Services
Black Lives Matter California
Border Line Crisis Center
California Alliance for Youth and Community Justice
California Immigrant Policy Center
California Latinas for Reproductive Justice
Cancel the Contract Antelope Valley
Change Begins With Me (INDIVISIBLE)
Chispa
Consumer Federation of California
Council of University of California Faculty Associations
Council on American-Islamic Relations, California
Courage California

Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Encode Justice
Fight for the Future
Food Empowerment Project
Free Speech Coalition
Gender Justice LA
Gente Organizada
Health Care 4 Us
If When How; Lawyering for Reproductive Justice
Immigrant Defense Advocates
Indivisible CA Statestrong
Indivisible East Bay
Indivisible Yolo
LA Defensa
National Harm Reduction Coalition
National Immigration Law Center
Oakland Privacy
Orale: Organizing Rooted in Abolition, Liberation, and Empowerment
Orange County Equality Coalition
Organization for Identity and Cultural Development
Parivar Bay Area
Positive Women's Network - USA
Privacy Rights Clearinghouse
San Diego Faculty Association
San Francisco Black & Jewish Unity Coalition
Santa Monica Democratic Club
Secure Justice
Silicon Valley De-bug
Stop LAPD Spying Coalition
Students Deserve
Surveillance Technology Oversight Project (STOP)
Team Justice San Diego
TechEquity Action
Tech Workers Coalition, San Diego
The Sidewalk Project
The Translatin@ Coalition
Training in Early Abortion for Comprehensive Healthcare (TEACH)
UC Irvine Faculty Association
Universidad Popular
University of California Riverside Faculty Association
Western Center on Law and Poverty
Youth Justice Coalition
One individual

RELATED LEGISLATION

Pending Legislation:

AB 1034 (Wilson, 2023) prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. It authorizes a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition. AB 1034 is currently on the Senate Floor Inactive File.

AB 1463 (Lowenthal, 2023) requires operators and end-users of automated license plate recognition systems ("ALPR system") to conduct annual audits to review ALPR searches. If the operator or end-user is a public agency, it further requires them to destroy all ALPR information that does not match information on a hot list within 30 days. It places restrictions on accessing certain systems and sharing ALPR information. AB 1463 is currently in this Committee.

Prior Legislation:

AB 642 (Ting, 2023) would have prescribed the acceptable and prohibited uses for FRT, as defined, by a law enforcement agency or peace officer. It would have set certain requirements for FRT systems and reference databases, as defined, used by law enforcement agencies. AB 642 was held in the Assembly Appropriations Committee.

AB 1215 (Ting, Ch. 579, Stats. 2019) prohibited law enforcement from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other camera worn or carried.

PRIOR VOTES:

Senate Public Safety Committee (Ayes 5, Noes 0)
Assembly Floor (Ayes 70, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)
Assembly Public Safety Committee (Ayes 7, Noes 0)
****