Date of Hearing: April 30, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1814 (Ting) – As Amended February 28, 2024

AS PROPOSED TO BE AMENDED

SUBJECT: Law enforcement agencies: facial recognition technology

SYNOPSIS

Law enforcement agencies around the country have used facial recognition technology (FRT) for almost two decades. FRT refers to the use of artificial intelligence technology to identify or verify a person from a digital image by determining whether two images of faces represent the same person. Essentially, when looking for a match, a still photograph taken from a surveillance video is compared with a database of photographs of identified individuals. Generally, the FRT search will result in a number of individuals who may match the image. Unfortunately, like many other artificial intelligence tools, FRT has a bias problem.

Recent studies continue to highlight that many FRT systems are less effective at identifying people of color, women, older people, and children. These race, gender, and age biases arise because FRT is often "trained" using non-diverse faces. Essentially, if the original training data set primarily contains photographs of white men with very few women or people of color, then the tool will have a more difficult time correctly identifying women and people of color. As a result, police relying on the technology to identify people have wrongfully arrested Black men based on mistaken FRT identifications, known as "false positives." This bill is intended to modestly restrict the use of FRT by law enforcement agencies by enshrining in state law that FRT results alone are not sufficient for determining probable cause.

This bill is supported by the Police Chiefs Association of California, the League of California Cities, the Security Industry Association, and several other organizations. Secure Justice, ACLU California Action, Oakland Privacy, and Access to Reproductive Justice are a few of the approximately one dozen opponents.

Committee amendments clarify that a violation of the bill constitutes false arrest for which damages of up to $25,000 may be awarded.

This bill passed the Public Safety Committee on a 7-0-1 vote.

SUMMARY: Prohibits a law enforcement agency or peace officer from using a facial recognition technology (FRT) match as the sole basis for an arrest, search or as an affidavit for a warrant. Specifically, **this bill**:

1) Prohibits the use of an FRT match as the sole basis for an arrest, search or as an affidavit for a warrant.

2) Requires a peace officer obtaining FRT matches to carefully examine the results and consider the possibility that FRT matches can be inaccurate.

3) Establishes that a violation of this section constitutes false arrest, as defined in Penal Code Section 236, and allows damages of up to $25,000 and reasonable attorney's fees to an individual who is subjected to such a false arrest.

4) Defines "facial recognition technology" 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.

5) Defines "probe image" to mean an image of a person that is searched against a database of known, identified persons or an unsolved photograph file.

6) Defines "reference photograph database" to mean a database populated with photographs of individuals that have been identified, including:

   a) Driver's licenses photographs or other documents made and issued by federal, state, or local governments.

   b) Databases operated by third parties.

   c) Arrest photograph databases.

7) Specifies that the definition of a "reference photograph database" does not abrogate the provisions in Vehicle Code section 12800.7, which specifies that certain documents used to prove identity are not public records, or any other law limiting the use of databases populated with photographs of individuals.

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. (Civil 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).)

10) Instructs a law enforcement agency using a third-party vendor to manage its data storage system to consider the following factors to protect the security and integrity of the data: Using an experienced and reputable third-party vendor; entering into contracts that govern the vendor relationship and protect the agency's data; using a system that has a built-in audit trail to prevent data tampering and unauthorized access; using a system that has a reliable method for automatically backing up data for storage; consulting with internal legal counsel to ensure the method of data storage meets legal requirements for chain-of-custody concerns; and using a system that includes technical assistance capabilities. (Pen. Code § 832.18(b)(7).)

FISCAL EFFECT: As currently in print, this bill is keyed non-fiscal.

COMMENTS:

1) **Research demonstrates significant problems with FRT and its ability to accurately identify people.** FRT refers to the use of artificial intelligence technology to identify or verify a person from a digital image by determining whether two images of faces represent the same person. Essentially, when looking for a match, a still photograph taken from a surveillance video is compared with a database of photographs of identified individuals. Generally, the FRT search will result in a number of individuals who may match the image.

FRT technology remains far from perfect. Recent studies continue to highlight that many FRT systems are less effective at identifying people of color, women, older people, and children. These race, gender, and age biases arise because FRT is often "trained" using non-diverse faces. Essentially, if the original training data set primarily contains photographs of white men with very few women or people of color, then the tool will have a more difficult time correctly identifying women and people of color. As a result, police relying on the technology to identify people have wrongfully arrested Black men based on mistaken FRT identifications, known as "false positives."

Numerous studies reveal the FRT performance inconsistencies in identifying non-white males and people with darker complexions, generally. The National Institute of Standards and

Technology (NIST) conducted the most prominent of these global studies. Their 2019 analysis of 189 facial recognition software programs found that people of color were up to 100 times more likely to be wrongfully identified than white men.[1] Clare Garvie, an expert in law enforcement use of FRT, notes that these NIST tests are performed in a controlled environment using clear images. They are not performed in the real world, where police routinely conduct searches using real world images–which are frequently blurry and/or distant–producing bad results that are even more likely to be mismatched by FRT.[2] Not only does FRT have a racial bias problem, research shows that it also has a gender problem. One study, conducted by Colorado University at Boulder, found that with a brief glance, facial recognition software can categorize gender with remarkable accuracy. But if that face belongs to a transgender person, such systems get it wrong more than one-third of the time. In addition, earlier studies suggest software tends to be most accurate when assessing the gender of white men but misidentify women of color as much as one-third of the time.

According to the study's lead author, Morgan Klaus Scheuerman, "We found that facial analysis services performed consistently worse on transgender individuals, and were universally unable to classify non-binary genders. While there are many different types of people out there, these systems have an extremely limited view of what gender looks like."

The Colorado study suggests that FRT systems identify gender based on outdated stereotypes. When Scheuerman, a male with long hair, submitted his picture, half categorized him as female. "These systems run the risk of reinforcing stereotypes of what you should look like if you want to be recognized as a man or a woman," said Scheuerman. "That impacts everyone."[3]

The inaccuracy, biases, and potential privacy intrusions inherent in many facial recognition systems used by law enforcement have led to criticism from civil rights advocates, especially in California. In March 2020, the ACLU, on behalf of a group of California residents, filed a class action lawsuit against Clearview AI, claiming that the company illegally collected biometric data from social media and other websites, and applied facial recognition software to the databases for sale to law enforcement and other companies.[4] An investigation by Buzzfeed in 2021 found that 140 state and local law enforcement agencies in California had used or tried Clearview AI's system.[5]

In a clear example of the flaws in the technology, in late 2023, Rite Aid settled a complaint brought by the Federal Trade Commission (FTC) that charged the drugstore chain with using FRT systems to identify shoppers that were deemed "likely to engage" in shoplifting and continually misidentified people, particularly women, and Black, Latino, or Asian people. The

---

[1] Johnson, et al. "Facial recognition systems in policing and racial disparities in arrests," *Government Information Quarterly* 39 (2022) 101753, Elsevier, https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892.
[2] Garvie. "Garbage In, Garbage Out: Face Recognition on Flawed Data," *Georgetown Law Center on Privacy and Technology*, (May 16, 2019) https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/.
[3] *Facial recognition software has a gender problem*, National Science Foundation (Nov. 1, 2019) https://new.nsf.gov/news/facial-recognition-software-has-gender-problem.
[4] *Clearview AI class-action may further test CCPA's private right of action*, JD Supra (Mar. 12, 2020), https://www.jdsupra.com/legalnews/clearview-ai-class-action-may-further-14597/.
[5] *Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here.* Buzzfeed News (Apr. 6, 2021). https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table.

complaint states that Rite Aid used facial recognition technology in hundreds of stores from October 2012 to July 2020 to identify the shoppers it had previously identified as likely to engage in criminal behavior and then the technology sent alerts to Rite Aid employees when it identified those people entering the store. The complaint goes on to explain that store employees would put those people under increased surveillance, ban them from making purchases, or accuse them in front of friends, family, and other customers of having previously committed crimes. The FRT systems were largely used in New York City; Los Angeles; San Francisco; Philadelphia; Baltimore; Detroit; Atlantic City; Seattle; Portland, Oregon; Wilmington, Delaware and Sacramento, California, according to the settlement.[6]

2) **Law enforcement uses of facial recognition systems.** Law enforcement agencies around the country have used FRT for almost two decades. The Security Industry Association, whose members include the leading providers of facial recognition software used by law enforcement, explain in their letter of support for this bill:

> In U.S. law enforcement, facial recognition technology is typically used in the beginning stages of a criminal investigation, when there is a lawfully obtained image of an unknown person of interest whose identification could help solve a crime. This is a post-incident investigative tool to aid identification – not "surveillance." The function is to generate or follow leads only, not to confirm an identity. Photos are compared against an available database of images using facial recognition software, which returns all potential match candidates with high similarity scores. Personnel then determine whether any of the returns represent leads that should be investigated further. At that point, other investigative techniques outside of facial comparison are used to find and confirm further information needed to positively identify a person and, if a suspect, information needed to establish probable cause to make an arrest or obtain a search warrant.

In September 2021, the *Los Angeles Times* reported that the Los Angeles Police Department had used facial recognition software nearly 30,000 times since 2009, despite years of "vague and contradictory information" from the department "about how and whether it uses the technology." According to the *Times*, "The LAPD has consistently denied having records related to facial recognition, and at times denied using the technology at all." Responding to the report, the LAPD claimed that the denials were just mistakes, and that it was no secret that the department used such technology. Although the department could not determine how many leads from the system developed into arrests, it asserted that "the technology helped identify suspects in gang crimes where witnesses were too fearful to come forward and in crimes where no witnesses existed."[7]

In 2023, Porcha Woodruff became the sixth known case overall and the first case of a woman being falsely arrested because of the results of an FRT search. According to the reporting on Ms. Woodruff's arrest, she was over eight months pregnant when she was arrested for robbery and carjacking. In February 2023, she was arrested in front of her home, handcuffed, taken to the Detroit jail, held for 11 hours, questioned about a crime she said she had no knowledge of, and

---

[6] *Federal Trade Commission v. Rite Aid Corporation.* Case 2:23-cv-05023, US District Court for the Easter District of Pennsylvania (Dec. 19, 2023)
[7] "Despite past denials, LAPD has used facial recognition software 30,000 times in last decade, records show," *Los Angeles Times,* (Sept. 21, 2020) https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software.

had her iPhone seized to be searched for evidence. Once released on a $100,000 bond, Ms. Woodruff was taken to the hospital where she was treated for dehydration. One month later all the charges against her were dropped.[8] According to Ms. Woodruff, since her arrest she has suffered from anxiety, depression and extreme stress. In August 2023, she filed a lawsuit against the city of Detroit and a detective in the U.S. District Court for the Eastern District of Michigan alleging false arrest, false imprisonment and a violation of her Fourth Amendment rights to be protected from unreasonable seizures.[9]

Closer to home, the seventh known case of a wrongful arrest due to facial recognition in the U.S. and the first case involving a white man, in January 2022, involves Harvey Eugene Murphy Jr., who was living in Sacramento, California, when a Sunglass Hut in Houston, Texas was robbed. When Mr. Murphy returned to Texas from California, he went to the department of motor vehicles to renew his license. According to news reports, within minutes of identifying himself, an officer approached him to notify him that there was a warrant out for his arrest for aggravated robbery. Despite being in Sacramento at the time of the robbery, 61 year old Mr. Murphy was arrested and held in local jails for nearly two weeks. According to the suit filed by Mr. Murphy in October 2023, while being held in jail he was beaten and raped.[10]

The controversy surrounding law enforcement use of facial recognition has led many California cities to ban the technology, including San Francisco, Oakland, Berkeley, Santa Cruz and Alameda. Despite the ban in San Francisco, officers there may have skirted the city's ban by outsourcing an FRT search to another law enforcement agency.[11]

Similar to the provisions in this bill, a number of cities have adopted similar ordinances and evidence suggests that they are not effective. For example, according to New York Police Department policy and in the guidelines provided by the developers of the technology, FRT is not supposed to be used as the sole basis for arresting someone. On the contrary, the results it produces instead are intended to assist in an investigation and require taking additional investigative steps. According to a 2023 *New York Times* investigation:

> Law enforcement officers generally say they do not need to mention the use of facial recognition technology because it is only a lead in a case and not the sole reason for someone's arrest, protecting it from exposure as if it were a confidential informant. But according to Clare Garvie, an expert on the police use of facial recognition, there are four other publicly known cases [beyond the case discussed in the article] of wrongful arrests that appear to have involved little investigation beyond a face match, all involving Black men.

---

[8] Hill. "Eight Months Pregnant and Arrested After False Facial Recognition Match," *The New York Times* (Aug. 6, 2023) https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.
[9] Cho. "Woman sues Detroit after facial recognition mistakes her for crime suspect," *The Washington Post* (Aug. 7, 2023) https://www.washingtonpost.com/nation/2023/08/07/michigan-porcha-woodruff-arrest-facial-recognition/.
[10] Bhuiyan. "Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit," *The Guardian* (Jan. 22, 2024) https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit.
[11] Cassidy "Facial recognition tech used to build SFPD gun case, despite city ban," *San Francisco Chronicle* (Sept. 24, 2020), https://www.sfchronicle.com/bayarea/article/Facial-recognition-tech-used-to-build-SFPD-gun-15595796.php.

> She has come across a handful of other examples across the country, she said, in her work with the National Association of Criminal Defense Lawyers.[12]

In another *New York Times* article related to the first known false arrest of a Black man based only on the use of faulty FRT, the facial recognition results explicitly instructed, in all bolded capital letters, "THIS DOCUMENT IS NOT A POSITIVE IDENTIFICATION. IT IS AN INVESTIGATIVE LEAD ONLY AND IS NOT PROBABLE CAUSE TO ARREST. FURTHER INVESTIGATION IS NEEDED TO DEVELOP PROBABLE CAUSE TO ARREST." That man, Robert Williams, was arrested and held in jail, apparently solely on the bases of the FRT results, for a burglary at a store he had not been in since 2014 and that he had an alibi for.[13] Mr. Williams testified in this Committee last spring about his experience and the impact it has had on his life. His statement is included in its entirety in the Committee analysis of AB 642 (Ting, 2023).

3) **Author's statement.** 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.

4) **Committee amendments.** Given the impact on people who are falsely arrested based on FRT results, the amendments agreed to by the author add a penalty for misuse of the technology. The amendments are as follows:

> ***(d) (1) A violation of this section constitutes false arrest, as defined in Section 236, for which damages of up to $25,000 may be awarded to an individual who is subjected to such a false arrest.***
> ***(2) A court shall award reasonable attorney's fees to a prevailing plaintiff under this subdivision.***
> ***(3) This subdivision does not preclude any other remedies available under other applicable laws.***

6) **Previous legislative efforts.** In 2019, the Legislature passed AB 1215 (Ting, Chap. 579, Stats. 2019), which banned the use of facial recognition technology and other biometric surveillance systems in connection with cameras worn or carried by law enforcement, including body-worn cameras (BWC), for the purpose of identifying individuals using biometric data. This ban covered both the direct use of biometric surveillance by a law enforcement officer or agency, as

---

[12] Hill and Mac "'Thousands of Dollars for Something I Didn't Do,'" *The New York Times* (Mar 30, 2023) https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

[13] Hill. "Wrongfully Accused by an Algorithm," *The New York Times* (Aug. 3, 2020) https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

well as a request or agreement by an officer or agency that another officer or agency, or a third party, use a biometric surveillance system on behalf of the requesting party. The ban also included narrow exceptions for processes that redact a recording prior to disclosure in order to protect the privacy of a subject, and the use of a mobile fingerprint-scanning device to identify someone without proof of identification during a lawful detention, as long as neither of these functions result in the retention of biometric data or surveillance information. AB 1215 included a sunset date of January 1, 2023.

SB 1038 (Bradford), of the 2021-2022 Legislative session, would have extended the ban on biometric surveillance and facial recognition systems in connection with cameras worn or carried by officers indefinitely. At its core, the question involved balancing the purported investigatory benefits of facial recognition technology against its demonstrated privacy risks, technical flaws and racial and gender biases. Senate Public Safety Committee staff did not identify or receive any evidence demonstrating that the ban on facial recognition technology used in connection with body worn cameras had significantly hampered law enforcement efforts in the two years since it became operative. SB 1038 failed passage in the Senate.

Last year, this Committee heard two bills related to law enforcement agencies' use of FRT: AB 642 (Ting, 2023) and AB 1034 (Wilson, 2023). Mr. Ting's bill intended to create a regulatory framework for the use of FRT and Ms. Wilson's bill proposed banning the use of the technology on images captured by body-worn cameras. The Committee's analysis of Ms. Wilson's bill appreciated the privacy protective and potentially lifesaving nature of prohibiting its use. The Committee analysis made the following observations:

> 1. *Allowing law enforcement to use FRT is contrary to the policy direction of the Legislature in recent years and likely violates the state's laws prohibiting discrimination on the basis of race and gender.* As noted previously in recent years, it has been a priority of the Legislature to end the racial violence and injustice that appears to be endemic in the criminal legal system as a whole, and specifically, in policing. By analyzing the results of FRT systems, experts continue to determine that there is a significant risk of a Black man being misidentified by FRT. Given the continued bias in the system, it is likely that allowing the use of FRT on any photographs, much less on images from a body-worn camera, will likely exacerbate biased policing, potentially with tragic outcomes. Therefore, the Committee finds that continuing the moratorium as the technology evolves is consistent with policymaking in this area.
>
> 2. The question before this Committee is whether or not [AB 1034 (Wilson)] furthers the Committee's policy priorities. First and foremost, protecting Californians' constitutional right to privacy. Along with that, the Committee is working to ensure that all Californians, and those coming from out of state, are protected from punitive and discriminatory draconian laws attacking the LGBTQ+ community and criminalizing people seeking abortion and gender affirming care. Another priority of the Committee is ensuring that the State's laws protect our immigrant neighbors from federal policies that make them vulnerable to being separated from their families, imprisoned, and ultimately returned to countries that many were often forced to flee from for their own safety. The answer to this question is "yes." Returning the moratorium on the use of FRT on these cameras and the data they generate provides the only guarantee that tools designed to increase police accountability are not turned in to tools of mass surveillance.

In contrast, the analysis of AB 642 (Ting) raised a number of concerns for this Committee—primarily that the technology is not accurate enough to safely use and establishing a regulatory framework that did not prohibit its use until it reached 100 percent accuracy created a significant risk. Among the issues raised in that analysis were the following:

> 1. *Significant bias remains in FRT systems, making their use dangerous.* While this issue was discussed in detail previously, it is worth repeating**.** NIST's 98% accuracy score does not account for racial bias. When looking at one algorithm that received a 99% accuracy rating from NIST, the false positive identification rate (FPIR) for Black men was more than 2x the FPR for white men, and for a couple of the thresholds, the disparity was more than 3x. Thus, NIST's own testing results indicate that an algorithm that may clear the standard in the bill may have a false positive rate for Black men 3x the false positive rate for white men.[14]
>
> In a 2020 study on facial recognition in body worn cameras, "the researcher conducted the study in conditions that were generally stable and controllable, yet matching performance error rates were as high as 100%." Notably, this conclusion is tied to two aspects of body cameras that aren't likely to change: the footage is the result of officers moving, and the footage is filmed with a wide angle, which skews faces. Importantly, as noted, the study was done in conditions that are unlikely to be the conditions officers encounter in the field where people are continually moving – including the officer.[15]
>
> 2. The question before this Committee was whether or not [AB 642 (Ting)] furthers the Committee's policy priorities. First and foremost, protecting Californians' constitutional right to privacy. Along with that, the Committee is working to ensure that all Californians, and those coming from out of state, are protected from punitive and discriminatory draconian laws attacking the LGBTQ+ community and criminalizing people seeking abortion and gender affirming care. A further priority of the Committee is ensuring that the State's laws protect our immigrant neighbors from federal policies that make them vulnerable to being separated from their families, imprisoned, and ultimately returned to countries that many were often forced to flee from for their own safety. The answer to this question when it comes to this bill is that in its current version it does not, but with further amendment, it is hoped that it will.
>
> As the author noted, law enforcement agencies are currently using FRT around the state without restriction or regulation. Given the faulty nature of the technology, Californians would likely be well served by robust regulation and strict limits on its use.
>
> However, the larger question before the Legislature this year remains, has the technology reached a stage where it can be used in a restricted manner to assist in law enforcement investigations? Based on the current research discussed previously, this is an open question.

AB 642 (Ting) was held on the Appropriation Committee's suspense file and AB 1034 (Wilson) is currently on the Senate's Inactive File and eligible to be brought up for a vote on the Senate Floor.

---

[14] Those test results that bear this out are available a https://pages.nist.gov/frvt/reports/demographics/annexes/annex_16.pdf.

[15] Bryan. *Effects of Movement on Biometric Facial Recognition in Body-Worn Cameras,* Purdue University, Department of Technology Leadership and Innovation (May 2020).

7) **Analysis.** As discussed, this issue is not a new one for this Committee and the same concerns remain. The author points to a previous ban on the use of FRT that expired at the end of December 2022 as part of the urgency behind this bill. However, that ban was only on one narrow use of the technology – its use in combination with body-worn or handheld cameras. The broader use of the technology by government and private entities is widespread and largely unrestricted. While the Committee staff continues to have serious reservations about the use of FRT, it is hoped that the bill, as proposed to be amended, provides significant incentive for law enforcement agencies to use FRT circumspectly in conjunction with other evidence sufficient to establish probable cause.

Going forward, the author is encouraged to consider adding a requirement that whenever the technology is used the law enforcement agency must provide a notice to the defendant identified in the search so that they can know FRT was used and that they have a right to seek damages if the police violate the provisions contained in this bill. As one of the opponents of the bill, ACLU California Action, rightly points out:

> AB 1814 does not require defendants be informed FRT played a role in their case. While *Brady* requirements should obligate law enforcement to inform defendants that FRT was used in their case, too often defendants are not informed or only informed by accident. In telling his story to members of the Legislature last year, for example, Mr. Williams related how it was only through a slip by one of the law enforcement officials interviewing him that he was given a clue that FRT may have been used in his case. (Footnote omitted.)

In addition, the author is encouraged to consider narrowing the definition of "reference photograph database" to only include mug shot databases. As currently written, the bill allows law enforcement to use probe images, e.g., an image from a closed circuit video, body-worn camera, dash camera, or any other surveillance camera, on virtually any database. Rather than being limited to running the photo through their mug shot database only, the FRT vendor can use any database, whether government-developed or one owned by a third party, e.g., Facebook, to search through hundreds of millions, if not billions, of images. This allows law enforcement to freely search the images of hundreds of millions of people without first obtaining a court order, warrant, or some other permission to do so.

On this particular point, the TechEquity Action warns in their opposition letter:

> AB 1814 newly exposes Californians, and specifically California drivers, to biometric surveillance. The bill defines "reference photo database" – the database of faces that facial recognition will search through – in a manner that explicitly includes "databases composed of driver's licenses," allowing police agencies to begin using drivers' license photos to build surveillance databases. Currently, California police are not authorized to mine driver's license photos for this kind of surveillance.
>
> Opening California's driver license photos for biometric surveillance will cause harm. The experience of other states shows that if California authorizes biometric surveillance of driver's license holders, a population that in California includes immigrants, Immigration and Customs Enforcement will demand access to that database to investigate and target those who are immigrants. Additionally, it will mean that every California driver will be placed in a perpetual virtual lineup. This has caused problems in other states, for example when police in Detroit relied on an FRT mismatch between Robert Williams' old driver license photo and the suspect, leading to a wrongful arrest.

> Recent amendments to AB 1814 do not prevent California drivers from having their California driver license photo added to facial recognition databases and subjected to invasive surveillance. The referenced Vehicle Code provision is an unrelated limit on the sharing of documents a person submits to prove their identity when seeking to obtain a license. This amendment does not prevent every California driver from being placed in a face surveillance database.

ARGUMENTS IN SUPPORT: Arguing in support of the bill, the California Police Chiefs Association argue for the importance of FRT:

> 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 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.

ARGUMENTS IN OPPOSITION: Echoing the concerns of other organizations opposed to the bill in print, the Electronic Frontier Foundation argues:

> This bill will not stop false face recognition matches that lead to arrests. In several of the known cases where face recognition led to wrongful arrests, police are already seeing warnings similar to those required by the bill. It is clear that warnings do not prevent law enforcement from pursuing people based on false face recognition matches.
>
> [. . . .]
>
> FRT is an inherently dangerous form of surveillance and there are no acceptable standards under which law enforcement can use face surveillance. Rather than aligning with the civil rights community and national consensus, AB 1814 grants law enforcement agencies authority to use face recognition technology to identify and track people across the state. It sets up ineffective guardrails and requires no accountability if law enforcement officials abuse it.

REGISTERED SUPPORT / OPPOSITION:

Support

California Faculty Association
California Police Chiefs Association
League of California Cities
National Police Accountability Project
Perk Advocacy
Security Industry Association

Opposition

Access Reproductive Justice
ACLU California Action
Asian Americans Advancing Justice - Asian Law Caucus
Council on American-islamic Relations, California
Electronic Frontier Foundation
Indivisible CA Statestrong
LA Defensa
National Action Network Orange County
Oakland Privacy
Resilience Orange County
Santa Monica Democratic Club
Secure Justice
Techequity Collaborative
The Partnership for The Advancement of New Americans

Oppose Unless Amended

California Public Defenders Association

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200