SENATE COMMITTEE ON PUBLIC SAFETY

Senator Aisha Wahab, Chair
2023 - 2024 Regular

Bill No:	AB 1814	**Hearing Date:**	June 11, 2024
Author:	Ting		
Version:	May 6, 2024		
Urgency:	No	**Fiscal:**	No
Consultant:	AB		

Subject: ***Law enforcement agencies: facial recognition technology***

HISTORY

Source: Author

Prior Legislation: AB 642 (Ting, 2023), held in Assembly Appropriations
AB 1034 (Wilson, 2023), currently on Senate Inactive File
AB 645 (Friedman, Ch. 808, Stats. of 2023)
SB 1038 (Bradford), died on Senate Inactive File
AB 1281 (Chau, Ch. 268, Stats. of 2020)
AB 2261 (Chau, 2020), held in Assembly Appropriations
AB 1215 (Ting, Ch. 579, Stats. of 2019)
SB 1186 (Hill, 2018), held in the Assembly Appropriations Committee
SB 21 (Hill, 2017), held in Assembly Appropriations Committee
AB 69 (Rodriguez, Ch. 461, Stats. of 2015)

Support: California Faculty Association; 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; Cancel the Contract Antelope Valley; Change Begins With Me (INDIVISIBLE); Chispa; Consumer Federation of California; Council of UC 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; Gente Organizada; If When How; Lawyering for Reproductive Justice; Indivisible CA Statestrong; Indivisible East Bay; Indivisible Yolo; LA Defensa; National Harm Reduction Coalition; Oakland Privacy; Orale: Organizing Rooted in Abolition, Liberation, and Empowerment; Orange County Equality Coalition; Organization for Identity and Cultural Development; 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; Tech Equity;

Tech Workers Coalition, San Diego; Techequity Collaborative; The Sidewalk Project; 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

Assembly Floor Vote: 70 - 0

As Proposed to Be Amended

PURPOSE

The purpose of this bill is to prohibit a facial recognition technology match from being used as the sole basis for an arrest or search conducted by police or as the sole basis for a warrant issued by a judge.

Existing law provides that the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (U.S. Const., 4th Amend.)

Existing law provides that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

Existing law requires the magistrate, before issuing an arrest warrant, to examine a declaration of probable cause made by a peace officer or, when the defendant is a peace officer, an employee of a public prosecutor's office of this state, as specified. (Pen. Code, § 817, subd. (a)(1).)

Existing law provides that a magistrate shall issue a warrant of probable cause for the arrest of the defendant only if the magistrate is satisfied after reviewing the declaration that there exists probable cause that the offense described in the declaration has been committed and that the defendant described therein has committed the offense. (Pen. Code, § 817, subd. (a)(1).)

Existing law requires that the declaration in support of the warrant of probable cause for arrest be a sworn statement made in writing, but that the magistrate may accept an oral statement made under penalty of perjury, as specified. (Pen. Code, § 817, subd. (b) & (c).)

Existing law defines a search warrant as an order in writing, in the name of the people, signed by a magistrate, directed to a peace officer, commanding him or her to search for a person or persons, a thing or things, or personal property, and, in the case of a thing or things or personal property, bring the same before the magistrate. (Pen. Code, § 1523.)

Existing law enumerates twenty distinct grounds upon which a judge may issue a search warrant. (Pen. Code, § 1524.)

Existing law prohibits cities and counties participating in the Speed Safety System Pilot Program from using facial recognition technology in conjunction with those systems. (Veh. Code, § 22425, subd. (l)(4).)

Existing law 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, subd. (a).)

Existing law encourages agencies to consider best practices in establishing when data should be downloaded to ensure the data is entered into the system in a timely manner, the cameras are properly maintained and ready for the next use, and for purposes of tagging and categorizing the data. (Pen. Code, § 832.18, subd. (b).)

Existing law encourages agencies to consider best practices in establishing specific measures to prevent data tampering, deleting, and copying, including prohibiting the unauthorized use, duplication, or distribution of body-worn camera data. (Pen. Code, § 832.18, subd. (b)(3).)

Existing law instructs a law enforcement agency using a third-party vendor to manage the 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, subd. (b)(7).)

Existing law encourages agencies to include in a policy a requirement that all recorded data from body-worn cameras are property of their respective law enforcement agency and shall not be accessed or released for any unauthorized purpose. Encourages a policy that explicitly prohibits agency personnel from accessing recorded data for personal use and from uploading recorded data onto public and social media Internet websites, and include sanctions for violations of this prohibition. (Pen. Code, § 832.18, subd. (b)(8).)

Existing law provides, pursuant to the California Consumer Privacy Act (CCPA), effective January 1, 2020, that a business that collects personal information must inform the consumer at or before the time of collection, the category and purpose of the personal information that is to be collected. (Civ. Code, § 1798.100, subd. (b).)

Existing law defines, for purposes of the CCPA, "biometric information" as including, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. (Civ. Code, § 1798.140, subd. (b).)

Existing law requires a person or business conducting business in California that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system under specified circumstances, and defines personal information to include unique biometric data includes physical or digital photographs used or stored for facial recognition purposes. (Civ. Code, § 1798.82, subd. (h)(1)(F))

This bill provides that a law enforcement agency shall not use a facial recognition technology (FRT) match as the sole basis for probable cause for an arrest or search.

This bill provides that a judge shall not grant an application for a warrant based solely on an FRT match.

This bill requires peace officer's using FRT information to examine the results with care and consider the possibility that matches could be inaccurate.

This bill sets forth the following definitions for terms used therein:

- "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.

- "Probe image" means an image of a person that is searched against a database of known, identified persons or an unsolved photograph file.

- "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.

This bill provides that a violation of the prohibition against law enforcement use of FRT as the sole basis for probable cause constitutes false arrest, for which damages of up to twenty-five thousand ($25,000) may be awarded to an individual who is subjected to the false arrested.

This bill provides that for the purposes of the above provision, a "false arrest" occurs when an individual is detained, arrested, or otherwise placed in custody without legal justification.

This bill requires a court to award reasonable attorney's fees to a prevailing plaintiff seeking remedy under the above provision.

This bill specifies that the penalty provision above does not preclude other remedies available under applicable laws.

COMMENTS

1. Need for This Bill

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.

2. Facial Recognition Technology

Facial recognition technology is capable of 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. Early versions of the technology were pioneered in the 1960s and 1970s, but true facial recognition technology as we understand it today did not come about until the early 1990s. In 1993, the United States military developed the Facial Recognition Technology (FERET) program, which aimed to create a database of faces and recognition algorithms to assist in intelligence gathering, security and law enforcement.[1] Since that time, advances in computer technology and machine learning have led to faster and more accurate recognition software, including real-time face detection in video footage and emotional recognition.

Today, facial recognition technology is used in a variety of applications. It is often a prominent feature in social media platforms, such as Facebook, Snapchat and TikTok. For instance, DeepFace, a "deep learning" facial recognition system created by Facebook, helps the platform identify photos of users so they can review or share the content.[2] Snapchat employs similar technology to allow users to share content augmented by "filters," which can add features or alter an image of the user's face. Facial recognition technology has also seen increasing use as a method of ID verification, such as with Apple's Face ID and Google's Android "Ice Cream Sandwich" systems.

As facial recognition technology has become more widespread, so have concerns about its shortcomings and potential for misuse. Many critics highlight that the use of facial recognition systems result in serious privacy violations, and that mechanisms to protect against the unwanted sale or dissemination of personal biometric data are insufficient.[3] Others suggest that the technology is still too inaccurate and unreliable to be used in such a broad array of applications. For instance, studies suggest that while facial recognition systems have had increasing success identifying cis-gendered individuals, these systems get it wrong more than one-third of the time if the face belongs to a transgender person.[4] However, even among cis-gendered individuals, research shows that facial recognition systems can be significantly less accurate when identifying women than when identifying men.[5] Additionally, a growing body of research demonstrates that

---

[1] "Facial Recognition Technology (FERET)." The National Institute of Standards and Technology, United States Department of Commerce. https://www.nist.gov/programs-projects/face-recognition-technology-feret

[2] Facebook has recently indicated that it would reduce its use of this technology, but its parent company, Meta, may continue to use it in other applications. See "Facebook is backing away from facial recognition. Meta isn't." 3 November 2021. https://www.vox.com/recode/22761598/facebook-facial-recognition-meta

[3] Schwartz, Adam. "Resisting the Menace of Face Recognition." *Electronic Frontier Foundation*. 26 October 2021. https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition

[4] "Facial Recognition Software Has a Gender Problem." *National Science Foundation*. 1 November 2019. https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=299486

[5] Buolamwini, Joy, et al. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." PMLR 81:77-91, 2018. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

facial recognition systems are significantly less accurate in identifying individuals with dark complexions, particularly women.[6]

3. Law Enforcement Uses of Facial Recognition Technology

Despite growing concerns, law enforcement agencies at the federal, state and local level continue to use facial recognition programs. A recent Government Accountability Office report revealed that 20 federal agencies employ such programs, 10 of which intend to expand them over the coming years.[7] Another recent study found that one in four law enforcement agencies across the country can access some form face recognition, and that half of American adults – more than 117 million people – are in a law enforcement face recognition network.[8] Very few of these agencies have a formal facial recognition policy, but one such agency, the New York Police Department, defines the scope of its policy as follows: "Facial recognition technology enhances the ability to investigate criminal activity and increases public safety. The facial recognition process does not by itself establish probable cause to arrest or obtain a search warrant, but it may generate investigative leads through a combination of automated biometric comparisons and human analysis."[9]

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.[10] 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.[11] 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.[12]

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

---

[6] Najibi, Alex. "Racial Discrimination in Face Recognition Technology." *Harvard University Graduate School of Arts and Sciences Blog.* 24 October 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

[7] "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks." *United States Government Accountability Office*. 3 June 2021. https://www.gao.gov/products/gao-21-518

[8] Garvie, Clare, et al. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *The Georgetown Law Center on Privacy and Technology*. 18 October 2016. https://www.perpetuallineup.org/

[9] "Facial Recognition Technology Patrol Guide." *City of New York Police Department.* Issued 12 March 2020. https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf

[10] "Clearview AI class-action may further test CCPA's private right of action." *JD Supra.* 12 March, 2020. https://www.jdsupra.com/legalnews/clearview-ai-class-action-may-further-14597/

[11] "Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here." *Buzzfeed News.* 6 April 2021. https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table

[12] "Facial recognition tech used to build SFPD gun case, despite city ban." S.F. Chronicle. 24 Sept. 2020 https://www.sfchronicle.com/bayarea/article/Facial-recognition-tech-used-to-build-SFPD-gun-15595796.php

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."[13]

Conversely, proponents of facial recognition technology see it as a useful tool in the law enforcement arsenal that has the ability, among other things, to help officials identify criminals. It was reportedly utilized to identify the man charged in the deadly shooting at The Capital Gazette's newsroom in Annapolis, Maryland in 2018.[14] Advocates of the technology in the law enforcement context also tout its ability to find missing people, act as a deterrent, and improve security in sensitive places, such as schools, banks and airports. They further argue that early deficiencies in the technology have been corrected - according to the Security Industry Association, which writes in support of the bill:

> Calls for restricting use of the technology have often stemmed from misconceptions regarding its performance. While there is evidence that some, especially older versions of facial recognition technology struggled to perform consistently across various demographic factors, the oft-repeated claim that it is inherently less accurate in matching faces of Black and female subjects is simply false, and based on information that is irrelevant, obsolete or nonscientific. […] Most of the leading facial recognition technologies are evaluated by the U.S. government's National Institute of Standards and Technology (NIST) on an ongoing basis. For over 20 years, the NIST Face Recognition Technology Evaluation (FRTE) Program has remained the world standard for objective, third-party scientific evaluation, providing an "apples to apples" comparison of the performance of facial recognition technologies.
>
> This U.S. government data, which is the most reliable information available, shows that a large number of leading technologies used in commercial and government applications today are well over 99% accurate overall and more than 97.5% accurate across more than 70 different demographic variables [and] s, the top 100 are over 99.5% accurate in matching images across Black male, white male, Black female and white female demographics.

4. Recent Facial Recognition Technology Legislation

In 2019, the Legislature passed Assembly Bill 1215 (Ting), Chapter 579, Statutes of 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. The ban covered both the direct use of biometric surveillance by a law enforcement officer or agency, as 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

---

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

[14] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, New York Times, July 26, 2018, Available at: https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html?login=facebook.

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 Legislature, would have extended the ban on biometric surveillance and facial recognition systems in connection with cameras worn or carried by officers indefinitely. However, SB 1038 failed on the Senate Floor, and ultimately died on the Senate inactive file. At the time that SB 1038 passed through this committee, committee staff had not identified nor received any evidence demonstrating that the ban on facial recognition technology used in connection with officer-worn cameras had significantly hampered law enforcement efforts in the two years since it had become operative.

Last year, the Legislature was asked once again to determine whether the investigatory benefits of facial recognition technology outweigh the risk to the communities served by law enforcement. AB 642 (Ting) would have set minimum standards for use of FRT by law enforcement, including requiring law enforcement agencies to have a written policy for FRT use, allowing for FRT use when a peace officer has reasonable suspicion that an individual has committed a felony, and providing that an FRT-generated match of an individual may not be the sole basis for probable cause for an arrest, search, or affidavit for a warrant. It did not include any limitation on the source of the input image submitted for comparison against the database of persons. Police could use traffic cameras, CCTV, and images from BWCs or dashcams. AB 642 was held in the Assembly Appropriations Committee.

By contrast, AB 1034 (Wilson), of the 2023-2024 Legislative Session, would have prohibited a law enforcement officer or agency from installing, activating, or using a biometric surveillance system solely in connection with a law enforcement agency's body-worn camera, thereby reinstating the outright ban on facial recognition technology used in connected with BWCs originally established by AB 1215, but only until January 1, 2027. AB 1034 is currently on the Senate Inactive file, where it was ordered in September 2023. Because neither AB 642 nor AB 1034 were enacted, there currently are only a very few, context specific restrictions on law enforcement's use of FRT.

5. The 'Probable Cause' Standard and Effect of This Bill

Both the United States and the California Constitutions guarantee the right of all persons to be secure from unreasonable searches and seizures, a protection that applies to all unreasonable government intrusions into legitimate expectations of privacy.[15] In general, a search is not valid unless it is conducted pursuant to a warrant - probable cause sufficient to justify a search warrant generally requires showing that "there is a fair probability that contraband or evidence of a crime will be found in a particular place" to be search, and case law establishes that "reasonable and probable cause exists if a man of ordinary care and prudence would be led to conscientiously entertain an honest and strong suspicion that the accused is guilty."[16] Additionally, police officers must have probable cause prior to arresting an individual, in which case probable cause exists "when, under the totality of the circumstances known to the arresting officers, a prudent

[15] U.S. Const., amend. IV; Cal. Const., art. 1, sec. 13; *United States v. Chadwick* (1977) 433 U.S. 1, 7, overruled on other grounds by *California v. Acevedo* (1991) 500 U.S. 565.
[16] *Illinois v. Gates* (1983) 462 U.S. 213, 238; *People v. Alvarado* (1967) 250 Cal.App.2d 584, 591.

person would have concluded that there was a fair probability that [that individual] had committed a crime."[17] In either case, whether justification for a search or an arrest exists is based on the totality of the circumstances known to law enforcement at the time of the arrest, search, or submitting of an affidavit for a warrant.[18]

California law prescribes the required form and contents of valid arrest warrants, and provides that a judge shall issue an arrest warrant if they are satisfied after reviewing the declaration of probable cause that probable cause based on the facts alleged in the declaration indeed exists. In addition, existing law specifies that the declaration in support of the warrant must be a sworn statement made in writing, signed under penalty of perjury.[19] However, officers may also make warrantless arrests based on probable cause in specified situations, including for a felony, domestic battery, violation of a DV restraining order, certain other assaults and batteries, a concealed firearm violation, or any other misdemeanor committed in the officer's presence.[20] With regard to search warrants, existing law imposes similar requirements that they may be issued only upon probable causes supported by affidavit, but also enumerates the 20 specific grounds upon which a search warrant may be issued.[21] However, as with arrests, peace officers may conduct searches without obtaining a warrant if the particular circumstances of the search fall into one of several well-established exceptions to the general warrant requirement, such as exigency, consent, searches incident to arrest, vehicle searches, and several others.[22]

This bill prohibits peace officers from using an FRT match as the sole basis for probable cause for an arrest or search, and expressly prohibits judges from granting an application for a warrant to search or arrest based solely on an FRT match. The bill also requires peace officers to use information obtained from the use of FRT to "examine the results with care and consider the possibility that matches could be inaccurate." The bill further provides that a violation of these provisions constitutes 'false arrest,' for which damages up to $25,000 may be awarded, and where 'false arrest' occurs when an individual is detained, arrested or otherwise placed in custody without legal justification.

These provisions raise some questions regarding the practical effect of this bill. First, as the analysis prepared by the Assembly Public Safety Committee points out, while this bill establishes that more than an FRT match is needed to establish probable cause or to grant a warrant, it is unclear how much more is needed. Will two matches be sufficient? Are all FRT matches created equal? The Author and Committee may wish to consider what additional evidence may be required in conjunction with an FRT match before the probable cause standard is met.[23]

---

[17] See *U.S. v. Garza* (9th Cir. 1992) 980 F.2d 546, 550; *U.S. v. Gonzales* (9th Cir. 1984) 749 F.2d 1329, 1337

[18] See e.g., *Illinois v. Gates*, supra, 462 U.S. at 238; *U.S. v. Buckner* (9th Cir. 1999) 179 F.3d 834, 837.)

[19] Penal Code § 817

[20] Penal Code §836

[21] Penal Code §1524.

[22] For more info, see Exceptions to Warrant Requirement | U.S. Constitution Annotated | US Law | LII / Legal Information Institute (cornell.edu)

[23] The Assembly Public Safety analysis usefully cites a recent report asserting that "there has been no jurisprudence establishing guidance on…what additional evidence, if any, is needed before officers can make an arrest" after an FRT match, and that, in many instances, "officers have relied heavily, if not exclusively, on leads generated by face recognition searches." Center on Privacy & Technology, Georgetown University, A Forensic Without The Science (Dec. 6, 2022) p. 6

Moreover, the bill provides the $25,000 remedy for a violation of the probable cause-related provisions *and* the provision requiring the exercise of care in examining FRT matches, but it is unclear how plaintiffs or defendants in cases related to such a violation would prove that officers did or did not examine results with care and consider possibilities that results could be inaccurate. Does such a violation actually rise to the level of 'false arrest?' The Author and Committee may wish to consider narrowing the applicability of the remedy to only the probable cause-related provisions.

6. Argument in Support

According to the California Police Chiefs Association:

> FRT has an unprecedented ability to combat criminal activity, identify persons of interest, develop actionable leads, and close cases faster than ever before. It is the objective of protecting our communities and preventing future crime that is driving law enforcement to develop responsible, appropriate, and effective FRT programs. However, there remains a need to ensure the technology is not used in way it was not intended. Through setting meaningful protections, including those within AB 1814, the legitimate use of FRT can lead to significant benefits for public safety.
>
> 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. 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.

7. Argument in Opposition

According to Oakland Privacy:

> By "reference photo database", we believe the author is describing the sources of photographs against which a probe image may be compared. The definition above is deeply problematic. The bill explicitly authorizes the use of "databases operated by third parties" as reference photo databases. The largest and most prominent third party facia recognition database is Clearview AI, the notorious company that scraped the entire Internet at scale without permission, notification or consent and now claims to have 20 billion+ photographs in their database or 60x the population of the entire United States. Use of Clearview AI has been banned in Canada , Australia, has been deemed illegal by the European data protection agency, and the company has been

---

https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/

fined repeatedly in EU nations including France, Italy and Greece for violations of privacy laws. Clearview AI is not the only third party database of faces available, but its collection is many magnitudes greater than any other product available to CA law enforcement agencies.

By broadly sanctioning the use of this widely-condemned database, the California State Legislature would be forfeiting its global leadership in privacy rights by falling short of accepted standards in the EU and Canada. Assembly Bill 1814 also fails to place critical restrictions on the use of facial recognition and in so doing so, signals to law enforcement agencies all over the state that such restrictions are not required. There are many that could be mentioned, but for the purposes of this letter, here are two prominent ones. The bill does not prohibit the use of facial recognition to monitor First Amendment protected activities. In order not to chill First Amendment rights and in deference to the right to privacy preserved in Article 1 of the California Constitution, FRT use must not encompass broad sweeps

of large gatherings of people where each individual at a protest may be scanned and identified for a vague public safety purpose. While it is possible that the author *meant* to restrict use in this way by mentioning probable cause, the language in the bill does not prevent use. It only prevents outcomes i.e. search, arrest or warrant and only when the FRT match is the sole basis for such an action. So its use to fish people out of crowd for further scrutiny is not prevented. This is not an academic concern, e.g in 2020, the Long Beach Police Department did over 700 facial recognition searches through LACRIS with the reason for the search logged as “PDProtest.”

The bill does not prohibit the use of live facial recognition on the street, via a tablet, smartphone or body camera. Recognition software has a significant error rate, especially with darker skinned people. If patrol officers believe that a person they encounter is a felon or dangerous due to a misidentification, they will act aggressively due to perceived danger. When law enforcement thinks someone is a criminal and they run away, it is well-documented that they start shooting in far too many cases, and sometimes with lethal results. Allowing facial recognition use live in the field will reverse many of the criminal justice reforms that California adopted in the wake of the Black Lives Matter movement to reduce police shootings of unarmed black and brown men. By not prohibiting it in a bill that would be the only standing statewide regulation on the use of this technology, the Legislature is sanctioning such use and lives will be lost. The author is trying to address the problem of people being arrested for crimes they didn’t commit (which is a problem and has already happened at least seven different times), but out on the street a misidentification can have lethal consequences before there is any search, arrest or warrant.

8. Committee Amendments

As reflected in the analysis above, the Author has agreed to take the following amendments in committee:

Section 13661 is added to the Penal Code, to read:

13661.

(a)(1) A law enforcement agency or peace officer shall not use a facial recognition technology (FRT) match as the sole basis for probable cause for an arrest ***or*** *search~~. or affidavit for a warrant.~~*

(2) A judge shall not grant an application for a warrant based solely on an FRT match.

(b) A peace officer using information obtained from the use of FRT shall examine results with care and consider the possibility that matches could be inaccurate.

(c) For purposes of this section, the following terms have the following meanings:

(1) "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.

(2) "Probe image" means an image of a person that is searched against a database of known, identified persons or an unsolved photograph file.

(3) "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.

(d) (1) A violation of this section constitutes false arrest, ~~as defined in Section 236,~~ for which damages of up to twenty-five thousand dollars ($25,000) may be awarded to an individual who is subjected to the 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.

(4) For the purpose of this subdivision, a "false arrest" occurs when an individual is detained, arrested, or otherwise placed in custody without legal justification.

-- END –