Date of Hearing: April 25, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 642 (Ting) – As Amended April 19, 2023

SUBJECT: Law enforcement agencies: facial recognition technology

SYNOPSIS

This bill proposes to regulate the use of facial recognition technology (FRT) by local law enforcement agencies. According to the author, the bill includes critical safeguards such as codifying an accuracy level; accountability and oversight; reporting; civil penalties; protections for immigrant communities and people seeking services such as abortion and gender affirming care; prohibiting law enforcement from using a match alone to arrest someone or to request a warrant; and protections against violating someone's constitutional right and discriminating on the basis of protected characteristics. Unfortunately, this bill does not yet include all of the safeguards the author is hoping for.

FRT technology remains far from perfect. Recent studies continue to highlight that many FRT systems continue to be less effective at identifying people of color, women, older people, and children, even when the technology is being tested in optimal conditions using clear probe photographs. Tests 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. 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.

Developing a workable regulatory framework that acknowledges the utility of FRT for safety, security, and efficiency, while remaining conscientious of the potential for FRT to infringe on fundamental rights and civil liberties, such as the individual right to privacy and the freedom to express viewpoints anonymously, is indeed difficult, and requires consideration of several critical questions, both practical and conceptual. Further exacerbating the complexity of this task is the necessity in such a framework for sensitivity to the current technical shortcomings of FRT, including performance disparities between demographic groups and entrenchment of existing cultural biases by those designing and training the algorithms underlying these technologies.

The question before this Committee is whether or not this bill furthers the Committee's policy priorities. First and foremost, protecting Californians' constitutional right to privacy. The Committee is also 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 significant 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 forced to flee for their own safety.

As the following excerpt from Robert Williams' letter of opposition articulates, there is current trauma being inflicted on men like Mr. Williams and their families by use of FRT. If the Legislature decides that the best path is regulation, as the author asserts, it needs to be done through a slow, deliberative, thoughtful process that includes a broad range of stakeholders and experts.

"I may be the first documented case of a wrongful arrest based on a false face recognition match, but I wasn't the last. In the years following my arrest, police have similarly misidentified and detained four other individuals we know of across the country. All of us are Black men. All of us suffered the trauma of being wrenched from our families, isolated, and interrogated by police officers who dismissed our claims of innocence because they believed the technology was infallible. In fact, studies have found that Black and Asian people are up to 100 times more likely to be misidentified than white men." – Robert Williams

This bill is author sponsored and has two supporters and over 30 civil rights and social justice organizations in opposition.

This bill previously passed the Assembly Public Safety Committee on a 6-0-2 vote.

SUMMARY: Sets minimum standards for use of facial recognition technology (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. Specifically, **this bill**:

1) Defines "facial recognition technology" or "FRT" 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.

    a) FRT includes any surveillance system that actively uses FRT to identify persons in a surveilled area in real time.

    b) FRT does not include any access control system used by a law enforcement agency that uses biometric inputs to confirm the identity of employees or other approved persons for the purpose of controlling access to any secured place, device, or system.

2) Defines "reference photograph database" to mean a database populated with photographs of individuals who 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, databases operated by third parties, and arrest photograph databases.

3) Defines "arrest photograph database" to mean a database populated primarily by booking or arrest photographs or other photographs of persons with law enforcement contacts.

4) 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.

5) Authorizes a peace officer to use or request the use of FRT for any of the following reasons:

a) To assist in identifying a person that officer has reasonable suspicion to believe has committed a felony.

b) To assist in identifying a person who is deceased or who has been reported missing, as specified.

c) To assist in identifying any person who has been lawfully arrested, during the process of booking or during that person's custodial detention.

d) To assist in identifying any person if a peace officer determines that an emergency situation exists that involves immediate danger of death or serious physical injury to any person and the identification of that person is necessary to prevent that death or injury.

6) Requires, if a peace officer uses or requests the use of FRT, documentation of all of the following information:

a) The identity of the peace officer using or requesting the use of FRT, and, if applicable, the officer authorizing the use or request;

b) A detailed description, as available, of the person being identified;

c) Any photograph or video being used as a probe image; and,

d) Any details regarding other investigative measures taken to identify the person and an explanation of why those measures failed or are reasonably unlikely to succeed.

7) Requires the custodian of any arrest photograph database being used in conjunction with FRT, beginning on July 1, 2024 and every six months thereafter, to remove from the database any of the following images:

a) Any photograph of a person under 18 years of age;

b) Any photograph of an arrested or detained person who has been released without being charged with an offense, or whose charges have been dismissed;

c) Any photograph of an arrested or detained person who has subsequently been acquitted of the charged offense; or,

d) Any photograph of a person whose conviction has been expunged, has been exonerated of the crime, or who has had their conviction reversed on appeal.

8) Provides that the image removal requirement applies only to the use of a reference photograph database for the use of FRT and shall not be construed to prohibit a peace officer from using any other investigative database including a fingerprint database.

9) Requires any agency that maintains and operates an arrest photograph database to establish procedures to ensure compliance with the image removal requirement.

10) Prohibits a peace officer using or requesting the use of FRT from doing any of the following:

a) Using FRT to identify any person solely on the basis that the person is exercising rights guaranteed by the United States Constitution, including free assembly, association, and speech;

b) Relying on actual or perceived race, ethnicity, national origin, religion, disability, gender, gender identity, or sexual orientation in selecting a person to identify using FRT, except when there is trustworthy information, relevant to the locality and timeframe, in the context of a particular area and for a particular period of time, that links a person with a particular characteristic described to an identified criminal incident or scheme;

c) Sharing FRT data with any state or federal agency for the purpose of enforcing federal immigration law;

d) Providing the results of, or information derived from, the use of FRT to any individual or to any agency or department in another state regarding the provision of lawful gender-affirming health care or gender-affirming mental health care performed in this state;

e) Providing the results of, or information derived from the use of FRT to any individual or agency or department in another state regarding the provision of abortion services in this state;

f) Using an FRT match as the sole basis upon which probable cause is established for a search, arrest, or affidavit for a warrant, and provides that any peace officer using information obtained from the use of FRT shall examine results with care and consider the possibility that matches could be inaccurate; and

g) Using FRT in conjunction with any reference photograph database that contains information, including images, obtained by any of the following means:

   i) In a manner that violates federal or state law;

   ii) In a manner that violates a service agreement between a provider of an electronic communication service to the public or a provider of a remote computing service and customers or subscribers of that provider;

   iii) In a manner that is inconsistent with the privacy policy of a provider, as specified;

   iv) By deceiving a person whose information was obtained;

   v) Through the unauthorized access of an electronic device or online account;

   vi) In violation of a contract, court settlement, or other binding legal agreement; or

   vii) From unlawful or unconstitutional practices by any governmental official or entity.

11) Provides that, for the purpose of prohibiting sharing FRT results regarding persons receiving abortion services or gender-affirming health care and gender-affirming mental health care, "information derived from the use of FRT" means information that would not have been discovered or obtained but for the use of FRT, regardless of any claim that the information would inevitably have been discovered or obtained through other means.

12) Requires each law enforcement agency using FRT or requesting the use of FRT of another agency, by no later than January 31, 2025, and annually thereafter, to prepare and submit a report to the California State Auditor containing only the following information regarding the use of FRT, as applicable:

    a) The information a peace officer is required to document when using or requesting the use of FRT;

    b) Whether modifications were made to any probe images and what those modifications were;

    c) The arrests that FRT results contributed to, and the offenses for which the arrests were made, disaggregated by race, ethnicity, gender, and age;

    d) A description of the reference photograph database that was used;

    e) A description of the FRT system that was used;

    f) The total number of searches performed;

    g) The total number of times FRT results were shared with another law enforcement agency, an outside agency, or a third party; and

    h) The actions taken to comply with requirement that a law enforcement agency remove certain images from a reference photograph database, as specified.

13) Requires each district attorney's office, city prosecutor's office, and the Attorney General, by no later than January 31, 2025 and annually thereafter, to report to the California State Auditor the following information regarding information obtained from FRT:

    a) The number of convictions that FRT results contributed to and the offenses for which the convictions were obtained, disaggregated by race, ethnicity, gender, and age; and

    b) The number of motion to suppress made related to FRT results, and the number granted or denied.

14) Requires the State Auditor, on or before July 1 of each year, to release to the public, post online, and transmit to the Legislature, a full and complete report concerning the use of FRT by law enforcement agencies and prosecutors, including any violations identified.

15) Requires any law enforcement agency using FRT to keep and maintain FRT activity logs or other required records, as specified.

16) Prohibits a law enforcement agency from operating an FRT system that has not been evaluated under the National Institute of Standards and Technology Face Recognition Vendor Testing Program and achieved an accuracy score of 98 percent true positives within two or more datasets relevant to investigative applications on a program report.

17) Prohibits a peace officer from using FRT in any manner that reduces the program's competency score below 98 percent.

18) Requires a law enforcement agency that uses FRT to have a written policy that includes, without limitation, all of the following:

    a) A requirement that FRT use be limited to specifically authorized personnel who have received certified training in the use of FRT by the Commission of Peace Officer Standards and Training;

    b) A requirement that a manger authorized to use FRT be assigned to oversee the FRT program;

    c) A policy that describes the parameters of acceptable inputs to be used as probe images and that prohibits the use of sketches or other manually produced images; and

    d) An acceptable use policy that includes specific allowances and restrictions on use.

19) Requires each law enforcement agency using FRT, by no later than July 1, 2024, to post the required written policy on its website.

20) Prohibits a law enforcement agency or peace officer from requesting or entering into an agreement with another law enforcement agency or other third party to perform FRT search on behalf of the requesting officer or agency if the program operated by the other agency or party does not meet the specified accuracy requirements.

21) Requires a law enforcement agency, if the State Auditor identifies any violations by that agency, to cease using FRT until all violations have been corrected.

22) Requires the law enforcement agency to notify the public if its use of FRT is suspended for violations, as specified.

23) Requires a law enforcement agency that uses FRT to attempt to identify an individual who is arrested to provide the individual with both of the following:

    a) A notice of the name of the law enforcement agency that operated the FRT system used, and the name of the database, if any, the was used to identify the individual; and

    b) A copy of the required accuracy or bias report, each probe image that was used by the agency, any modifications made to the probe image, the candidate list, in rank order, produced by the facial recognition system, and any other documentation related to the use of FRT in the law investigation.

24) Requires the notice provided by the law enforcement agency to the individual arrested to be an appropriate language for the person if they are not fluent or literate in English.

25) Provides that, if a court or law enforcement agency determines that a peace officer has used FRT in violation of the law, and the court or agency finds that the circumstances surrounding the violation raise serious questions about whether or not the officer acted intentionally with respect to the violation, the agency shall promptly initiate a proceeding to determine whether disciplinary action against the officer is warranted.

26) Provides that, notwithstanding any other law, a violation of this title is not punishable as a crime.

27) Authorizes a person who is subject to identification or attempted identification through FRT in violation of the law to bring a civil action against the peace officer or law enforcement agency responsible for the violation.

28) Provides that a person who is the subject of disparate treatment or adverse impact on the basis of race, ethnicity, gender, or age, whether individually or as a member of a class of individuals, due to use of FRT or any technological element, criteria, method, or design feature thereof, by a law enforcement agency, may bring a cause of action against the peace officer, law enforcement agency, or maker of the facial recognition or face surveillance technology responsible for the violation.

29) Provides that the following relief may be recovered or obtained in a civil action for an FRT use violation:

    a) Any actual damages sustained by that person as a result of the violation;

    b) The greater of either of the following:

        i) Statutory damages of $50,000 per violation; or

        ii) Profits earned as a result of each violation.

    c) Exemplary damages, as specified;

    d) Injunctive, equitable, or declaratory relief as may be appropriate, including preliminary injunctive relief; and,

    e) Costs of the action, together with reasonable attorney's fees.

30) Prohibits a civil action from commencing later than two years after the date upon which the claimant discovered or first had a reasonable opportunity to discover the violation.

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 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.)

4) Establishes the California Values Act, which prohibits state law enforcement from using state resources to assist in the enforcement of federal immigration law, except as specified. (Gov. Code § 7282 et seq.)

5) Establishes California as a sanctuary state and prohibits any law enforcement agency from cooperating with federal immigration enforcement authorities. (Gov. Code § 7284, et seq.)

6) Prohibits use of California state funds for travel to any state that is subject to a ban on state-funded and state-sponsored travel because that state enacted a law that voids or repeals, or has the effect of voiding or repealing, existing state or local protections against discrimination on the basis of sexual orientation, gender identity, or gender expression, or has enacted a law that authorizes or requires discrimination against same-sex couples or their families on the basis of sexual orientation, gender identity, or gender expression. (Gov. Code § 11139.8.)

7) Establishes the Reproductive Privacy Act, which provides that the Legislature finds and declares that every individual possesses a fundamental right of privacy with respect to personal reproductive decisions, which entails the right to make and effectuate decisions about all matters relating to pregnancy, including prenatal care, childbirth, postpartum care, contraception, sterilization, abortion care, miscarriage management, and infertility care. Accordingly, it is the public policy of the State of California that:

   a) Every individual has the fundamental right to choose or refuse birth control.

   b) Every individual has the fundamental right to choose to bear a child or to choose to obtain an abortion, with specified limited exceptions.

   c) The state shall not deny or interfere with a person's fundamental right to choose to bear a child or to choose to obtain an abortion, except as specifically permitted. (Health & Saf. Code § 123462.)

8) Provides that the state may not deny or interfere with a person's right to choose or obtain an abortion prior to viability of the fetus or when the abortion is necessary to protect the life or health of the person. (Health & Saf. Code § 123466 (a).)

9) States that a person shall not be compelled in a state, county, city, or other local criminal, administrative, legislative, or other proceeding to identify or provide information that would identify or that is related to an individual who has sought or obtained an abortion if the information is being requested based on either another state's laws that interfere with a person's rights under subdivision (a) or a foreign penal civil action. (Health & Saf. Code § 123466(b).)

10) Declares that it is the intent of the Legislature to establish policies and procedures to address issues related to the downloading and storage 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).)

11) 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.)

12) 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).)

13) 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).)

14) Requires that a public agency that operates or intends to operate an Automatic License Plate Recognition (ALPR) system to provide an opportunity for public comment at a public meeting of the agency's governing body before implementing the program. (Civ. Code § 1798.90.55.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal

COMMENTS:

1) **Facial recognition technology (FRT)** refers to the use of automated devices to identify or verify a person from a digital image by determining whether two images of faces represent the same person. FRT consists of two component processes: face detection, or locating a face within a photo, and face identification, or the matching of facial information to an image or images in a specified database that links to identifying information. FRT relies on the use of biometrics, the statistical analysis of measurements of biological data, in order to compare these images, reducing complex images to numerical values that represent key facial measurements that distinguish individuals.

2) **Research demonstrates significant problems with FRT and its ability to accurately identify people.** 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. 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 these 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. (Johnson, et al, *Facial recognition systems in policing and racial disparities in arrests*, Government Information Quarterly 39 (2022) 101753, Elsevier, *available at* https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892.)

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. (Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*. Georgetown Law Center on Privacy and Technology, (May 16, 2019) *available at* https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/.)

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." (*Facial recognition software has a gender problem*, National Science Foundation (Nov. 1, 2019), *available at* https://new.nsf.gov/news/facial-recognition-software-has-gender-problem.)

3) **Law Enforcement Uses of Facial Recognition Systems.** 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. (*Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, United States Government Accountability Office. (Jun. 3, 2021), *available at* https://www.gao.gov/products/gao-21-518.) One study found that one in four law enforcement agencies across the country can access some form of FRT, and that half of American adults–more than 117 million people–are in a law enforcement face recognition network. (Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy and Technology (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.) 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." (*Facial Recognition Technology Patrol Guide*, City of New York Police Department (Mar. 12, 2020), *available at* https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf.)

Proponents of facial recognition technology see it as a useful tool in helping 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. (Singer, *Amazon's Facial Recognition*

Wrongly Identifies 28 Lawmakers, A.C.L.U. Says, New York Times, (Jul. 26, 2018), *available at* https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html?login=facebook.)

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. (*Clearview AI class-action may further test CCPA's private right of action*, JD Supra (Mar. 12, 2020), *available at* https://www.jdsupra.com/legalnews/clearview-ai-class-action-may-further-14597/.) 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. (*Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here.* Buzzfeed News (Apr. 6, 2021). *available at* https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table.)

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. (Cassidy, *Facial recognition tech used to build SFPD gun case, despite city ban*, San Francisco Chronicle (Sept. 24, 2020), *available at* https://www.sfchronicle.com/bayarea/article/Facial-recognition-tech-used-to-build-SFPD-gun-15595796.php.)

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

As noted in the NYPD 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 recent *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. 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. (Hill and Mac, *'Thousands of Dollars for Something I Didn't Do,'* New York Times (Mar. 30, 2023), *available at* https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.)

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." (Hill, Wrongfully *Accused by an Algorithm*, New York Times (Aug. 3, 2020) *available at* https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html). 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. (For a detailed account of his experience, please see ***ARGUMENTS IN OPPOSITION***)

4) **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 or restrictions 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. We can't go another year with no protections. AB 642 is a response to a battle that we cannot afford to risk losing. The bill includes critical safeguards such as codifying an accuracy level, accountability and oversight, reporting, civil penalties, protections for immigrant communities, people seeking services such as abortion and gender affirming care, prohibits law enforcement from using a match alone to arrest someone, to request a warrant, to violate someone's constitutional rights, and to discriminate against protected characteristics. Most importantly, this bill does not prohibit nor deter local governments from choosing to ban the use of facial recognition technology.

5) **How this bill would regulate the use of facial recognition technology by law enforcement.** According to the author, in an effort to strictly regulate the use of FRT, the bill is intended to work as follows:

> 1. Defines facial recognition technology as, in part, including any surveillance system that actively uses FRT to identify people in a surveilled area in real time.
>
> 2. Allows the broad use of virtually all available data bases, including arrest photograph databases and reference photograph databases owned by third parties.
>
> 3. Establishes the authorized uses for FRT, including identifying a person the officer reasonably believes is suspected of committing a felony; identifying a dead or missing person; identifying a person who has been arrested; or identifying any person if the officer decides an emergency situation exists.

4. Establishes prohibited uses of FRT, including identifying people exercising First Amendment rights, people seeking gender affirming care or abortion services, or immigrants.

4. Establishes oversight provisions, including the information that is required to be documented when the technology is used; preparing and submitting an annual report to the California State Auditor; and requiring the State Auditor, in turn, to produce an annual report.

5. Requires the arrest database being used to be purged of certain images every six months.

6. Establishes acceptable accuracy standards, which are a 98 percent accuracy rating from the National Institute of Standards and Technology (NIST) and prohibits an officer from using the technology in a way that reduces the accuracy rating.

7. Requires when FRT is used to identify a person who is subsequently arrested, that the person must be provided with certain information.

8. Establishes civil penalties for intentionally violating the statute.

9. Sets a 2-year statute of limitations for civil suits.

6) **Committee amendments.** The Committee amendments are intended as a modest first step towards addressing the privacy issues that are of concern in this bill. There are four changes:

1. Clarification that the prohibitions in the bill apply not just to individual officers, but to the entire agency, whether the person using the database for a prohibited use is a sworn police officer or not.

> A peace officer using or requesting the use of FRT shall not do any of the following:

Will now be --

> ***A law enforcement agency or officer authorizing the use of, maintaining the database for, or using FRT shall not do any of the following:***

2. Tightening of the language in the bill designed to protect people seeking abortion services and gender affirming care to mirror other laws prohibiting the sharing of data related to these services.

> (d) (1) Provide the results of, or information derived from, the use of FRT to any individual or to any agency or department in another state regarding the provision of lawful gender-affirming health care or gender-affirming mental health care performed in this state.

Will now be --

> ***(d)(1) Notwithstanding any other provision of this title, a law enforcement agency or officer shall not release any FRT data or results, or allow access to databases used with FRT, in response to a subpoena or request if that subpoena or request is based on any of the following:***

(A) Another state's laws that interfere with a person's rights under the Reproductive Privacy Act (Article 2.5 (commencing with Section 123460) of Chapter 2 of Part 2 of Division 106 of the Health and Safety Code.

(B) A foreign penal civil action, as defined in Section 2029.200 of the Code of Civil Procedure.

(C) An investigation related to a natural person seeking gender affirming health care or gender affirming mental health care.

3. Similar to #2, tightening the language in the bill which prohibits the sharing of data with federal agencies seeking to enforce federal immigration law.

(c) Share FRT data with any state or federal agency for the purpose of enforcing federal immigration law.

Will now be --

(c) Notwithstanding any other provision of this title, a law enforcement agency or officer shall not release any FRT data or results, or allow access to the databases used with FRT, in response to a subpoena or request if that subpoena or request is in violation of the California Values Act.

4. Adding a requirement that the Department of Technology, the state's primary repository of cybersecurity expertise, issue standards related to FRT data.

(b) ***(1) By July 1, 2024, the California Department of Technology, in consultation with the Chief of the Office of Information Security, shall issue standards to ensure the confidentiality and cybersecurity of FRT data and results. A law enforcement agency is required to establish a written policy that adheres to these standards. Nothing in this paragraph shall prevent a law enforcement agency from adopting a written policy that provides for standards stronger than those issued by the Department.***

(2) A law enforcement agency that uses FRT shall have a written policy that includes, without limitation, all of the following:

(3) A requirement that FRT use be limited to specifically authorized personnel who have received certified training in the use of FRT by the Commission on Peace Officer Standards and Training.

(4) A requirement that a manager authorized to use FRT be assigned to oversee the FRT program.

(5) A policy that describes the parameters of acceptable inputs to be used as probe images and that prohibits the use of sketches or other manually produced images.

(6) An acceptable use policy that includes specific allowances and restrictions on use.

7) **Significant issues remain with this bill.** As noted in the previous section on Committee amendments, the changes made to the bill in this Committee are not meant to be all encompassing, nor do they resolve the largest concerns with the bill. The author has stated that

he is attempting to establish real and robust guardrails limiting the use of FRT, that these are complicated issues and would benefit from the input of a broad range of experts and stakeholders. The expectation is that if this bill passes out of the Committee, the larger issues will be addressed prior to it coming back to the Assembly for concurrence. The following is a list of the major issues identified by the Committee:

1. *The bill contains broad permission to use any FRT system on images from any device, including real-time identification of people from body-worn camera video, against any database chosen. This latitude may be excessive.*

A. *As currently written, this bill allows for the adoption of any type of FRT* (*see* 1) a) in the **SUMMARY**). While perhaps intended to clarify that any future technology will fall under this statute, this broad definition appears to give tacit approval to law enforcement agencies to use any FRT system, regardless of its privacy implications. Robust guardrails ought to precisely enumerate how and what technology can be used and prohibit other uses without express permission from the Legislature.

B. *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 millions of people without first obtaining a court order, warrant, or some other permission to do so.

2. *The 98% NIST accuracy requirement likely will not improve the accuracy of the results.* A 98 percent NIST rating does not appear to mean the results are accurate 98 percent of the time. It means that during the controlled NIST testing, 98 percent of the time, the system accurately identified the person in the picture along with an unknown number of other people that the system also identified as possibly being the person. In other words, the correct person could be among one of 50 other people who were also identified as possibly being the person.

In addition, as discussed previously, an overall 98 percent accuracy rating, is not the same as determining that the system was able to identify the person in the photo 98 percent of the time when tested against all demographics.

Finally, the NIST test determines the accuracy rating using a particular database and particular types of photographs, e.g., an employee identification photo compared to a database containing all of the employees of a company. It does not test the ability of the system to not identify potential matches when the person in the probe photo is not in the database, for example. Also, it is important to note, that in order to guarantee a 98 percent accuracy rating, NIST would need to test every probe photo on the specific database being used to determine the accuracy level.

3. *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. (Those test results that bear this out are available at https://pages.nist.gov/frvt/reports/demographics/annexes/annex_16.pdf.)

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.

4. *The bill provides broad latitude for an officer to use the system in ways that are intended to be prohibited.* Specifically, bill language currently includes words and phrases that dilute the guidelines. As an example, section 5 in the **SUMMARY** describes authorized situations in which FRT can be used (e.g., to identify someone suspected of committing a felony or someone who is missing or dead). While these limitations may seem clear and sensible, 5) d) in that section waters down those prohibitions by allowing an officer to use the system if the officer determines an emergency situation exists that involves immediate danger of death or serious injury.

In addition, the specific prohibition against using FRT on people who are exercising their First Amendment rights states that officers cannot use the system to "identify any persons *solely* on the basis that the person is exercising their rights." (10) a) in the **SUMMARY.**)

Using the exceptions in both of these parts of the bill, for example, means that FRT could in fact be used by an officer who is doing crowd control at a protest where people are exercising their First Amendment rights. In order to freely surveil the protesters, all the officer would need to assert is that they were concerned that the protest may devolve and someone may get injured or killed therefore it was a permissible use.

5. *The bill lacks robust oversight and data collection requirements.* Under the bill, the State Auditor is tasked with collecting information and overseeing the use of the technology. The State Auditor lacks strong enforcement authority and, regardless of the language in this bill, could be tasked with auditing agencies' use of FRT at any time. In developing an oversight framework that seeks to create robust oversight and data collection, the Legislature should consider tasking the Attorney General with oversight and vest the office with the power to prohibit the use of the technology in the event it is being misused or proper security measures are not in place. In addition, any legislation should include comprehensive data collection that will be uploaded in the OpenJustice data portal allowing for open access to the data for policy-makers, the public and researchers.

6. *The bill lacks any cybersecurity requirements and speaks only to the regulation of law enforcement agencies, not restrictions on third-party vendors*. Law enforcement agencies that take advantage of this technology are not purchasing a system that is self-contained and housed within their agency. They are contracting with third-party vendors that run the images for them.

As has been demonstrated by the actions of companies like Clearview AI, any legislation that contemplates regulating the use of FRT should consider the relationship between the law enforcement agency and the vendor. At a minimum, the bill should contemplate a prohibition against images shared by California law enforcement being added to the vendors' databases.

7. *Lacks any training requirements for the use of the system.* This bill requires that officers receive training from the Commission on Peace Officer Standards and Training (POST) prior to using FRT. However, a review of the POST catalog shows that there is currently no POST certified training on the appropriate use of FRT. This lack of training poses challenges for the bill as it is currently drafted. In considering a regulatory framework more in-depth discussion related to what the training must include and how often it needs to be taken should be considered.

Beyond the specific concerns of the bill, however, the lack of POST certified training means that many law enforcement agencies around the state are using this technology without any proper training and may not understand that the results are not definitive and can be further compromised by poor quality probe images.

8. *Regardless of the restrictions put in place in state law, experience from departments around the country and recent discoveries related to the use of Automated License Plate Reader (ALPR) data in California suggests that they may be ignored, putting people in danger.* In contemplating the regulation of FRT versus restricting or prohibiting its use, the Legislature should use the experience with ALPR systems as a guide, particularly the findings of the State Auditor's office as a result of their 2019 audit. (See this Committee's analysis of AB 1436 (Lowenthal, 2023) for a detailed discussion of the report.)

Experience in California and around the country has shown that not infrequently, law enforcement officers and agencies are either unaware of or choose to ignore state laws designed to establish limits and restrictions related to policing. This is already being seen in the misuse of FRT. According to a recent *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. 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. (Hill and Mac, '*Thousands of Dollars for Something I Didn't Do,*' New York Times (Mar. 30, 2023), *available at* https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.)

[A letter in opposition to this bill from one of the five men identified by Clare Garvie, Robert Williams, is included in its entirety at the end of this analysis.]

8) **Final analysis.** The question before this Committee is whether or not this bill 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 notes, 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.

9) **Related legislation.** AB 1034 (Wilson, 2023) would prohibit a law enforcement officer or agency from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other officer camera. AB 1034 is being heard in this Committee today.

AB 793 (Bonta, 2023) would provide that a government entity may not seek, from any court, a compulsory process to enforce a reverse-location demand or a reverse-keyword demand, as defined. AB 793 is pending hearing in the Assembly Appropriations Committee.

AB 1483 (Lowenthal, 2023) requires a local public agency end-user of an automated license plate reader (ALPR) to purge information that does not match information on a hot list, as defined, within 30 days and explicitly prohibits the selling, sharing or transferring of ALPR data with an out-of-state or federal agency without a valid California court order or warrant. That bill is currently pending before this Committee.

AB 1281 (Chau, 2019) would have required any business that uses facial recognition technology in California to disclose that usage in a physical sign that is clear and conspicuous at the entrance of every location. This bill was placed on the inactive file on the Senate Floor.

AB 1215 (Ting, Ch. 579, Stats. 2019) prohibits a law enforcement officer or agency from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other camera. It sunsetted effective January 1, 2023.

AB 375 (Chau, Ch. 55, Stats. 2018) enacted the CCPA to ensure the privacy of Californians' personal information through various consumer rights.

SB 1121 (Dodd, Ch. 735, Stats. 2018) ensured that a private right of action applied only to the CCPA's section on data breach and not to any other section of the CCPA, as specified, corrected numerous drafting errors, made non-controversial clarifying amendments, and addressed several policy suggestions made by the AG in a preliminary clean-up bill after the passage of AB 375.

10) **Next steps for this bill.** Should this bill pass, the author has committed to working on the issues raised in this Committee analysis. It is expected the bill will be amended further to address these issues. As an example, it may be appropriate, for example, to prohibit the use of any facial

recognition technology until NIST determines that all biases have been eliminated. Discussions around this bill's provisions are far from over, and if the bill is not amended to satisfy the concerns of the Committee, it is likely that this Committee will assert its power to re-hear the bill on concurrence.

ARGUMENTS IN SUPPORT: 18 law enforcement entities that were in support of the previous version of the bill, have removed their support. The League of California Cities remains in support and writes:

> The League of California Cities (Cal Cities) is pleased to support AB 642 (Ting). This measure would require any law enforcement agency that uses facial recognition technology (FRT) to have a written policy governing the use of that technology and would require any FRT system used to meet certain national standards and would limit the use of FRT to use as an investigative aid. Additionally, the measure would specifically prohibit the use of any FRT-generated match from being the sole basis for probable cause in an arrest, search, or warrant and would also require an agency using FRT to post their written policy and an annual summary of FRT usage on their internet website.
>
> 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.
>
> Cal Cities supports accountability on the part of law enforcement agencies concerning police 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.

ARGUMENTS IN OPPOSITION: Over 50 civil rights and social justice organizations are opposing this bill. In addition, Robert Williams, the first man who has been identified as being arrested because of faulty FRT, has also written in opposition to this bill. His letter is included here in its entirety so that it can be included in the record.

Statement of Robert Williams.

> Three years ago, I was arrested for a crime I didn't commit based on a false face recognition match. The nightmarish ordeal upended my life and convinced me that law enforcement should not have access to this inherently flawed, racially biased technology.
>
> My story began in January 2020 with a phone call from Detroit police advising me to turn myself in. They refused to tell me why, so I assumed it was a prank.
>
> When I arrived home, police were waiting for me. With no explanation, officers handcuffed me on my front lawn while my distressed wife and young daughters watched. At the detention center, officers took my fingerprints, DNA sample and mugshot. Scared and confused, I spent the night on the cold and filthy concrete floor of an overcrowded cell.

The next day, police accused me of stealing thousands of dollars' worth of watches from a store I hadn't visited in years.

I could prove I was driving home from my job 40 minutes outside Detroit at the time of the robbery. It didn't matter. Facial recognition software had matched a blurry image pulled from the store's grainy surveillance footage to my driver's license photo, and a security consultant who watched the video, but who had not seen the suspect in person, picked me out of a shoddy photo lineup. Even though police were specifically told the facial recognition result was just a lead and was not to be used as the sole basis for an arrest, for the detectives, it was enough to arrest me.

Even after police acknowledged the face recognition software had made a mistake, they didn't immediately release me. I spent 30 hours in custody before I was allowed to return to my worried family. After dropping the charges, in August 2020 the Wayne County prosecutor's office expunged my record and deleted my fingerprints from the police department's database.

I may be the first documented case of a wrongful arrest based on a false face recognition match, but I wasn't the last. In the years following my arrest, police have similarly misidentified and detained four other individuals we know of across the country. All of us are Black men. All of us suffered the trauma of being wrenched from our families, isolated, and interrogated by police officers who dismissed our claims of innocence because they believed the technology was infallible. In fact, studies have found that Black and Asian people are up to 100 times more likely to be misidentified than white men.

In my case, Detroit police were supposed to treat face recognition matches as an investigative lead, not as the only proof they need to charge someone with a crime. They should have collected corroborating evidence such as an eyewitness identification, cell phone location data or a fingerprint. They had none of that – just an out-of-focus image of a large Black man in a baseball cap that a faulty algorithm had determined was me.

My message to this committee is that AB 642 is dangerous. It would be a grave mistake to assume that AB 642 will prevent what happened to me from happening to people in California. As in my situation, this bill instructs officers not to solely rely on facial recognition results.

Regardless of the bill's language, if the software identifies a match, police will think they've found the right person. Once that happens, they will zero in on that individual, subjecting them to unjustified scrutiny, disregarding evidence that doesn't fit their chosen narrative, and ignoring other potential suspects. Face recognition matches would become a driving force behind police investigations and false positives will lead to bad arrests.

There is no acceptable number of misidentifications. One out of 50, one out of 100, one out of 10,000, it's all too high. No one should have to go through what I did, but I fear if this bill is passed, they will.

If the California legislature embraces the widespread use of face recognition technology, there will be many more cases like mine – innocent people put in harm's way and damage that can never be undone. But they may not be as lucky as I was to avoid a conviction, or worse, a fatal encounter with police.

> False matches don't only harm the person who is arrested. The experience traumatizes the entire family. My daughters have not forgotten seeing their father shoved into the back of a patrol car. To this day, the frightening memory sometimes makes them cry.
>
> Face recognition software is flawed and dangerous. None of the provisions in this bill will adequately prevent police from abusing the technology and arresting someone simply because a racially biased algorithm scanned their face. The only safe path forward is a total prohibition on police use of face recognition.

REGISTERED SUPPORT / OPPOSITION:

Support

League of California Cities
Orange County Board of Supervisors - Supervisor Vicente Sarmiento

Opposition

A New Way of Life
Access Reproductive Justice
ACLU California Action
All of Us or None - Riverside
Anti Police-Terror Project
Asian Americans Advancing Justice - Asian Law Caucus
Asian Law Alliance
Bend the Arc California
Bend the Arc: Jewish Action
California Association of Black Lawyers
California Coalition for Women Prisoners
California Immigrant Policy Center
California Innocence Coalition: Northern California Innocence Project, California Innocence Project, Loyola Project for The Innocent
California United for A Responsible Budget (CURB)
Cancel the Contract
Care First California
Central American Resource Center of San Francisco
Citizens for A Better Los Angeles
Clergy and Laity United for Economic Justice
Coalition for Homelessness San Francisco
Council on American Islamic Relations
Electronic Frontier Foundation
Equal Justice Society
Family Reunification Equity & Empowerment (F.R.E.E.)
Fight for The Future
Free Speech Coalition
If/when/how: Lawyering for Reproductive Justice
Indivisible CA Statestrong
Initiate Justice
Lawyers' Committee for Civil Rights of The San Francisco Bay Area
Legal Services for Prisoners With Children

Long Beach Immigrant Rights Coalition
Media Alliance
MediaJustice
Muslim Democrats and Friends
National Center for Lesbian Rights
Oakland Privacy
Orange County Rapid Response Network
Partnership for The Advancement of New Americans
People's Budget Orange County
Positive Women's Network - USA
Privacy Rights Clearinghouse
Safer Streets LA
San Francisco Public Defender - Racial Justice Committee
San Jose Nikkei Resisters
Secure Justice
Silicon Valley De-bug
St James Infirmary
Starting Over INC.
Stop the Musick Coalition
Tenth Amendment Center
Training in Early Abortion for Comprehensive Healthcare (TEACH)
Transforming Justice Orange County
Transgender, Gendervariant, Intersex Justice Project
Urge: Unite for Reproductive & Gender Equity
2 Individuals

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