Date of Hearing: April 25, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 1034 (Wilson) – As Amended March 2, 2023

As Proposed to be Amended

SUBJECT: Law enforcement: facial recognition and other biometric surveillance

SYNOPSIS

Since the killing of George Floyd sparked outrage around the country, policy makers, including this Legislature, have been searching for ways to reduce police violence, particularly against unarmed Black people. Since the start of 2020, police officers have killed a reported 3,710 people across the United States, 567 of whom were Black. In 2022 alone a Black person was killed somewhere in the country by a police officer almost every day.

One of the key tools in that effort was increasing the use of body-worn cameras by police officers. The intention, in encouraging the use of those cameras, was as a tool to increase police accountability in the wake of the growing numbers of police killings. Instead of serving that purpose, it appears that we may be on the cusp of having them turned into a tool of police surveillance through the use of facial recognition technology (FRT)—meaning 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—on everyone officers encounter during their shifts.

The intent of this bill is to continue a moratorium on allowing law enforcement to use facial recognition technology on images obtained through the use of body worn or other personal officer cameras. The previous ban expired on January 1, 2023.

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.

This bill, however, concerns only prohibiting its use on body-worn and other personal use police cameras. Given all of the evidence condemning the use of FRT systems across the board, this is a very narrow prohibition. Recent research supports the need for this prohibition. In a 2020 Purdue University dissertation study, the researcher concluded:

> *Results of the study showed that matching results are poor in a biometric system where the test body-worn camera was the sensor, with error rates as high as 100% when the body-worn camera wearer was in motion. The general conclusion of this study is that a body-worn camera is not a suitable sensor for a biometric facial recognition system at this time, though advances in camera technology and biometric systems may close the gap in the future.*

Notably, this conclusion is tied to two aspects of body cameras that are not likely to change: the footage is the result of officers moving, and the footage is filmed with a wide angle, which skews faces.

In an effort to acknowledge that improvements in technology often happen very quickly, the Committee amendments shorten the 10 year moratorium to three years, thus allowing the Legislature to revisit the issue in two years.

The question before this Committee is whether or not this bill furthers the Committee's policy priorities. First and foremost, protecting Californian's constitutional right to privacy. Along with that, the Committee is working to ensuring that all Californians, and those coming from out of state, are protected from punitive and discriminatory draconian laws attacking the LGBTQ+ community and criminalizing people seeking abortion and gender affirming care. Another priority of the Committee is ensuring that our 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 the question above is "yes." Returning the moratorium on the use of FRT on these cameras provides the only guarantee that tools designed to increase police transparency are not turned into tools of mass surveillance that put people at risk.

This bill is supported by over 50 civil rights and social justice organizations and is opposed by over 20 law enforcement organizations. It passed the Public Safety Committee on a 6-2 vote.

SUMMARY: Prohibits law enforcement agencies from use of Facial Recognition Technology on an officer camera, as defined, or data collected by an officer camera. Sunsets the provisions of this bill on January 1, 2027. Specifically, **this bill**:

1) Provides the following definitions:

    a) "Biometric data" means a physiological, biological, or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish individual identity.

    b) "Biometric surveillance system" means any computer software or application that performs facial recognition or other biometric surveillance.

    c) "Facial recognition or other biometric surveillance" means either of the following, alone or in combination:

        i) An automated or semiautomated process that captures or analyzes biometric data of an individual to identify or assist in identifying an individual.

        ii) An automated or semiautomated process that generates, or assists in generating, surveillance information about an individual based on biometric data.

    d) "Facial recognition or other biometric surveillance" does not include the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information.

    e) "Law enforcement agency" means any police department, sheriff's department, district attorney, county probation department, transit agency police department, school district police department, highway patrol, the police department of any campus of the University

of California, the California State University, or a community college, the Department of the California Highway Patrol, and the Department of Justice.

f) "Law enforcement officer" means an officer, deputy, employee, or agent of a law enforcement agency.

g) "Officer camera" means a body-worn camera or similar device that records or transmits images or sound and is attached to the body or clothing of, or carried by, a law enforcement officer.

h) "Surveillance information" means either of the following, alone or in combination:

i) Any information about a known or unknown individual, including, but not limited to, a person's name, date of birth, gender, or criminal background.

ii) Any information derived from biometric data, including, but not limited to, assessments about an individual's sentiment, state of mind, or level of dangerousness.

i) "Use" means either of the following, alone or in combination:

i) The direct use of a biometric surveillance system by a law enforcement agency or officer.

ii) A request, agreement, or practice by a law enforcement agency or officer that another law enforcement agency or other third party use a biometric surveillance system on behalf of the requesting officer or agency.

2) Prohibits any law enforcement agency or officer from installing, activating, or using any biometric system in connection with an officer camera or data collected by an officer camera.

3) Allows a person to bring an action for equitable or declaratory relief in court against a law enforcement agency or officer who violates this section.

4) Clarifies that this section does not preclude a law enforcement agency or officer from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric data or surveillance information.

5) Sunsets these provisions on January 1, 2027.

6) States legislative findings and declarations, among them:

a) Police body cameras were intended to guard against police misconduct, not to be exploited for surveillance of Californians. Face surveillance would break this promise, transforming a tool for police accountability into a powerful surveillance system that will harm Californians and undermine civil rights.

b) These are the exact type of dangerous interactions that would increase if police use of facial recognition were to expand. Body cameras produce low-quality footage that is blurry, skewed, and in near-constant motion. To date, at least four Black men have been wrongly arrested and accused of crimes because of facial recognition errors and misuse.

c) The widespread use of facial recognition on police body cameras would be the equivalent of requiring every Californian to show their photo ID card to every police officer they pass. This new mass surveillance system would suppress civic engagement and inspire fear. People who are afraid of having their identities and locations recorded and potentially shared with out-of-state agencies will be discouraged from seeking reproductive health care, attending protests, or reporting public safety issues.

d) While this violates everyone's rights, the danger is greatest for immigrants, over-policed Black and Brown communities, LGBTQIA people, and those coming to California for health care criminalized in their home states. Today there is strong and growing public consensus that face surveillance is simply too dangerous and corrosive to our rights to be used by law enforcement.

e) Prominent technology companies like Microsoft, Amazon, and IBM, have forbidden sales of their face surveillance systems to law enforcement. Axon, the most prominent body camera maker, also rejected the use of facial recognition for body cameras, citing the potential inaccuracy and abuse.

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

5) Encourages agencies to consider best practices in establishing policies related the use, storage and retention of footage from body-worn cameras. (Pen. Code § 832.18.)

6) 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(a).)

7) Prohibits a public agency from selling, sharing, or transferring ALPR information, except to another public agency, and only as otherwise permitted by law. (Civil Code, § 1798.90.55(b).)

8) Prohibits a local agency from acquiring cellular communications interception technology unless approved by its legislative body at a regularly scheduled public meeting, as specified. (Gov. Code, § 53166(c)(1).)

9) 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.)

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

11) 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.)

12) 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.)

13) 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).)

14) 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).)

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

COMMENTS:

1) **Purpose.** Since the killing of George Floyd sparked outrage around the country, policy makers, including this Legislature, have been searching for ways to reduce police violence, particularly against unarmed black people. Since the start of 2020, police officers have killed a reported 3,710 people across the United States, of whom 567 were Black. In 2022 alone a Black person was killed somewhere in the country by a police officer almost every day. (*Mapping Police Violence* database (last updated Feb. 15, 2023) *available at* https://mappingpoliceviolence.org/.)

One of the key tools in that effort was increasing the use of body-worn cameras by police officers. The intention, in encouraging the use of those cameras, was as a tool to increase police accountability in the wake of the growing numbers of police killings. Instead of serving that purpose, it appears that we may be on the cusp of having them turned into a tool of police surveillance through the use of facial recognition technology (FRT) on everyone officers encounter during their shifts.

The intent of this bill is to continue a moratorium on allowing law enforcement to use facial recognition technology on images obtained through the use of body worn or other personal officer cameras. The previous ban expired on January 1, 2023.

2) **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 link 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.

3) **Authors statement.** According to the author:

> Police body cameras were promised as a guard against police misconduct. Biometric surveillance, such as facial recognition, would break this promise, transforming a tool for police accountability into a vehicle for mass surveillance.
>
> The deployment of face recognition on body cameras would make face recognition ubiquitous throughout the state, inevitably resulting in additional unnecessary encounters between police and Californians as a result of both accurate and false matches, which would lead to people being wrongfully arrested, injured, and even killed by police.
>
> Face recognition systems are incompatible with body camera systems. The nature of body camera footage–captured by shaky cameras with wide angle lenses that warp people's faces–raises the possibility of false matches and dangerous mistakes. Outside the body camera context, face recognition software has been found to be notoriously inaccurate with Black and Asian faces. As things stand, there are already five known cases of Black men being wrongly arrested as the result of facial recognition misuse and errors by law enforcement.

> But police use of facial recognition is dangerous, regardless of its accuracy. The widespread use of face recognition on police body cameras would be tantamount to requiring every Californian to show their photo ID card to every police officer they pass. Fear of mass police surveillance also could have a chilling effect on protests. Officer-based biometric surveillance across the state would discourage people from seeking medically necessary reproductive healthcare or gender-affirming care in California.
>
> Given the rise of legislative attacks on abortion access and trans people across the country, California should be taking steps to increase health and safety, not greenlighting surveillance systems that capture and track identities and movements. We know once these systems are built, they are abused to target marginalized people here in the state, or by out-of-state governments who do not share California values.
>
> For three years, a now-expired state law prohibiting body camera face surveillance successfully helped prevent the misidentification and wrongful imprisonment of Californians, safeguarded our freedom of speech, impeded creation of dangerous biometric databases, and protected our privacy. This bill would restore those protections under California law.

4) **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, distant, and even doctored—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 were wrong more than one third of the time. In addition, earlier studies suggest they tend 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.)

FRT systems in general remain flawed and biased, even in the most ideal of testing environments. This bill, however, concerns *only* prohibiting its use on body-worn and other personal use police cameras and research suggests that using FRT on these images is even more concerning. In a 2020 Purdue University dissertation study, the researcher concluded:

> Results of the study showed that matching results are poor in a biometric system where the test body-worn camera was the sensor, with error rates as high as 100% when the body-worn camera wearer was in motion. The general conclusion of this study is that a body-worn camera is not a suitable sensor for a biometric facial recognition system at this time, though advances in camera technology and biometric systems may close the gap in the future. (Bryan, *Effects of Movement on Biometric Facial Recognition in Body-Worn Cameras*, Purdue University, Department of Technology Leadership and Innovation (May 2020).)

Notably, this conclusion is tied to two aspects of body cameras that are not likely to change: the footage is the result of officers moving, and the footage is filmed with a wide angle, which skews faces.

5) **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. (June 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 (Sep.. 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 (Sep. 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*** in this Committee's analysis of AB 642)

6) **Committee amendments.** Given how quickly technology evolves, the Committee amendments sunset this bill after three years, rather in ten, to insure that the Legislature has an opportunity to review any advancements in the technology to determine whether or not there might be some value in allowing its use.

7) **Joint Hearing of the Privacy and Consumer Protection Committee and the Select Committee on Emerging Technologies and Innovation 2020 hearing on facial recognition technology.** This Committee held a joint hearing in March of 2020, to explore the implications of the use of FRT in California. While that hearing explored the broader uses of FRT and was not exclusively focused on its use by law enforcement, there were several key findings related to the erosion of privacy that are important to remember when considering the merits of reinstating the lapsed ban on the use of FRT on personal police cameras:

> While the United States Constitution does not explicitly guarantee a right to privacy, the Supreme Court has consistently ruled that the Constitution includes an implicit right to privacy granted by the First, Third, Fourth, and Fifth Amendments. Emphasizing the fundamental importance of a right to privacy, the California Constitution made this right explicit and inalienable under Article 1, Section 1, which states, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." In addition, Sections 24 and 28 of the same Article reassert this right to privacy as it applies specifically to defendants and victims of criminal conduct, respectively, by preventing its universal suspension due to suspicion of criminal behavior.
>
> Because FRT is capable of passively identifying virtually any individual in a recording or real-time feed, and without that individual's knowledge, the expanding adoption of FRT in

both the public and private sectors has come under scrutiny for its implications for individual privacy. FRT poses particularly serious threats to privacy because it is, at present, minimally regulated. In response to concerns relating to the lack of regulation of FRT, the California Legislature passed AB 1215 (Ting, Chap. 579, Stats. 2019), which placed a three-year moratorium on the use of any biometric surveillance system, including FRT, in connection with police-worn body cameras. Apart from this measure, however, the use of FRT is generally unregulated, and it is unclear how existing privacy protections apply to the use of FRT.

While law enforcement collection of biometric information (e.g., mouth swabs, fingerprinting, etc.) typically constitutes a "search" subject to certain protections under the Fourth Amendment, FRT, which can collect biometric information passively, does not require the physical seizure of that biometric information, and is thus categorically unique. Federal district courts in California have held that an individual's reasonable expectation of privacy extends to records of their movements revealed by cell-site location information, and that a warrant must be approved for obtaining this information, indicating that a physical search is not necessary for the Fourth Amendment to apply. However, no state or federal court has yet ruled on the application of Fourth Amendment protections to the use of FRT.

Other applications of FRT include tracking the behavior of an individual over time by identifying and compiling when an individual is in front of a given recording device/feed, or identifying individuals in public without their knowledge. These capacities raise concerns that adoption of FRT could spell the end of public anonymity. One can imagine the privacy and security threats in a world in which each person wears glasses with FRT that can identify any individual they encounter; a malicious person inadvertently bumped while passing another on the street could immediately identify their name, address, and any other publically available information to harass or harm that person. Already, a New York Times exposé revealed that a company specializing in FRT, *Clearview AI*, has aggregated over three billion images scraped from publically accessible media, including Facebook, YouTube, and Venmo, to create a database of online identities matched with images of those individuals that can be used for facial recognition. *Clearview AI* has allegedly provided this service to over 600 law enforcement agencies, allowing identification of virtually any individual in an image so long as that individual maintains an online presence.

One can also imagine highly invasive public uses of this technology by a regime that places surveillance cameras in all public areas to constantly aggregate information on the behavior of individuals, and sort that information by identity. In effect, application in this manner would create a database of where each person was, what their actions were, and who they were with any time they enter a public space. In conjunction with private technology in the home, e.g. one’s smartphone, the same FRT could expand this database to include the behavior of that individual in private. This use of FRT for surveillance is already becoming commonplace in China, in which a vast network of over 300 million public-facing closed circuit surveillance cameras, coupled with advanced FRT, has been used to monitor its population for criminal conduct or dissident behavior. China's government aims to couple the video data collected by these surveillance cameras with other personal data collected on citizens, including criminal and medical records, travel bookings, online purchases, and social media comments, to create a comprehensive government profile of each citizen. Such invasive use of this technology highlights the potential for FRT to be used in manners that

disregard personal privacy and suppress the exercise of expressed fundamental rights championed by the United States as a whole and California in particular.

(*Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges*, Assembly Committee on Privacy and Consumer Protection (Mar. 10, 2020) *available at* https://privacycp.assembly.ca.gov/sites/privacycp.assembly.ca.gov/files/FRT_Hearing_Background_3_10_20.pdf.)

8) **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. Another priority of the Committee is ensuring that the State's laws protect our immigrant neighbors from federal policies that make them vulnerable to being separated from their families, imprisoned, and ultimately returned to countries that many were often forced to flee from for their own safety. The answer to this question is "yes." Returning the moratorium on the use of FRT on these cameras and the data they generate provides the only guarantee that tools designed to increase police accountability are not turned in to tools of mass surveillance.

1. *Allowing law enforcement to use FRT is contrary to the policy direction of the Legislature in recent years and likely violates the state's laws prohibiting discrimination on the basis of race and gender.* As noted previously in recent years, it has been a priority of the Legislature to end the racial violence and injustice that appears to be endemic in the criminal legal system as a whole, and specifically, in policing. By analyzing the results of FRT systems, experts continue to determine that there is a significant risk of a Black man being misidentified by FRT. Given the continued bias in the system, it is likely that allowing the use of FRT on any photographs, much less on images from a body-worn camera, will likely exacerbate biased policing, potentially with tragic outcomes. Therefore, the Committee finds that continuing the moratorium as the technology evolves is consistent with policymaking in this area.

2. *Allowing law enforcement to use FRT puts vulnerable Californians and visitors to California at risk.* There are a suite of bills in the Legislature this year, several of them being heard in this Committee today, to insure that proper protections are in place for people traveling from out of state seeking sanctuary in California for abortion and gender affirming care, protection from federal immigration authorities, or fleeing the large number of states that have introduced or passed anti-LBGTQ+ laws. This bill, while not prohibiting the use of all FRT, is in keeping with those efforts.

3. *Prohibiting v. regulating the use of FRT.* This year, the Legislature is asked once again to determine whether the investigatory benefits of facial recognition technology outweigh the risk to the communities served by law enforcement. This bill would prohibit 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 or any other camera.

In contrast, AB 642 (Ting) would set minimum standards for the use of facial recognition technology by law enforcement, including requiring a law enforcement agency to have

written policy governing FRT use, allowing for FRT use to identify both individuals who are suspects in a crime and those that are not, 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. AB 642 does not include any limitation on the source of the input image to be identified against the database of persons. Police could use traffic cameras, CCTV, and images from body-worn cameras or dashboard cameras. In addition, AB 642 would allow any new facial recognition technology to be adopted by law enforcement, including technology that will run facial recognition on body-worn cameras in real time and immediately send the results to the officer wearing the camera in real time. AB 642 would permit more input images from more sources than this bill would ban—the two bills could be reconciled.

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, it appears not.

In addition, the Legislature might want to consider if it is appropriate to continue allowing law enforcement to use surveillance technology of this type at all. Given what appears to be the widespread misuse and disregard for the laws that have been in place for almost a decade limiting the use of Automated License Plate Reader (ALPR) technology, even if the Legislature were to regulate the use of FRT, as proposed in AB 642 (Ting), it is no guarantee that the privacy rights of Californians and those seeking refuge in California will be protected. (Please see this Committee's analysis of AB 1463 for a detailed discussion of the use of ALPR.)

9) **Facial Recognition Technology Legislation in California**. In 2019, the Legislature passed AB 1215 (Ting, Chap. 579, Stats. 2019), which banned the use of facial recognition technology and other biometric surveillance systems in connection with cameras worn or carried by law enforcement, including body-worn cameras (BWC), for the purpose of identifying individuals using biometric data. This ban covered both the direct use of biometric surveillance by a law enforcement officer or agency, as well as a request or agreement by an officer or agency that another officer or agency, or a third party, use a biometric surveillance system on behalf of the requesting party. The ban also included narrow exceptions for processes that redact a recording prior to disclosure in order to protect the privacy of a subject, and the use of a mobile fingerprint-scanning device to identify someone without proof of identification during a lawful detention, as long as neither of these functions result in the retention of biometric data or surveillance information. AB 1215 included a sunset date of January 1, 2023.

SB 1038 (Bradford), of the 2021-2022 Legislature, would have extended the ban on biometric surveillance and facial recognition systems in connection with cameras worn or carried by officers indefinitely. At its core, the question involved balancing the purported investigatory benefits of facial recognition technology against its demonstrated privacy risks, technical flaws and racial and gender biases. Senate Public Safety Committee staff did not identify or receive any evidence demonstrating that the ban on facial recognition technology used in connection with body worn cameras had significantly hampered law enforcement efforts in the two years since it became operative. (Sen. Comm. on Public Saf., com. on Sen. Bill No. 1038 (2021-2022 Reg. Sess.).) SB 1038 failed passage in the Senate.

10) **Related legislation (in addition to bills in #9).** AB 642 (Ting), would authorize law enforcement to use facial recognition technology to identify a witness to a crime or a suspect in alleged criminal behavior where reasonable suspicion exists that a crime has been or is being committed and the person whose image is being analyzed is the person who has committed or is committing the crime. AB 642 will be heard today in this Committee.

AB 1281 (Chau, Chap. 268, Stats. 2020) requires a business in California that uses facial recognition technology to disclose that usage in a physical sign that is clear and conspicuous at the entrance of every location that uses facial recognition technology.

SB 21 (Hill, 2017) would have required local law enforcement agencies to have a policy, approved by the local governing body, in place before using surveillance technology. SB 21 was held in the Assembly Appropriations Committee.

AB 69 (Rodriguez, Chap. 461, Stats. 2015) required law enforcement agencies to follow specified best practices when establishing policies and procedures for downloading and storing data from body-worn cameras.

SB 34 (Hill, Chap. 532, Stats. 2015) imposed a variety of security, privacy and public hearing requirements on the use of automated license plate recognition systems, as well as a private right of action and provisions for remedies.

ARGUMENTS IN SUPPORT. A large coalition of over 50 civil rights and social justice organizations write in support of this bill as it is currently in print:

> Police body cameras were intended to guard against police misconduct, not to be exploited for surveillance of Californians. The only responsible standard for facial recognition on body cameras is a prohibition.
>
> Body cameras that automatically scan the faces of Californians will facilitate more profiling, stops, and placement of Black and Brown people into face surveillance databases, further feeding a cycle of racially biased policing and incarceration. To date, at least four Black men have been wrongly arrested and accused of crimes because of facial recognition errors and misuse. Body cameras produce low-quality footage that is blurry, skewed, and in near-constant motion. According to research by the National Institute of Standards and Technology (NIST), facial recognition was up to 100 more times likely to misidentify Asian and Black people. Facial recognition-enabled body cameras will result in more false identifications and arrests.
>
> Face scanning body cameras would also suppress civic engagement and inspire fear. The widespread use of face recognition on police body cameras would be the equivalent of requiring every person to show their photo ID to every police officer they pass. People who do not want their identities and locations recorded and potentially shared with out-of-state agencies will be discouraged from seeking reproductive healthcare, attending protests, or reporting public safety issues.
>
> From 2020 to 2023, a California law prohibited law enforcement from using biometric surveillance systems in connection with an officer camera, thereby protecting people going about their daily lives, upholding the constitutional guarantees of freedom of speech and movement, and preventing misidentification.

ARGUMENTS IN OPPOSITION. Over 20 law enforcement organizations have written in opposition to the bill as it is currently in print, expressing similar sentiments to the ones expressed by the Peace Officers Research Association of California in their letter:

> We regret to inform you of our opposition to AB 1034 regarding law enforcement: facial recognition and other biometric surveillance.
>
> Would prohibit a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. The bill would authorize a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition. The bill would repeal these provisions on January 1, 2034.
>
> PORAC opposes prohibiting law enforcement from installing, activating, or using any biometric surveillance system.

REGISTERED SUPPORT / OPPOSITION:

Support

Access Reproductive Justice
ACLU California Action
Asian Americans Advancing Justice - Asian Law Caucus
California Immigrant Policy Center
California Innocence Coalition: Northern California Innocence Project, California Innocence Project, Loyola Project for The Innocent
California Latinas for Reproductive Justice
California Public Defenders Association (CPDA)
Cancel the Contract
Citizens for Choice
Clue (clergy and Laity United for Economic Justice)
Communities United for Restorative Youth Justice (CURYJ)
Council on American-Islamic Relations, California
Courage Campaign
Drug Policy Alliance
Electronic Frontier Foundation
Ella Baker Center for Human Rights
Fight for The Future
If/When/How: Lawyering for Reproductive Justice
Initiate Justice
Initiate Justice Action
Lawyers Committee for Civil Rights of The San Francisco Bay Area
Legal Services for Prisoners With Children
Media Alliance
MediaJustice
MPower Change
Muslim Democrats and Friends
National Action Network
Oakland Privacy
Orange County Rapid Response Network

Partnership for The Advancement of New Americans
People's Budget Orange County
Policing Project At NYU Law School
Policy Link
Resilience Orange County
San Francisco Public Defender - Racial Justice Committee
San Francisco Public Defender's Office
San Jose Nikkei Resisters
Secure Justice
Silicon Valley De-bug
Sister Warriors Freedom Coalition
St. James Infirmary
Stop the Musick Coalition
Support Life Foundation
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

Opposition

Arcadia Police Officers' Association
Burbank Police Officers' Association
California Coalition of School Safety Professionals
California Police Chiefs Association
California State Sheriffs' Association
Claremont Police Officers Association
Corona Police Officers Association
Culver City Police Officers' Association
Deputy Sheriffs' Association of Monterey County
Fullerton Police Officers' Association
League of California Cities
Los Angeles County Professional Peace Officers Association
Los Angeles County Sheriff's Department
Los Angeles Police Protective League
Los Angeles School Police Officers Association
Murrieta Police Officers' Association
Newport Beach Police Association
Palos Verdes Police Officers Association
Peace Officers Research Association of California (PORAC)
Placer County Deputy Sheriffs' Association
Pomona Police Officers' Association
Riverside Police Officers Association
Riverside Sheriffs' Association
Santa Ana Police Officers Association
Upland Police Officers Association

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