SENATE COMMITTEE ON PUBLIC SAFETY

Senator Nancy Skinner, Chair
2019 - 2020 Regular

Bill No:	AB 1215	**Hearing Date:**	June 11, 2019
Author:	Ting		
Version:	April 25, 2019		
Urgency:	No	**Fiscal:**	No
Consultant:	GC		

Subject: ***Law Enforcement: Facial Recognition and Other Biometric Surveillance***

HISTORY

Source: American Civil Liberties Union of California

Prior Legislation: SB 21 (Hill), 2017 held in the Assembly Appropriations
AB 69 (Rodriguez) Ch. 461, Stats. of 2015

Support: API Chaya; Anti Police-Terror Project; Asian Law Alliance; California Attorneys for Criminal Justice; California Civil Liberties Advocacy; California Immigrant Policy Center; California Public Defenders Association; Center for Media Justice; Color of Change; Council on American-Islamic Relations of California; Data for Black Lives; Defending Rights and Dissent; Electronic Frontier Foundation; Fight for the Future; Indivisible CA; Justice Teams Network; Media Alliance; Oakland Privacy; RAICES; San Jose/Silicon Valley NAACP; Secure Justice; National Association of Criminal Defense Lawyers; Library Freedom Project; Tor Project; X-Lab

Opposition: California Police Chiefs Association; California State Sheriffs' Association; CSAC Excess Insurance Authority; Los Angeles County Sheriff; Peace Officers' Association of California (PORAC); Riverside Sheriffs' Association

Assembly Floor Vote: 45 - 17

PURPOSE

The purpose of this bill is to prohibit law enforcement from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other camera.

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

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

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

Existing law encourages agencies to consider best practices in establishing the length of time that recorded data is to be stored. States that nonevidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of 60 days, after which it may be erased, destroyed, or recycled. Provides that an agency may keep data for more than 60 days to have it available in case of a civilian complaint and to preserve transparency. (Pen. Code, § 832.18, subd. (b)(5)(A).)

Existing law states that evidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of two years under any of the following circumstances:

1) The recording is of an incident involving the use of force by a peace officer or an officer-involved shooting;
2) The recording is of an incident that leads to the detention or arrest of an individual; or,
3) The recording is relevant to a formal or informal complaint against a law enforcement officer or a law enforcement agency. (Pen. Code, § 832.18, subd. (b)(5)(B).)

Existing law states that the recording should be retained for additional time as required by law for other evidence that may be relevant to a criminal prosecution. (Pen. Code, § 832.18, subd. (b)(5)(C).)

Existing law 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, subd. (b)(5)(D).)

Existing law encourages agencies to adopt a policy that records or logs of access and deletion of data from body-worn cameras should be retained permanently. (Pen. Code, § 832.18, subd. (b)(5)(E).)

Existing law encourages agencies to include in a policy information about where the body-worn camera data will be stored, including, for example, an in-house server which is managed internally, or an online cloud database which is managed by a third-party vendor. (Pen. Code, § 832.18, subd. (b)(6).)

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

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

Existing law 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. (Civil Code, § 1798.90.55.)

Existing law prohibits a local agency from acquiring cellular communications interception technology unless approved by its legislative body. (Gov. Code, § 53166, subd. (c)(1).)

Existing law permits a court to award attorney fees to a successful party against one or more opposing parties in any action which has resulted in the enforcement of an important right affecting the public interest if: (a) a significant benefit, whether pecuniary or nonpecuniary, has been conferred on the general public or a large class of persons, (b) the necessity and financial burden of private enforcement, or of enforcement by one public entity against another public entity, are such as to make the award appropriate, and (c) such fees should not in the interest of justice be paid out of the recovery, if any. With respect to actions involving public entities, this section applies to allowances against, but not in favor of, public entities, and no claim shall be required to be filed therefor, unless one or more successful parties and one or more opposing parties are public entities, in which case no claim shall be required to be filed. (Code of Civ. Proc., § 1021.5.)

This bill states that a law enforcement agency or law enforcement official shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera.

This bill defines "biometric data" to mean "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."

This bill defines "biometric surveillance system" to mean "any computer software or application that performs facial recognition or other biometric surveillance."

This bill declares that facial recognition and other biometric surveillance technology pose unique and significant threats to the civil rights and civil liberties of residents and visitors. Declares that the use of facial recognition and other biometric surveillance is the functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights. States that this technology also allows people to be tracked without consent and would also generate massive databases about law-abiding Californians, and may chill the exercise of free speech in public places.

COMMENTS

1. Need for This Bill

According to the author of this bill:

> In response to public concern over police-involved shootings, agencies across the state have implemented body camera programs to help increase accountability and mend trust with the communities they are sworn to protect. However, technology has been developed to allow for facial recognition and biometric scanning in body cameras, which can lead to dire consequences for Californians.
>
> This technology has the potential to subject law-abiding citizens to perpetual police line-ups, tracking their movements without their consent, and creating new databases susceptible to exploitation and hacking undermines public trust and the effectiveness of law enforcement, threatens the safety of Californians, and unduly intrudes on constitutional rights to privacy. AB 1215 would ban law enforcement agencies and officials from using, installing, or activating facial recognition and biometric scanners in body cameras in order to protect Californians from unnecessary and potentially dangerous surveillance.

2. Facial Recognition Surveillance

Facial recognition has drastically improved in recent years through machine learning called "deep learning." This system is based on the analysis of facial features then a comparison of that analysis with labeled faces in a database. However, there are concerns because the systems fail to accurately identify and recognize persons with dark complexions and women to the same degree the systems correctly identify males with fair complexions.

According to the author, "Facial recognition applies computer software that automatically converts the unique features on a person's face into a mathematical code, called a faceprint. But unlike other biometric identifiers like fingerprints or DNA, facial recognition technology allows faceprints to be taken without our permission or knowledge, with no way to opt-out – taking away an individual's longstanding legal right to protect their identity if they haven't done anything wrong…

"Law enforcement body cameras coupled with facial recognition software would transform thousands of individual cameras carried by law enforcement officers into roving surveillance devices that record who we are, where we go, and where we have been over time – from the homes of friends, to medical offices, therapists, places of worship, and political gatherings. Such constant and pervasive surveillance would not only corrupt the purpose of body cameras, it would undermine trust in law enforcement and discourage victims and vulnerable groups from seeking help. Errors could result in false accusations or the inappropriate use of force, with potentially tragic consequences."

In January, 85 privacy advocacy groups wrote a letter to Amazon, Google and Microsoft requesting that the companies pledge not to sell facial recognition technology to the government.[1] "We are at a crossroads with face surveillance, and the choices made by these companies now will determine whether the next generation will have to fear being tracked by the government for attending a protest, going to their place of worship, or simply living their lives," said Nicole Ozer, technology and civil liberties director for the American Civil Liberties Union of Northern California.[2]

Use of facial recognition by law enforcement has been particularly pronounced in China. The *Washington Post* reported in May 2018 that a man was plucked from a crowd of 20,000 concertgoers after passing through security.[3] "Facial recognition cameras at a stadium led to the arrest of a fugitive at a Jacky Cheung concert in China, making it the third time in two months that the technology was used to catch a wanted person at one of the pop star's concerts."

Google recognizes that facial recognition technology poses unique concerns, posting on its blog titled "Google in Asia" that "Google has long been committed to the responsible development of [artificial intelligence]. These principles guide our decisions on what types of features to build and research to pursue. As one example, facial recognition technology has benefits in areas like new assistive technologies and tools to help find missing persons, with more promising applications on the horizon. However, like many technologies with multiple uses, facial recognition merits careful consideration to ensure its use is aligned with our principles and values, and avoids abuse and harmful outcomes. We continue to work with many organizations to identify and address these challenges, and unlike some other companies, Google Cloud has chosen not to offer general-purpose facial recognition [application programing interfaces] before working through important technology and policy questions."[4]

3. Accuracy of Facial Recognition

The U.S. Commerce Department released a report in November 2018. The report found that the entire facial recognition industry improved massively. The report showed that at least 28 developers' algorithms now outperform the most accurate algorithm from late 2013, and just 0.2 percent of all searches by all algorithms tested failed in 2018 compared with a 4 percent failure rate in 2014 and a 5 percent rate in 2010.

However, the American Civil Liberties Union reported last year that facial recognition software is, at best, inaccurate and at worst, "flawed, biased and dangerous." [5] "The errors emerged as part of a larger test in which the civil liberties group used Amazon's facial software to compare the

---

[1]Available at: https://www.aclu.org/coalition-letter-amazon-urging-company-commit-not-release-face-surveillance-product

[2]Makena Kelly, *Google, Amazon, and Microsoft Face New Pressure Over Facial Recognition Contracts*, The Verge, January 15, 2019, Available at: https://www.theverge.com/2019/1/15/18183789/google-amazon-microsoft-pressure-facial-recognition-jedi-pentagon-defense-government

[3] Hamza Shaban, *Facial Recognition Cameras in China Snag Man who Allegedly Stole $17,000 Worth of Potatoes*, Washington Post, May 22, 2018, Available at: https://www.washingtonpost.com/news/innovations/wp/2018/05/22/facial-recognition-cameras-lead-to-arrest-of-a-man-wanted-for-allegedly-stealing-17000-worth-of-potatoes/?utm_term=.cd62c7d10735.

[4]Kent Walker, *AI for Social Good in Asia Pacific*, Google in Asia, December 13, 2018, Available at: https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/amp/.

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

photos of all federal lawmakers against a database of 25,000 publicly available mug shots. In the test, the Amazon technology incorrectly matched 28 members of Congress with people who had been arrested, amounting to a 5 percent error rate among legislators. The test disproportionally misidentified African-American and Latino members of Congress as the people in mug shots."[6]

Countering ACLU's concerns, Nina Lindsey, an Amazon Web Services spokeswoman, said in a statement that the company's customers had used its facial recognition technology for various beneficial purposes, including preventing human trafficking and reuniting missing children with their families, and said that police departments should utilize the technology differently than the ACLU did during its testing of the system's accuracy. Lindsey added that, "police departments do not typically use the software to make fully autonomous decisions about people's identities. 'It is worth noting that in real-world scenarios, Amazon Rekognition is almost exclusively used to help narrow the field and allow humans to expeditiously review and consider options using their judgment.'" Lindsey also said that the "confidence threshold" ACLU used for its test, 80 percent confidence score, was lower than what law enforcement should use, a 95 percent confidence score.

Still, even manufacturers of the technology recognize that it is flawed. In August 2018, *Gizmodo* reported that Rick Smith, the CEO of Axon, one of the largest body camera manufacturers in the U.S., said the company was not implementing facial recognition software into their products, yet.[7] Smith said on a call to shareholders that privacy and policy concerns regarding the accuracy of face recognition was the cause for pause: "The 'accuracy thresholds,' Smith said on the call, aren't 'where they need to be to be making operational decisions off the facial recognition.'"[8]

4. Fourth Amendment

The Fourth Amendment to the United States Constitution grants the following right to all citizens of the United States:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The American Civil Liberties Union of California writes that, "The Fourth Amendment to the US Constitution prohibits police from demanding identification without suspicion. The US Supreme Court has held, that absent specific statutory authority and limitations, there is no justification for police officers to arrest a suspect who refused to identify herself to authorities. *Hiibel v. Sixth Judicial District Court of Nevada*, 542 U.S. 177; 2004. At one time, California did have a statute, former California Penal Code Section 647 (e), permitting police officers to question people who were loitering on the streets about their identity. However, that statute was repealed after it was determined to be unconstitutional. That case, Lawson v. Kolender, 461 U.S. 352 (1983), involved a black man who was repeatedly asked to identify himself to police for doing nothing more than walking in so-called white neighborhoods.

---

[6] Id.
[7] Sidney Fussell, *Axon CEO Says Face Recognition Isn't Accurate Enough for Body Cams Yet*, Gizmodo, August 8, 2018, Available at: https://gizmodo.com/axon-ceo-says-face-recognition-isnt-accurate-enough-for-1828205723.
[8] Id.

"By prohibiting the use of facial recognition software on police body cameras, AB 1215 (Ting) codifies the US Supreme Court's recognition that, absent valid legal reasons, Californians may not be required to identify themselves to government officials.

"Our country appropriately values the freedom to walk down the street without being compelled to identify ourselves to law enforcement. Such liberty is one of the differences between this country and others. Governments in China, for example, subject residents to intense surveillance and scrutiny using public face surveillance systems.

"In addition to codifying existing privacy protections, there are other compelling civil rights justifications for preventing the implantation of facial recognition software on police body cameras."

5. Investigatory Benefits of Facial Recognition Technology

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, MD.[9]

This bill asks the Legislature whether it is ever appropriate to permit the use of facial recognition technology for investigatory purposes. There are no exceptions to the ban on using facial recognition software.

Opponents of the bill point to the fact that many large events occur in California and that this bill would make Californians less safe. For instance, Los Angeles is set to host the Olympics in 2028. California will host athletes, dignitaries, and travelers from across the globe. This bill will prevent the use of facial recognition technology and events such as the Olympics in California.

6. San Francisco Ban on Facial Recognition Technology

San Francisco has become the first city in the United States to prohibit its government from using facial-recognition technology in May of this year. The San Francisco Board of Supervisors passed the ban as a part of a broader anti-surveillance ordinance.[10] The ban prohibits the use of facial-recognition technology by police and other governmental departments. The San Francisco ban exempts federally controlled facilities at San Francisco International Airport and the Port of San Francisco.

7. Previous Legislative Efforts in the Area of Facial Recognition in California

In 2017, Senator Hill introduced SB 21 which 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.

---

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

[10] https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A

8. Argument in Support

According to the American Civil Liberties Union of California:

> People should be able to walk down the street without being forced to identify themselves for no reason. The US Supreme Court has concluded, that absent specific statutory authority, there is no constitutional justification for police officers to compel a person to identify herself to authorities. *Hiibel v. Sixth Judicial District Court of Nevada*, 542 U.S. 177 (2004). At one time, California did have a statute, former California Penal Code Section 647 (e), permitting police officers to question people who were loitering on the streets about their identity. However, that statute was repealed after it was determined to be unconstitutional. That case, *Lawson v. Kolender*, 461 U.S. 352 (1983), involved a black man who was repeatedly asked to identify himself to police for doing nothing more than walking in so-called white neighborhoods.
>
> The public deployment of facial recognition-enabled body cameras would be like requiring people to constantly carry and display a photo ID card, which would be an unacceptable mass violation of privacy. By preventing the use of such technology with officer body cameras, AB 1215 (Ting) codifies the U.S. Supreme Court's recognition that, absent valid and clear legal reasons, Californians may not be required to identify themselves to government officials.
>
> Our country appropriately values the freedom to walk down the street without being compelled to identify ourselves to law enforcement. Such liberty is one of the differences between this country and others. Governments in China, for example, subject residents to intense surveillance and scrutiny using public face surveillance systems
>
> Police body cameras were promised as a way to reduce and document unjustified police violence, strengthen police-community relations, and improve trust. They were not promised as an additional prosecutorial tool for law enforcement. And they were not designed to turn California into a scene from the movie *Minority Report*, where facial recognition helps fuel arrests based on potential future actions. Police have no right to automatically record who we are and where we go -- from the homes of friends, to medical offices, therapists, places of worship, and political gatherings. Embedding facial recognition into body cameras would be a sweeping transformation of those devices into dragnet surveillance networks.
>
> If police officers can use facial recognition software on body cameras, the consequences for Californians will be grave. This use is not an imagined threat. The Financial Times recently reported that one body camera company, Axon, has filed for a facial recognition patent that would enable the real-time tracking and identification of people passing by an officer. If a body camera with facial recognition notifies a police officer that a person has a prior conviction or mislabels that person as a "threat" based on a secretive corporate algorithm, police may engage that person with potentially tragic consequences.

Flaws in facial recognition systems raise the risk of such harms. Facial recognition technology has been shown to be inaccurate, particularly as to women and people of color. Peer-reviewed academic research by researchers at MIT has demonstrated that prominent facial recognition technology products perform more poorly for people with darker skin and for women. In fact, when ACLU ran photos of members of Congress through Amazon's "Rekognition" face surveillance product, 28 members of Congress incorrectly "hit" with mugshot booking photos of arrestees. Of the false matches, 39 percent were people of color, although people of color make up only 19 percent lawmakers of color in Congress.

Using Rekognition in that way, former California legislators (and current Congress members) Mark DeSaulnier, Steve Knight, Jimmy Gomez, and Norma Torres would all be subject to potential arrest for just walking down the street in the vicinity of a police officer with a body camera. If a police body camera with face surveillance misidentified a person, that error could misinform or bias an officer's decision about how to approach a person or even use deadly force. Moreover, fear of misidentification or being added to a government photo face-surveillance database may cause people to avoid seeking and offering assistance to police.

Facial recognition-enabled body cameras will make us less safe *and* less free.

In a March 2019 poll of likely 2020 California voters, 62% of respondents agreed that body cameras should be used *solely* "to record how police treat people and provide a tool for public oversight and accountability" rather than "to give law enforcement a tool to identify and track people." In that same poll, 82% of likely 2020 voters said they disagree with the government being able to monitor and track a person using biometric information. Concerns about the use of face and other biometric information by the government, on public cameras, such as officer-worn body cameras, is consistent across Democrats, Republicans, and Independents, both men and women, in all regions of Californian, across generations.

9. Argument in Opposition

According to the Riverside Sheriffs' Association:

On behalf of the thousands of members of the Riverside Sheriffs' Association, we regret that we must oppose AB 1215, a bill that will significantly impair the ability of law enforcement to protect the public. This measure prohibits the use of facial recognition software in conjunction with law enforcement body-worn camera video.

While the bill properly acknowledges the importance of privacy rights, it erroneously presumes that persons in public possess or are afforded a reasonable expectation of privacy. Moreover, the U.S. Supreme Court has repeatedly held that no reasonable expectation of privacy exists for persons on public streets or in public places.

The proponents of AB 1215 contend that police body-worn-camera footage captures too many members of the public without cause or justification.

Additionally, the proponents contend that persons in public may be more easily identified via police body-worn cameras if the recording were filtered through facial recognition.

These arguments were not raised during debates last session, when supporters of AB 1215 advocated in favor of the passage of AB 66 (Weber) and AB 748 (Ting) which established the requirements for public disclosure of law enforcement body worn camera video.

Now, proponents seem to want to have their cake and eat it too. They supported body cameras to hold officers accountable, hoping to capture video of officers doing something wrong. The anti-police lobby never spoke a word of concern about the "privacy rights" of officer, whose every action and word uttered would become subject to public disclosure. If these civil libertarians were so willing to infringe upon the "privacy rights" of sworn law enforcement officers, why, then, would it now be inappropriate for the same police body cameras to capture recordings of wanted persons or convicted criminals?

Another principal argument in favor of AB 1215 seems to be that facial recognition software is too unreliable and may misidentify persons recorded on the body cams. This argument, however, is just another red herring.

Our state has been a world leader in the development and advancement of technology. Californians do not have a history of banning technology until it is perfected. Could any of us imagine a statutory ban on Microsoft Office or Apple's iOS until the software was able to be certified as100% flawless?

Similarly, when it comes to driverless / auto-pilot cars, this legislature has not banned such vehicles due to the risk of a deadly collision. Instead, we have decided to regulate these cars for the safety of our residents, despite the possibility of traffic-related deaths.

Proponents have not identified a compelling reason to prohibit the use of this software with the body cameras. They have inadvertently however, raised legitimate questions of the need for oversight and regulation of this developing technology.

If AB 1215 instead sought to establish minimum standards and policies related to the use of facial recognition in conjunction with body camera video, we could then discuss the issues of privacy and legitimate law enforcement usage, working together towards a compromise that would protect privacy and the public.

Huge events such as the annual Coachella Music and Arts Festival, the upcoming Los Angeles Olympics, World Cup Soccer Tournament, Rose Bowl, Disneyland and scores of popular tourist attractions should have access to the best available security-including the use of body cameras and facial recognition technology. By banning this technology, California will be announcing to the nation and world

that it doesn't want our law enforcement officers to have the necessary tools they need to properly protect the public and attendees of these events.

-- END –