SENATE COMMITTEE ON PUBLIC SAFETY

Senator Nancy Skinner, Chair
2017 - 2018 Regular

Bill No:	SB 1186	**Hearing Date:**	April 3, 2018
Author:	Hill		
Version:	February 15, 2018		
Urgency:	No	**Fiscal:**	Yes
Consultant:	GC		

Subject: ***Law Enforcement Agencies: Surveillance: Policies***

HISTORY

Source: Author

Prior Legislation:
SB 21 (Hill) Failed passage in Assembly Appropriations – 2016
SB 868 (Jackson) Failed Assm. Privacy and Consumer Protection 2016
SB 34 (Hill) Ch. 532, Stats. 2015
SB 167 (Gaines) Not heard 2015
SB 170 (Gaines) Vetoed 2015
SB 262 (Galgiani) Failed Senate Judiciary 2015
SB 263 (Gaines) Not heard 2015
SB 271 (Gaines) Vetoed 2015
SB 741 (Hill) Ch. 741, Stats. 2015
AB 56 (Quirk) Inactive Senate Floor
SB 15 (Padilla) Failed Assembly Public Safety 2014
AB 1327 (Gorell) Vetoed 2014

Support: Unknown

Opposition: Association of Orange County Deputy Sheriffs; California Association of Code Enforcement Officers; California College and University Police Chiefs Association; California District Attorneys Association; California Narcotics Officers Association; California Peace Officers' Association; California Public Defenders Association; California State Sheriffs' Association; California Statewide Law Enforcement Association; Fraternal Order of Police; Long Beach Police Officers Association; Los Angeles County Professional Peace Officers Association; Los Angeles County Sheriff's Department; Los Angeles Police Protective League; Sacramento County Deputy Sheriffs' Association; San Bernardino County Sheriff

PURPOSE

The purpose of this bill is to require local law enforcement agencies to have a policy, approved by the local governing body, in place before using surveillance technology as defined.

Existing law authorizes certain persons who are not peace officers to exercise the powers of arrest under certain circumstances, if they have completed a specific training course prescribed by the Commission on Peace Officer Standards and Training. (Penal Code § 830.7).

Existing federal regulations require all drone owners to register their drones with the Federal Aviation Administration (FAA). Commercial drone operators, but not recreational drone operators, must also obtain FAA authorization, which is granted on a case-by-case basis.

Existing law establishes a Division of Aeronautics within the California Department of Transportation (Caltrans). (Public Utilities Code §§ 21001 et seq)

Existing law prohibits wiretapping or eavesdropping on confidential communications. (Penal Code § 630.)

Existing law makes it a crime for a person, intentionally, and without requisite consent, to eavesdrop on a confidential communication by means of any electronic amplifying or recording device. (Penal Code § 632.)

Existing law makes a person liable for "physical invasion of privacy" for knowingly entering onto the land of another person or otherwise committing a trespass in order to physically invade the privacy of another person with the intent to capture any type of visual image, sound recording, or other physical impression of that person engaging in a personal or familial activity, and the physical invasion occurs in a manner that is offensive to a reasonable person. (Civil Code § 1708.8 (a).)

Existing law makes a person liable for "constructive invasion of privacy" for attempting to capture, in a manner highly offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of another person engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there was a physical trespass, if the image or recording could not have been achieved without a trespass unless the visual or auditory enhancing device was used. (Civil Code § 1708.8 (b).)

Existing law provides that a person who commits an invasion of privacy for a commercial purpose shall, in addition to any other damages or remedies provided, be subject to disgorgement to the plaintiff of any proceeds or other consideration obtained as a result of the violation of this section. Existing law defines "commercial purpose" to mean any act done with the expectation of sale, financial gain, or other consideration. (Civil Code § 1708.8 (d), (k).)

This bill requires, beginning July 1, 2019, that each law enforcement agency submit to its governing body at a regularly scheduled hearing, open to the public, a proposed Surveillance Use Policy for the use of each type of surveillance technology and the information collected.

This bill requires law enforcement agencies to cease using the surveillance technology within 30 days if the proposed plan is not adopted.

This bill requires law enforcement agencies to submit an amendment to the surveillance plan, pursuant to the same open meeting requirements, for each new type of surveillance technology sought to be used.

This bill requires the policy and any amendments to be posted on the agency's website.

This bill requires agencies to make specified reports, at approved intervals, concerning the use of surveillance technology, and to make those reports available on the agency's website.

This bill would prohibit a law enforcement agency from selling, sharing, or transferring information gathered by surveillance technology, except to another law enforcement agency, as permitted by law and the terms of the Surveillance Use Policy.

This bill would provide that any person could bring an action for injunctive relief to prevent a violation of these provisions and, if successful, could recover reasonable attorney's fees and costs.

This bill would require an agency to discipline an employee who knowingly or intentionally uses surveillance technology in violation of these provisions, as specified.

This bill would authorize an agency to temporarily use surveillance technology during exigent circumstances without meeting the requirements of these provisions, provided that, among other things, the agency submits a specified report to its governing body within 45 days of the end of the exigent circumstances.

This bill would establish separate procedures for a sheriff's department or a district attorney to establish their own Surveillance Use Policies, instead of submitting them through their governing body. The procedures would include holding a noticed public hearing on the proposed policy, posting the policy on the department's website, amending the policy to include new types of surveillance technology, and publishing a biennial report regarding the department's use of surveillance technology.

This bill would also establish procedures for the Department of the California Highway Patrol (CHP) and the Department of Justice (DOJ) to establish their own Surveillance Use Policies. The bill would, among other things, require that these agencies ensure that the collection, use, maintenance, sharing, and dissemination of information or data collected with surveillance technology is consistent with respect for individual privacy and civil liberties, and that the policy be publicly available on the agency's website. The bill would also require that if these agencies intend to acquire surveillance technology, they provide 90 days advance notice on the agency's website.

This bill defines the following terms for the purposes of this section:

- "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of death or serious physical injury to any person requires use of a surveillance technology or the information it provides.

- "Governing body" means the elected body that oversees the law enforcement agency or an appointed overseeing body if there is no elected body that provides direct oversight of the law enforcement agency.

- "Law enforcement agency" means any police department, sheriff's department, district attorney, county probation department, transit agency police department, school district

police department, the police department of any campus of the University of California, the California State University, or community college, the Department of the California Highway Patrol, and the Department of Justice.

- "Surveillance technology" means any electronic device or system with the capacity to monitor and collect audio, visual, locational, thermal, or similar information on any individual or group. This includes, but is not limited to, drones with cameras or monitoring capabilities, automated license plate recognition systems, closed-circuit cameras/televisions, International Mobile Subscriber Identity (IMSI) trackers, global positioning system (GPS) technology, software designed to monitor social media services or forecast criminal activity or criminality, radio frequency identification (RFID) technology, body-worn cameras, biometric identification hardware or software, and facial recognition hardware or software.

- "Surveillance technology" does not include standard public agency hardware and software in widespread public use and not used by the law enforcement agency for any surveillance or surveillance-related functions, such as televisions, computers, printers, parking ticket devices, case management databases, medical equipment used to diagnose, treat, or prevent disease or injury, fingerprint scanners, ignition interlock devices, cellular or standard telephones, and two-way radios, or other similar electronic devices.

This bill finds and declares the following:

- While law enforcement agencies increasingly rely on surveillance technologies because those technologies may enhance community safety and aid in the investigation of crimes, those technologies are often used without any written rules or civilian oversight, and the ability of surveillance technology to enhance public safety should be balanced with reasonable safeguards for residents' civil liberties and privacy.

- Promoting a safer community through the use of surveillance technology while preserving the protection of civil liberties and privacy are not mutually exclusive goals, and policymakers should be empowered to make informed decisions about what kind of surveillance technologies should be used in their community.

- Decisions about whether to use surveillance technology for data collection and how to use and store the information collected should not be made by the agencies that would operate the technology, but by the elected bodies that are directly accountable to the residents in their communities who should also have opportunities to review the decision of whether or not to use surveillance technologies.

COMMENTS

1. Need for This Bill

According to the author:

> California enacted two laws, SB 34 (Hill, 2015) and SB 741 (Hill, 2015), which require law enforcement agencies to develop privacy and use policies for automatic license plate readers (ALPR) systems and a cell-phone intercept

devices. These surveillance technologies are capable of collecting a wide-range of personal information. SB 34 and SB 741 also generally require a public discussion before ALPR systems or cell-phone intercept devices are used by law enforcement agencies.

SB 34 and SB 741 help to balance protecting civil liberties and privacy with law enforcement's ability to use technology to fight crime, but these laws only apply to ALPR systems and cell-phone intercept devices. Similar privacy or transparency standards are not in place for other surveillance technologies used by law enforcement.

A wide array of surveillance technology is available to and used by law enforcement agencies. The Washington Post reported in 2016 that the "number of local police departments that employ some type of technological surveillance increased from 20 percent in 1997 to more than 90 percent in 2013.[1]
The increased use of surveillances technology has serious implications for civil liberties and privacy. Surveillance technology allows law enforcement agencies to capture detailed information about where people go, who they associate with, and what they say. Protections should be established to ensure surveillance devices are only used for their intended purposes, to catch criminals and fight crime, and not to collect vast amounts of data on non-criminal residents.
Surveillance technology law enforcement agencies are utilizing includes but is not limited to the following:

- *Facial recognition*: Facial recognition uses software to compare a person's photo to databases like those maintained by the Department of Motor Vehicles which hold driver's license photos. According to the Georgetown University School of Law, "nearly half of all American adults have been entered into law enforcement facial recognition databases."[2] Facial recognition is widely used by California law enforcement agencies. In San Diego alone there are 433 devices used by 991 law enforcement personnel.[3] All law enforcement agencies in Los Angeles County have access to facial recognition software.

- *Social media scrubbers:* Products like Geofeedia and Media Sonar allow law enforcement agencies to monitor online activity (e.g. Facebook and Twitter posts). At least 21 law enforcement agencies across the state use social media scrubbers. This technology is often deployed to monitor protest events. For example, Oakland Police admitted to using the technology to monitor Black Lives Matter protests.

---

[1] Jouvenal, Justin. "The new way police are surveilling you: Calculating your threat score." *The Washington Post*, WP Company, 10 Jan. 2016, www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.
[2] Sydell, Laura. "It Aint Me, Babe: Researchers Find Flaws In Police Facial Recognition Technology." *NPR*, NPR, 25 Oct. 2016, www.npr.org/sections/alltechconsidered/2016/10/25/499176469/it-aint-me-babe-researchers-find-flaws-in-police-facial-recognition.
[3] Walsh, Tom Jones Lynn. "Use of Facial Recognition Software Increases." *NBC 7 San Diego*, 6 May 2016, www.nbcsandiego.com/investigations/Use-of-Facial-Recognition-Software-By-San-Diego-Law-Enforcement-Increasing--378006081.html.

- *Video surveillance:* This type of surveillance typically involves mounting closed caption cameras on light or utility poles. Many of the cameras are capable of capturing video in 360-degree views for 24 hours a day. Cameras are often capable of zooming and recording sound. At least 61 departments have surveillance cameras, though only 3 of the departments have any type of privacy or use policy.

- *Portable surveillance cameras:* Unlike video surveillance equipment, portable surveillance cameras capture still images rather than continuous footage. These cameras can be placed anywhere and take pictures of any person that crosses their path. The City of Orinda in the Bay Area deployed 13 cameras and over a 90 day period, 5.7 million pictures were taken.[4] It is not known how many law enforcement agencies use the technology statewide, but at least 13 different agencies in the Bay Area deploy them.

- *Portable biometric scanners:* Similar to facial recognition software, biometric scanners come in many forms and can analyze physical characteristics like faces, fingerprints, and retinas. According to the Electronic Frontier Foundation, biometric scanners can be used to capture personal data whether or not someone is suspected for a crime.

- *Drones:* Local law enforcement agencies use drones to perform surveillance. The devices are outfitted with cameras that capture photos and video, which can be transmitted to centralized databases. There are no laws dictating that law enforcement agencies disclose their use of drones or what they are used for.

- *Radar systems:* Radar systems use radio waves to see inside structures like homes or businesses. Originally deployed in war-zones this handheld and highly portable technology can be used by an officer at a distance of over 50 feet to detect whether someone is inside a structure.

- *ALPR systems:* Used primarily by law enforcement agencies on police vehicles, ALPR systems use a combination of high-speed cameras, software, and criminal databases to rapidly check the license plates of millions of Californians. Use of ALPR is subject to the requirements of SB 34 (Hill, 2015).

- *Cell-phone intercept devices:* Commonly known by its brand name "Stingray," Cell-phone intercept device**s** allow law enforcement agencies to mimic a cell phone tower. The device, which is portable and usually the size of a briefcase, can be used to find out who a person is calling, when a call is made, and where a call is made from. In some cases these devices can capture the content of a conversation. The use of this technology is subject to the requirements of SB 741 (Hill, 2015).

[4] Wagner, David Paredes and Liz. "Orinda Surveillance Cameras Violate Privacy, Critics Say." *NBC Bay Area*, NBC Bay Area, 8 Aug. 2016, www.nbcbayarea.com/investigations/Orinda-Surveillance-Cameras-Violates-Privacy-Critics-Say-389333452.html.

2. Current Regulation

The FAA does not permit commercial drone operation except on a case-by-case basis. However, in February 2015, the FAA proposed regulations on commercial drone users. Among the proposals was a 55-pound weight limitation, line-of-sight operation, maximum airspeed of 100 mph, a ban on operation over any people, a maximum operating altitude of 500 feet, and training and licensing for the operator. Those rules have not been finalized but are expected by mid-year. In December 2015, the FAA required commercial and recreational drone users to register their drones. Nearly 300,000 drone users registered within the first 30 days, according to the FAA. This is modest success given the more than 1 million drones in use.

Several California local governments have enacted their own drone regulations. In October 2015, the City of Los Angeles enacted drone regulations similar to the FAA proposal. In December, the city filed the first criminal charges under the ordinance, citing two individuals for operating a drone which interfered with a Los Angeles Police Department air unit, causing it to change its landing path. In northern California, the Golden Gate Bridge, Highway and Transportation District banned drones near the Golden Gate Bridge after a drone crashed on the roadway.

As noted in the author's statement, state law requires law enforcement agencies to develop privacy and use policies if an agency uses either an automatic license plate readers system or a cell-phone intercept device.

3. Requires a Surveillance Use Policy

This bill requires a law enforcement agency that wants to use surveillance technology (technology) to submit a Surveillance Use Policy (policy) to the governing body. The policy should then be heard at an open hearing of the governing body and be published on the agency's website.

The policy shall contain (at minimum) the following:

- Authorized purposes for using the surveillance technology.
- Types of data that can be and is collected by the surveillance technology.
- A description of the job title or other designation of employees and independent contractors who are authorized to use the surveillance technology or to access data collected by the surveillance technology. The policy shall identify and require training for those authorized employees and independent contractors.
- Title of the official custodian, or owner, of the surveillance technology responsible for implementing this section.
- A description of how the surveillance technology will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- The length of time information gathered by the surveillance technology will be retained, and a process to determine if and when to destroy retained information.
- Purposes of, process for, and restrictions on the sale, sharing, or transfer of information to other persons and whether, if so, how the collected information can be accessed by members of the public, including criminal defendants.

- A process to maintain a record of access of the surveillance technology or information collected by the surveillance technology. At a minimum, the record shall include all of the following:
    - The date and time the technology is used or the information is accessed.
    - The data elements the employee used to query the information.
    - The username of the employee who uses the technology or accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.
    - The purpose for accessing the information or using the technology.
- The existence of a memorandum of understanding or other agreement with another local agency or any other party, whether or not formalized, for the shared use of the surveillance technology or the sharing of the information collected through its use, including the identity of the parties.

The policy shall include any technologies already in use.

The policy shall include in separate sections specific to each unique type of surveillance technology, a description of each surveillance technology used by the law enforcement agency.

4. Reports

This bill requires a report that is to be available on the agency's website on the use of any technologies. The governing body and law enforcement agency can agree on the time interval of the report. The bill states that the report shall at minimum contain:

- The acquisition costs for each surveillance technology, as well as the annual operating cost, including personnel costs.
- The total number of times each type of technology was used in the preceding year and the total number of times each type of technology helped apprehend suspects or close a criminal case.
- The total number of times the surveillance technology was borrowed from or lent to another agency, the identity of that agency, and the purposes for which the surveillance technology was shared, including any exigent circumstances.
- The total number of the agency employees trained and authorized to use each type of surveillance technology.
- The total number of times any surveillance technology was used in a manner out of compliance with the agency's Surveillance Use Policy, whether data collected through the use of surveillance technology was inappropriately disclosed, released, or in any other way revealed for a nonapproved reason, and the steps the agency took to correct the error.
- The total costs of the technology; a description of how often it was used; a description of the type of data collected by each technology; the number of times the technology was borrowed or lent to another agency; the number of employees trained and authorized to use each type of technology; and, disclosure on whether the technology was ever used out of compliance with the policy.

5. Exigent circumstances

This bill does allow for the use of a technology which has not had a policy approved for or was not included in the policy under exigent circumstances. 45 days after the use, the agency must

report its use to the governing body as well as submit an amendment to the policy. It also requires the technology use to be included in the report.

This seems to presuppose a policy in place for at least some technology. What about a jurisdiction in which the governing board has explicitly prohibited the use of the technology or explicitly limited what technologies can be used?

6. Argument in Opposition

According to the State Sheriffs' Association:

> This bill will dangerously provide a roadmap to criminals as to how and when law enforcement agencies deploy surveillance technology and techniques. SB 1186 requires the surveillance policy, among other things, to detail the types of surveillance used, what data can be and are collected by the technology, and how the surveillance technology is monitored for security. The risk involved in publicizing this sensitive information dwarfs any perceived benefit emanating from the desire to inform the public about how law enforcement operates as it relates to lawful surveillance techniques.

-- END –