SENATE COMMITTEE ON PUBLIC SAFETY

Senator Nancy Skinner, Chair
2017 - 2018 Regular

Bill No:	SB 21	**Hearing Date:**	March 21, 2017
Author:	Hill		
Version:	March 14, 2017		
Urgency:	No	**Fiscal:**	Yes
Consultant:	MK		

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

HISTORY

Source: Author

Prior Legislation: 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: California Attorneys for Criminal Justice; California Civil Liberties Advocacy; California Public Defenders Association

Opposition: ACLU of California (unless amended); Asian Americans Advancing Justice - Asian Law Caucus (unless amended); Asian Law Alliance (unless amended); California District Attorneys Association; California Police Chiefs Association, California State Sheriffs' Association; Center for Media Justice (unless amended); Center for Employment and Training - Immigration and Citizenship Program (unless amended); Coalition for Justice and Accountability(unless amended); Color of Change (unless amended); Consumer Federation of California (unless amended); Council on American-Islamic Relations – California (unless amended); Electronic Frontier Foundation (unless amended); LIVE Free Fresno (unless amended); Media Alliance(unless amended); Oakland Privacy(unless amended); Peace Officers Research Association of California; Peninsula Peace and Justice Center (unless amended); Restore the 4th SF-Bay Area(unless amended); Root & Rebound; San Jose Peace and Justice Center (unless amended); Working Partnerships USA(unless amended)

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 provides that on or before July 1, 2018 a law enforcement agency shall submit to its governing body a Surveillance Use Policy.

This bill provides that the Surveillance Use Policy shall be in writing and made publicly available on the agency's Internet Web site prior to the public hearing and after adoption.

This bill provides that the governing body shall consider the policy for adoption by resolution or ordinance on the regular, nonconsent calendar at a regularly scheduled hearing.

This bill provides that the policy shall pertain to any surveillance technologies already in use by the law enforcement agency and 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 of each surveillance technology used by the law enforcement agency.

This bill provides that each section covering a separate technology shall at a minimum include 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 and, if so, how the collected information can be accessed by members of the public, including criminal defendants.

This bill provides that after July 1, 2018, if a law enforcement agency intends to acquire a new type of surveillance technology after the adoption of the policy the agency shall submit an amendment to the policy to include the new type of technology as a new section of the policy and submit the amendment to its governing body for approval as provided. The amendment shall be submitted prior to the acquisition of the technology and shall be submitted to the governing body at a properly noticed hearing and be in writing and publicly available on the agency's Internet Web site prior to the public hearing and after adoption.

This bill provides that if before July 1, 2018, a law enforcement agency has implemented the requirements for automated license plate readers as provided for in law or cellular communications interception technology as provided for in law, the law enforcement agency shall include the required information as part of the Surveillance Use Policy.

This bill provides that at a time interval agreed to by the law enforcement agency and the governing body, a law enforcement agency shall submit a report on its surveillance use of approved technologies to the governing body and that report shall be made available on the agency's Internet Web site.

This bill provides that the report shall at minimum include the following:

- The total costs for each surveillance technology, including personnel costs.
- A description of how many times each type of technology was used in the preceding year and how many times each type of technology helped apprehend suspects or close a criminal case.
- A description of the type of data collected by each surveillance technology, including whether each technology captured images, sound, or other data.
- The number of times and the purposes surveillance technology was borrowed from or lent to another agency, including technologies used under exigent circumstances.
- The number and classification of the agency employees trained and authorized to use each type of surveillance technology, along with a description of the training provided to agency employees on each type of surveillance technology and how often the training was provided.
- Disclosure of whether any surveillance technology was used in a manner out of compliance with the agency's policy, whether data was collected through the use of surveillance technology was inappropriately disclosed, released, or in any other way revealed for a non-approved reason, and the steps the agency took to correct the error.

This bill provides that nothing in this section shall be construed to prohibit a governing body from adopting additional protocols as they relate to surveillance technology.

This bill provides that a law enforcement agency may temporarily acquire or temporarily use a surveillance technology in exigent circumstances unless that acquisition or use conflicts with or is preempted by state or federal law.

This bill provides that if a law enforcement agency acquires or uses a surveillance technology in exigent circumstance, the agency shall report to the governing body within 90 days following the end of the exigent circumstance, submit an amendment to the agency's Surveillance use Policy for the technology, and include the technology in the report. The governing body may grant an extension of the 90 day requirement.

This bill allows a civil action to be brought by an individual harmed by a violation of the Surveillance Technology Policy against a person who knowingly caused a violation of a surveillance policy.

This bill includes the following definitions:

- Exigent circumstances – 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 information it provides.
- Governing body – ay police department, sheriff's department, college campus, or special district agency created to enforce the law and prevent crime.
- Surveillance technology – any electronic device or system primarily intended 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 readers, closed-circuit cameras/televisions, international mobile subscriber identity trackers, global positioning system technology,

radio-frequency identification technology, biometrics-identification technology, and facial-recognition technology.

This bill provides that surveillance technology does not includes standard electronic devices or systems that have a primary function other than monitoring or collecting audio, visual, locational, thermal or similar information on any individual or group, including but not limited to standard law enforcement agency computers and software, fingerprint scanners, ignition interlock devices, cell phones, two-way radios or other similar electronic devices.

COMMENTS

1. Need for This Bill

According to the author:

> California enacted two laws in 2015 – SB 34 & SB 741 – that require 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, both of which are surveillance technologies intended to collect wide-ranging information on members of the public. The laws also generally require a public discussion before either of the surveillance technologies are deployed.
>
> While these laws appropriately balance protecting Californian's civil liberties and privacy with law enforcement's ability to use the technologies to fight crime, they are only applicable to two specific technologies. The laws do not apply to the other surveillance technologies used by the police.
>
> Increasingly, law enforcement agencies are using a wider array of surveillance technologies as they become available. The technologies include: facial recognition, social media scrubbers, radar, and more. The Washington Post reported 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, according to the latest information from the Bureau of Justice Statistics."[i] The data collected with the surveillance devices can be stored for undefined periods of time, often in large, regional databases.
>
> While surveillance technologies can help improve public safety, the proliferation of the technologies has also profound impacts on Californians civil liberties and privacy. As police agencies continue to use a varied array of surveillance devices, they gain a greater ability to capture detailed information about where people go, who they associate with, what they say, and more. There should be laws in place to ensure that surveillance devices are only used for their intended purposes – to catch criminals and fight crime – and not to collect vast amounts of data on a wide array on non-criminal residents.

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: the authorized purposes for using the technology; the type of data that can be collected; the job title of the employees and independent contractors authorized to use the technology and access the data; they type of training required to use the technology; the title of the official custodian of the technology; a description of how the technology will be monitored to ensure the security of 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; purpose of, process for and restrictions on the sale, sharing , or transfer of information to other persons and whether and, if so, how the collected information can be accessed by members of the public, including criminal defendants.

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 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. 90 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?

Is the 90 day time fame an appropriate one? Exigent circumstances is an emergency so by it is definition should not go on too long so is allowing three months to report the use to a governing board excessive?

6. Civil action

This bill allows a person harmed by the misuse of technology to bring a civil action against a person who knowingly violated the policy. The bill specified that the person can receive actual damages, but no less than $2,500 as well as punitive damages upon proof of a willful or reckless disregard of the law. This bill will be going to Senate Judiciary next so they will likely deal with the civil penalties, but does this Committee believe the right to a civil action is appropriate?

7. Support

The California Public Defenders Association "strongly" supports this bill stating:

> [L]aw enforcement has been increasingly using covert surveillance technologies for investigative purposes and has been collecting information on the citizens of this state without any written rules or oversight. While surveillance technology may enhance public safety, this does not come without significant cost to civil liberties. It is simply not sufficient for law enforcement to promise the public that will only use these technologies to investigate criminal activity. There must be some accountability and oversight over the use of these technologies that routinely permit law enforcement to surveil private citizens and collect data without oversight by any entity including the courts.

> Additionally, it is essential that elected bodies who represent the citizens of these communities determine what types of surveillance may be conducted, what data may be obtained, collect and stored, as well as how the data may be used. It is the elected bodies that are directly accountable to the residents in their communities who should have the opportunity to weigh in on how these technologies are being used to police their communities.

8. Oppose unless amended

The following groups oppose this bill unless amended: ACLU of California; Asian Americans Advancing Justice - Asian Law Caucus; Asian Law Alliance; Center for Media Justice; Center for Employment and Training - Immigration and Citizenship Program; Coalition for Justice and Accountability; Color of Change; Consumer Federation of California; Council on American-Islamic Relations – California; Electronic Frontier Foundation; LIVE Free Fresno; Media Alliance; Oakland Privacy; Peninsula Peace and Justice Center; Restore the 4th SF-Bay Area; San Jose Peace and Justice Center; Working Partnerships USA. They state a number of specific concerns but state generally:

> Right now, California communities such as Oakland, Santa Clara County, and the BART district have adopted or are moving forward with strong legislation that ensures transparency, accountability, and oversight for all surveillance technology proposals.[1] Relative to SB 21, these local efforts give communities essential information about proposals, more power to evaluate proposed technologies and supervise their use, and more appropriate tools to address misuse. SB 21 substitutes an ineffective alternative for these reforms.
>
> Local law enforcement's secretive acquisition and use of surveillance technology disproportionately impacts California's low income residents, people of color, and immigrants.[2] In Oakland, the use of license plate readers by police has been concentrated in low income and black communities, according to a 2015 report.[3] In San Jose, police secretly purchased a drone without consulting Muslim community members and other residents.[4] In Compton, the LA Sheriff conducted secretive

[1] Santa Clara County enacted a surveillance technology ordinance in June 2016. http://sccgov.iqm2.com/Citizens/FileOpen.aspx?Type=4&ID=149330&MeetingID=7193. Oakland's proposed ordinance: http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak062224.pdf. Committees and commissions for BART and in Berkeley and Palo Alto have voted to move forward with similar legislation. BART: https://www.bart.gov/sites/default/files/docs/agendas/12-21-16%20Tech%20%26%20Comm_0.pdf Palo Alto: http://www.cityofpaloalto.org/civicax/filebank/documents/56292; Berkeley: http://www.ci.berkeley.ca.us/uploadedFiles/Health_Human_Services/Commissions/Commission_for_Peace_and_Justice/01-09-17-PJC-Minutes.pdf.

[2] A 2014 ACLU of California survey found that at least 90 California communities were in possession of various surveillance technologies, and that public debate rarely occurred when technologies were proposed. State of Surveillance in California – Findings & Recommendations, January 2015, https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf.

[3] Dave Maass, *What You Can Learn From Oakland's Raw ALPR Data*, Electronic Frontier Foundation, Jan. 21, 2015, https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

[4] Thomas Mann Miller, *San Jose Police Department's Secret Drone Purchase: Where's the Accountability?*, ACLU-NorCal, July 30, 2014, https://www.aclunc.org/blog/san-jose-police-departments-secret-drone-purchase-wheres-accountability.

aerial surveillance with high-powered cameras without telling residents.[5] Any proposed state-level legislation should enact a meaningful floor, as well as lift up local efforts to address these real problems.

Californians want robust statewide oversight of surveillance technology.[6] As the federal government signals it will increase the use of its surveillance and enforcement powers against Muslims and immigrants, the California legislature has a special responsibility to enact strong measures that protect the most vulnerable Californians from suspicionless monitoring and the collection of information that can exploited for discriminatory ends. SB 21 does not adequately address these challenges, and it will undermine local efforts.

END –

[i] https://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

[5] Conor Friedersdorf, *Eyes Over Compton: How Police Spied on a Whole City*, The Atlantic, Apr. 21, 2014, https://www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/.

[6] *California Statewide Survey Finds Voters Concerned about Privacy and Want to See Reforms Made to Surveillance Technology Use by Law Enforcement*, Tulchin Research, https://www.aclunc.org/docs/20150821-aclu_surveillance_privacy_polling.pdf.