SENATE COMMITTEE ON TRANSPORTATION
Senator Dave Cortese, Chair
2025 - 2026 Regular

Bill No:	SB 1013	**Hearing Date:**	4/14/2026
Author:	Cervantes		
Version:	3/25/2026 Amended		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Isabelle LaSalle		

SUBJECT: Automated license plate recognition systems

DIGEST: This bill requires operators and end-users of automated license plate recognition (ALPR) systems to bolster their safeguards relating to employee access and usage of such systems. This bill requires the Department of Justice (DOJ) to audit public agency operators and end-users to ensure compliance with their usage and privacy policies, as provided. This bill places retention limits on ALPR data, with exceptions.

ANALYSIS:

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) Defines "automated license plate recognition system" or "ALPR system" to mean a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data. "ALPR information" means information or data collected through the use of an ALPR system. "ALPR operator" means a person that operates an ALPR system, except as specified. "ALPR end-user" means a person that accesses or uses an ALPR system, except as specified. The definitions for both "ALPR operator" and" ALPR end-user" exclude transportation agencies subject to certain provisions of the Streets and Highways Code that apply to electronic toll collection. (Civ. Code § 1798.90.5.)

3) Requires an ALPR operator to maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction,

use, modification, or disclosure. ALPR operators must implement usage and privacy policies in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. (Civ. Code § 1798.90.51.)

4) Requires ALPR end-users to maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. ALPR end-users must implement usage and privacy policies in order to ensure that the access, use, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. It further requires the policies to include, at a minimum, certain elements. (Civ. Code § 1798.90.53.)

5) Provides that a public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law. For purposes of this section, the provision of data hosting or towing services is not considered the sale, sharing, or transferring of ALPR information. (Civ. Code § 1798.90.55.)

6) Authorizes the California Highway Patrol (CHP) to retain license plate data captured by a license plate reader for no more than 60 days, except in circumstances when the data is being used as evidence, or for all felonies being investigated, including, but not limited to, auto theft, homicides, kidnaping, burglaries, elder and juvenile abductions, Amber Alerts, and Blue Alerts. (Veh. Code § 2413(b).)

7) Prohibits CHP from selling license plate reader data for any purpose and from making the data available to an agency that is not a law enforcement agency or an individual who is not a law enforcement officer. The data may be used by a law enforcement agency only for purposes of locating vehicles or persons when either are reasonably suspected of being involved in the commission of a public offense. (Veh. Code § 2413(c).)

8) Requires CHP to monitor internal use of the license plate reader data to prevent unauthorized use. (Veh. Code § 2413(d).)

9) Requires CHP to annually report license plate reader practices and usage, including the number of license plate reader data disclosures, a record of the agencies to which data was disclosed and for what purpose, and any changes in policy that affect privacy concerns, to the Legislature. (Veh. Code § 2413(e).)

10) Establishes the Data Breach Notification Law, which requires any agency, person, or business that owns, licenses, or maintains data including personal information to disclose a breach, as provided. (Civ. Code §§ 1798.29; 1798.82.) Includes ALPR data within the definition of "personal information," if combined with an individual's first name or first initial and last name, when either piece of data is not encrypted. (Civ. Code §§ 1798.29(g), 1798.82(h).)

11) Prohibits a transportation agency from selling or otherwise providing to any other person or entity personally identifiable information of any person who subscribes to an electronic toll or electronic transit fare collection system or who uses a toll bridge, toll lane, or toll highway that employs an electronic toll collection system, except as expressly provided. (Sts. & Hwy. Code § 31490.)

12) 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.)

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

14) Authorizes a public transit operator to install automated forward facing parking control devices on city-owned or district-owned public transit vehicles, for the purpose of video imaging of parking violations occurring in transit-only traffic lanes and at transit stops. (Veh. Code § 40240)

This bill:

1) Provides that the current requirements for ALPR operators and end-users to maintain reasonable security procedures and practices must include:

   a) Safeguards for managing which employees can see the data from their systems, including requiring supervisory approval, robust authentication protocols for establishing an account to access an ALPR system, and tracking searches of ALPR information made by employees.

   b) Requiring data security training and data privacy training for all employees that access ALPR information.

2) Requires DOJ to conduct audits of public agency ALPR operators and end-users, as provided.

3) Requires that the usage and privacy policies must indicate the purpose for which specified employees and contractors are granted access to, and permission to use, ALPR information.

4) Prohibits a public agency from retaining ALPR information that does not match information on a hot list for more than 30 days after the date of collection.

5) Defines a "hot list" as a list or lists of license plates of vehicles of interest against which ALPR system is comparing vehicles on the roadways. Authorized hot lists are limited to the National Crime Information Center (NCIC) list, the Stolen Vehicle System (SVS), California Department of Justice lists, official alerts, including AMBER, Silver, Feather, Blue, Yellow, Ebony, and any new alerts authorized by the Legislature, and custom BOLO lists that pertain solely to missing and at-risk persons, witness locations, burglaries, grand theft, and violent crimes.

6) Requires a public agency to, within 14 days, delete all ALPR information that has been held for more than 30 days and does not match information on an authorized hot list.

7) Excludes from the definitions for both "ALPR operator" and" ALPR end-user" transportation agencies, public transit operators, and local transportation departments subject to certain provisions of the Vehicle Code that apply to red light cameras, speed cameras, toll collection, and transit operator parking enforcement cameras.

8) Excludes from the definitions for both "ALPR operator" and" ALPR end-user" an airport or airport operator when collecting, accessing, or using ALPR information solely for parking access control, fee calculation, lost-ticket resolution, fraud prevention, or transaction dispute resolution in an airport parking facility.

COMMENTS:

1) *Purpose of the bill.* According to the author, "Currently, at least 230 police and sheriff departments in California use an automated license plate recognition (ALPR) system, with at least three dozen more plan to use them in the future. Senate Bill 34 by Senate Hill in 2016 requires operators of these systems and those using ALPR data to implement policies to govern the usage of the data and provide safeguards to protect individual privacy. However, a 2020 report from the State Auditor confirmed that law enforcement agencies across the state are not complying with SB 34.

"ALPRs are a form of location surveillance, the data they collect can reveal our travel patterns and daily routines, the places we visit, and the people with whom we associate and love. Along with the threat to civil liberties, these data systems pose significant security risks. There have been multiple known breaches of ALPR data and technology in recent years, indicating potential cybersecurity threats. In a climate where the current federal administration is pursuing mass deportations of U.S. citizens and undocumented individuals alike, Automated License Plate Recognition (ALPR) is a powerful surveillance technology that can invade the privacy of all individuals and violate the rights of entire communities.

"Aggregated location data allows law enforcement and private companies to create detailed profiles of a person's daily life. When considered in bulk, ALPR data can form an intimate picture of a driver's activities and even deter First Amendment-protected activities. This kind of targeted tracking threatens to erode fundamental freedoms of speech. The extensive use of ICE's access to ALPR databases has surfaced at a pivotal moment, highlighting urgent concerns about data collection and retention practices. Ultimately, these practices not only compromise community trust but also undermine the very principles of safety and protection that sanctuary laws aim to uphold. Most ALPR data is stored in databases for extended periods, often up to five years. While police departments typically maintain these databases, they are frequently managed by private companies. It has been five years since the troubling audit published in 2020 highlighted the alarming misuse of ALPR (Automated License Plate Recognition) data in our state. We continue to witness abuse by law enforcement, including the sharing of data with other states, ICE and CBP. Under the 10-year-old California measure, Senate Bill 34, state law enforcement agencies, are barred from sharing license plate reader data with out-of-state public agencies or federal entities. The law has been routinely violated; civil liberties groups in 2023 found that 71 California law enforcement agencies had broken it. Later that year, Attorney General Rob Bonta issued an advisory providing law enforcement with specific guidance on how to comply with the law. Senate Bill 1013 establishes robust safeguards regarding the use of ALPR data. The bill would prohibit ALPR information from being retained by public agencies for longer than 30 days unless it is on a hot list. The bill would also require the California Department of Justice to conduct random annual audits of public agencies that are ALPR operator or end-users to determine whether they are complying with their usage and privacy policies. SB 1013 would require those security procedures and practices to include safeguards restricting which employees can see ALPR data from their systems. It would also require data security training and data privacy training for all employees who access ALPR information. Additionally, it requires a case

number to query the database, and deletion of data held for more than 30 days that does not match info on an authorized hot list, within 14 days. Senate Bill 1013 strikes a balance between protecting public safety and ensuring individual privacy rights in our increasing digital world. The temptation to "collect it all" should never overshadow the critical responsibility to "protect it all."

2) *Automated License Plate Reader (ALPR) systems.* ALPR systems are searchable computerized databases resulting from the operation of one or more cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data. The cameras can be mobile, e.g., mounted on patrol cars, or fixed, e.g., mounted on light poles. ALPR systems allow for the widespread and systematic collection of license plate information. ALPR data can have legitimate uses, including for law enforcement purposes. These cameras continuously record the vehicles passing in front of them. Software extracts the license plate number from the image and stores it, with the date, time, and location of the scan and sometimes a partial image of the vehicle, in a searchable database. The software also automatically compares the plate number to stored lists of vehicles of interest, called hot lists, then issues alerts, called hits, if the plate number matches an entry on the hot list. Law enforcement can perform searches to see where exactly a vehicle, and by extension a person, was at a certain time or map out their movements across a wide date range. Currently, at least 230 police and sheriff's departments in California use an ALPR system, with at least three dozen more planning to use them. While such systems are useful, there are serious privacy concerns associated with the systematic collection, storage, disclosure, sharing, and use of ALPR data.

3) *State audit identified data privacy abuse.* Current law requires operators of these systems and those using the data to implement usage and privacy policies. However, concerns have remained about the widespread collection of this data and the highly inconsistent and opaque ways the data is used, stored, and destroyed. A critical report from the California State Auditor confirmed that police departments in the state are not complying with existing law and recommended further regulation of these systems.

   The audit, released in February 2020, focused on four law enforcement agencies that have ALPR systems in place. The report found that "the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use." In addition, the audit found that three of the four agencies failed to

establish ALPR policies that included all of the elements required by SB 34 (Hill, Chapter 532, Statutes of 2015). All three failed to detail who had access to the systems and how they will monitor the use of ALPR systems to ensure compliance with privacy laws. Other elements missing were related to restrictions on the sale of the data and the process for data destruction. The fourth entity, the Los Angeles Police Department, did not even have an ALPR policy.[1]

The Auditor's report calls into question how these systems are being run, how the data is being protected, and what is being done with the data. The report reveals that agencies commingled standard ALPR data with criminal justice information and other sensitive personal information about individuals, heightening the need for stronger security measures and more circumscribed access and use policies. This bill implements some of the report's recommendations by requiring more specific safeguards regarding employee access to ALPR systems and providing more authority for DOJ to oversee these systems.

4) *More recent examples*. Concerns about ALPR data misuse have only grown in recent years. For example, in October of 2025, Attorney General Rob Bonta filed a lawsuit against the El Cajon Police Department over, "its refusal to comply with state law prohibiting the sharing of license plate data with federal and out-of-state law enforcement agencies." According to DOJ, despite outreach from the department notifying the city of the violation, "the El Cajon Police Department and the City of El Cajon have refused to cease the unlawful practice of sharing ALPR data with out-of-state agencies. These include law enforcement agencies in Alabama, Arizona, Arkansas, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Massachusetts, Minnesota, Missouri, Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Texas, Utah, Virginia, Washington, and Wisconsin."[2]

5) *This bill requires safeguards, training, and oversight.* This bill implements a number of audit recommendations aimed at ensuring local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use. For example, the 2020 State Audit recommended that the Legislature mandate that those with access to ALPR systems must receive data privacy and data security training. In accordance

---

[1] California State Auditor, *Automated License Plate Readers, To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects* (Feb. 2020), https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [State Auditor Report].

[2] Attorney General Bonta Sues El Cajon for Illegally Sharing License Plate Data with Out-of-State Law Enforcement | State of California - Department of Justice - Office of the Attorney General

with this recommendation, this bill would require a local agency to mandate data security training and data privacy training for all employees who access ALPR information.

This bill also requires local agencies to establish stronger safeguards for managing which employees can see the data from their ALPR systems, including requiring supervisory approval, robust authentication protocols for establishing an account to access an ALPR system, and tracking searches of ALPR information made by employees. Building off another audit recommendation related to DOJ auditing of ALPR system usage, this bill requires DOJ to conduct annual random audits on a public agency that is an ALPR operator or ALPR end-user to determine whether they have implemented and are adhering to a usage and privacy policy.

Additionally, current law requires ALPR operators to maintain a record of who accessed ALPR data, at what date and time it was accessed, and for what purpose. Building off this requirement, this bill would also require the record to include a case file number that justifies the search query.

6) *30-day deletion requirement.* The 2020 State Audit recommended that the Legislature "establish a maximum data retention period for ALPR images." This bill caps the retention of ALPR information that does not match information on an authorized hot list for more than 30 days after the date of collection. If the data has been held for 30 days and does not match information on an authorized hot list, the public agency would then be required to delete the data within 14 days. Hot lists are limited to the NCIC list, SVS, California Department of Justice lists, official alerts, including AMBER, Silver, Feather, Blue, Yellow, Ebony, and any new alerts authorized by the Legislature, and custom BOLO lists that pertain solely to missing and at-risk persons, witness locations, burglaries, grand theft, and violent crimes.

Much of the opposition argues that having to purge data not on a hot list after 30 days will hinder their ability to solve crimes. Many public agencies keep data far beyond 30 days, even if it is not on a hot list. For example, the 2020 State Audit found that, "at Los Angeles only 400,000 of the 320 million images it has accumulated over several years and stores in its database generated an immediate match against its hot lists. In other words, 99.9 percent of ALPR images Los Angeles stores are for vehicles that were not on a hot list at the time the image was made. Nevertheless, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to determine the vehicles present at particular locations and to track

vehicles' movements at particular times in order to gather or resolve leads in investigations."

7) *Governor's veto of SB 274.* Last year the Legislature passed SB 274 (Cervantes, 2025), which, in its final form, was nearly identical to this bill. The most substantive difference between the two bills is the data retention limit, which was 60 days in SB 274 and is 30 days in this bill. Governor Newsom vetoed SB 274 and provided the following veto message:

"I appreciate the author's intent to prevent information regarding a person's whereabouts from falling into the wrong hands. Nevertheless, this measure does not strike the delicate balance between protecting individual privacy and ensuring public safety. For example, it may not be apparent, particularly with respect to cold cases, that license plate data is needed to solve a crime until after the 60-day retention period has elapsed. Conversely, restrictions on inter-agency data sharing may impair solving crimes in real time, such as highway shootings, where the suspect may be rapidly crossing jurisdictional boundaries. Further, by restricting law enforcement agencies' use of ALPR information only for locating persons or vehicles suspected of involvement in crimes, this bill would prevent the use of this information to locate missing persons.

"This bill also creates cost pressures, which are not accounted for in this year's budget, by requiring the Department of Justice to conduct random audits of public entities in order to ensure compliance with this bill. In partnership with the Legislature this year, my Administration has enacted a balanced budget that recognizes the challenging fiscal landscape our state faces while maintaining our commitment to working families and our most vulnerable communities. With significant fiscal pressures and the federal government's hostile economic policies, it is vital that we remain disciplined when considering bills with significant fiscal implications that are not included in the budget, such as this measure."

8) *Transportation agencies, public transit operators, and others excluded.* This bill specifically exempts red light cameras, speed cameras, transit operator parking enforcement cameras, and airports under specific circumstances from the definition of ALPR operator and ALPR end user.

9) *Double Referral.* This bill has been double referred to the Senate Privacy, Digital Technologies, and Consumer Protection Committee.

RELATED/PREVIOUS LEGISLATION:

SB 274 (Cervantes, 2025) – Would have prohibited a public agency from retaining ALPR information that does not match information on a hot list for more than 60 days after the date of collection. T*his bill was vetoed by Governor Newsom.*

SB 34 (Hill, Chapter 532, Statutes of 2015) – Established regulations on the privacy and usage of ALPR data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system.

AB 1463 (Lowenthal, 2023) – Would have required operators and end-users of ALPR systems to conduct annual audits to review ALPR searches. If the operator or end-user is a public agency, it would have further required them to destroy all ALPR information that does not match information on a hot list within 30 days. AB 1463 would have placed restrictions on accessing certain systems and sharing ALPR information. *This bill died in the Assembly Transportation Committee.*

AB 2192 (Ramos, 2022) – Would have authorized a public agency that uses an ALPR to share the data that they collect with a law enforcement agency of the federal government or another state if ALPR information is being sold, shared, or transferred to locate a vehicle or person reasonably suspected of being involved in the commission of a public offense, except as specified. *This bill was taken up in Assembly Privacy and Consumer Protection for testimony only.*

SB 210 (Wiener, 2021) – Would have provided greater transparency and accountability with respect to ALPR systems by requiring, similar hereto, ALPR operators and end-users to conduct annual audits to review ALPR searches. It would have further required an operator or end-user that is a public agency to destroy all ALPR data that does not match information on a hot list within 24 hours. *SB 210 died in the Senate Appropriations Committee.*

SB 1143 (Wiener, 2020) – This bill was largely identical to AB 1463 and was held under submission in the Senate Transportation Committee.

AB 1782 (Chau, 2019) – Would have required those operating ALPR systems and those accessing or using ALPR data to have policies that include procedures to ensure nonanonymized ALPR information is timely destroyed, except as specified, and that all ALPR information that is shared is anonymized. The bill was subsequently gutted and amended to address a different topic. *This bill died in the Senate Appropriations Committee.*

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: Yes

POSITIONS: (Communicated to the committee before noon on Wednesday, April 8, 2026.)

SUPPORT:

None received.

OPPOSITION:

Arcadia Police Officers' Association
Brea Police Association
Burbank Police Officers' Association
California Narcotic Officers' Association
California Reserve Peace Officers Association
California State Sheriffs' Association
Claremont Police Officers Association
Corona Police Officers Association
Culver City Police Officers' Association
Fullerton Police Officers' Association
Murrieta Police Officers' Association
Newport Beach Police Association
Novato Police Officers Association
Palos Verdes Police Officers Association
Peace Officers Research Association of California (PORAC)
Placer County Deputy Sheriffs' Assocation
Pomona Police Officers' Association
Riverside Police Officers Association
Riverside Sheriffs' Association

California Police Chiefs Association (Oppose Unless Amended)

-- END --