Office of Senate Floor Analyses
(916) 651-4171

THIRD READING

Bill No: SB 1013
Author: Cervantes (D)
Amended: 5/14/26
Vote: 21

SENATE TRANSPORTATION COMMITTEE: 9-3, 4/14/26
AYES: Cortese, Archuleta, Arreguín, Blakespear, Gonzalez, Grayson, Menjivar, Richardson, Wiener
NOES: Strickland, Dahle, Seyarto
NO VOTE RECORDED: Valladares

SENATE PRIV., DIGITAL TECH. & CONS. PROT. COMMITTEE: 7-2, 4/20/26
AYES: Cabaldon, Gonzalez, McNerney, Padilla, Reyes, Umberg, Wiener
NOES: Jones, Seyarto

SENATE APPROPRIATIONS COMMITTEE: 5-2, 5/14/26
AYES: Cervantes, Cabaldon, Grayson, Richardson, Wahab
NOES: Seyarto, Dahle

SUBJECT: Automated license plate recognition systems

SOURCE: Author

DIGEST: This bill (1) 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; (2) requires the Department of Justice (DOJ) to conduct random annual audits of public agency operators and end-users to ensure compliance with their usage and privacy policies; (3) imposes additional use restrictions on public agencies and 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. (California Constitution (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 who operates an ALPR system, except as specified. "ALPR end-user" means a person who accesses or uses an ALPR system, except as specified. The definitions for both ALPR operator and ALPR end-user exclude transportation agencies when subject to Section 31490 of the Streets and Highways Code. (Civil (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. It further requires the policies to include, at a minimum, certain specified elements. (Civ. Code § 1798.90.51.)

4) Requires an ALPR operator, if it accesses or provides access to ALPR information, to do both of the following:

    a) Maintain a record of that access. At a minimum, the record shall include all of the following:

        i) The date and time the information is accessed.

        ii) The license plate number or other data elements used to query the ALPR system.

        iii) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

        iv) The purpose for accessing the information.

b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy. (Civ. Code § 1798.90.52.)

5) 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.)

6) 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 shall not be considered the sale, sharing, or transferring of ALPR information. (Civ. Code § 1798.90.55.)

7) Authorizes the Department of 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, kidnapping, burglaries, elder and juvenile abductions, Amber Alerts, and Blue Alerts. (Vehicle (Veh.) Code § 2413(b).)

8) 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).)

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

10) Requires CHP to annually report the 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).)

11) 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(a), (b), (c) and 1798.82(a), (b), (c).) Includes within the definition of "personal information" ALPR data when 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).)

12) 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. (Streets and Highways (Sts. & Hy.) Code § 31490.)

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 who access ALPR information.

2) Requires DOJ to conduct annual random audits on public agency ALPR operators and end-users to determine whether they have implemented and are adhering to a usage and privacy policy in compliance with the law. This is contingent upon appropriation, as provided.

3) Provides that usage and privacy policies shall be implemented under the supervision of DOJ, as applicable.

4) Requires that ALPR operators record the case file number that justifies each search query. A query shall not be allowed without a log entry with a valid and current case file number from the agency conducting the query. In the event of a

search query that is conducted as part of an inter-agency task force established by the Attorney General and overseen by the office's Bureau of Investigation, in lieu of a case file number, the log entry shall include the name of the task force and the name of the bureau commander in charge of the task force.

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

6) Provides that, beginning January 1, 2027, all new, updated, expansions of, or addendums of contractual agreements with ALPR vendors, manufacturers, or suppliers shall mandate that no default access is provided to any national ALPR database and that an agency's collected scans are by default not accessible to any other agency. A law enforcement agency may manually implement agency to agency sharing with other California state law enforcement agencies only as authorized by Department of Justice General Order 2023-05.

7) Provides that ALPR information 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 or locating an individual who has been reported as missing to a law enforcement agency.

8) Requires law enforcement agency ALPR operators and end-users to establish a maximum data retention period for ALPR information.

9) Prohibits a public agency from retaining ALPR information for more than 30 days if it does not match information on an authorized hot list.

10) Requires a public agency, as of January 1, 2027, to delete all ALPR information, within 14 days, unless it is retained in the evidence file of an active investigation or criminal proceeding or matches information on an authorized hot list.

11) Carves the following entities out of the definition of ALPR end-user and ALPR operator:

    a) A public transit operator when subject to Section 40240 of the Vehicle Code.

    b) A local department of transportation or public works department when subject to specified provisions of law.

c) 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.

12) Carves the following entities out of the definition of "public agency":

a) A transportation agency when subject to Section 31490 of the Streets and Highways Code.

b) A public transit operator when subject to Section 40240 of the Vehicle Code.

c) A local department of transportation or public works department when subject to specified provisions of law.

13) Defines "hot list" to mean a list or lists of license plates of vehicles of interest against which the 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.

Comments

1) *Purpose of this 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 their movements across a wide date range. Currently, at least 230 police and sheriff's departments in California use an ALPR system, with more agencies 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."[1]

[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].

While the report deeply investigated only four entities, it conducted a statewide survey of law enforcement agencies, revealing that 70 percent operate or plan to operate an ALPR system, and 84 percent of those operating a system shared their images. The report indicates that this "raises concerns that these agencies may share the deficiencies [they] identified at the four agencies [they] reviewed."

4) *This bill requires safeguards, training, and oversight.* This bill implements several 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 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 accounts 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.

   Under SB 1013, public agencies would be required to contractually mandate that no default access is provided to national ALPR databases and that scans are not by default accessible to any other agencies. ALPR information 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.

5) *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 to no more than 30 days after the date of collection. After 30 days, the public agency would then be required to delete the data within 14 days, unless the ALPR information is retained in the evidence file of an active investigation or criminal proceeding, or matches information on an authorized hot list. Authorized hot lists are limited to the 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.

Related/Prior 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.*

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

According to the Senate Appropriations Committee:

- Unknown General Fund cost pressures, likely in the low millions of dollars annually, for the DOJ to conduct random audits of public agencies that are ALPR operators or end-users. DOJ costs would only be incurred to the extent sufficient funds are appropriated in the annual Budget Act for these purposes, and the magnitude of this funding would determine how many audits could be conducted in a given year.

- Unknown, potentially significant state-mandated local costs for affected local public agencies who are ALPR operators or end-users to comply with the requirements of this bill, including costs to revise policies and procedures to ensure ALPR information is not retained longer than 30 days, to revise security procedures and practices to restrict access to ALPR information, and to develop and conduct training for all employees who access ALPR information, as specified. These local costs may be subject to reimbursement by the state, subject to a determination by the Commission on State Mandates. (General Fund)

- Unknown, potentially significant costs in the aggregate, for state agencies who are ALPR operators or end-users to comply with the requirements of the bill. The California Highway Patrol indicates that any costs would be absorbable within existing resources. (various funds)

SUPPORT: (Verified 5/14/26)

Oakland Privacy

OPPOSITION: (Verified 5/14/26)

Arcadia Police Officers' Association
Brea Police Association
Burbank Police Officers' Association
California Narcotic Officers' Association
California Reserve Peace Officers Association
California State Sheriffs' Association
City of Colton

City of LA Verne
City of Los Alamitos
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
Orange County Sheriff's Department
Palos Verdes Police Officers Association
Peace Officers Research Association of California
Placer County Deputy Sheriffs' Association
Pomona Police Officers' Association
Riverside Police Officers Association
Riverside Sheriffs' Association

ARGUMENTS IN SUPPORT: Writing in support, Oakland Privacy states, "Automated License Plate Reader programs, as currently operated, directly threaten everything the State of California has done to protect access to reproductive care and gender treatment and to defend non-citizen residents from kidnapping, detention, deportation and rendition. Senate Bill 1013 seeks to close the leaks to immigration and return the program to its intended purpose of helping to locate stolen cars and identifying the perpetrators of criminal incidents…SB 1013 would implement new and timely (if not long overdue) protections for this geolocation information as we face enormous challenges with the federal weaponization of personal information against vulnerable groups. There has been a recent flood of disclosures regarding clear violations of the Legislatures existing statutes regulating license plate collection (SB 34 (Hill) – 2015) and the California Values Act. We want to emphasize that these violations are only the ones that happen to have been uncovered by diligent public records work by groups like Oakland Privacy, Electronic Frontier Foundation and the Lucy Parsons Lab in Illinois. There are likely many more that have not yet been uncovered. The latest showed 2.6 million violations of existing law by the San Francisco Police Department alone in one 4 year period."

ARGUMENTS IN OPPOSITION: Writing in opposition, the California State Sheriffs' Association states, "Law enforcement agencies across the state and nation have used ALPR data to solve crimes and apprehend criminal suspects and continue to do so today. While some cases are solved quickly using this technology, it can also be exceptionally helpful in solving crimes that have

occurred deeper in the past. Setting a data retention limit such as 30 days in statute will significantly hinder the use of a valuable law enforcement tool.

“Additionally, SB 1013 limits the hot lists to which ALPR data can be compared. The bill also prohibits an ALPR query unless the requesting entity has a case file number. In many situations that necessitate the use of ALPR data, no case file number will have been generated at the time when the ALPR query is needed. This will drastically reduce the availability and utility of this vital crime-fighting tool, especially in fresh cases where a crime has just occurred or a person has just gone missing.”

Prepared by: Isabelle LaSalle / TRANS. / (916) 651-4121
5/18/26 15:17:59

****** END ******