SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

SB 1013 (Cervantes)
Version: March 25, 2026
Hearing Date: April 20, 2026
Fiscal: Yes
Urgency: No
CK

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 conduct random annual audits of public agency operators and end-users to ensure compliance with their usage and privacy policies. The bill imposes additional use restrictions on public agencies and places retention limits on ALPR data, with exceptions.

EXECUTIVE SUMMARY

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. Currently, at least 230 police and sheriff 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.

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 wildly inconsistent and opaque ways the data is used, stored, and destroyed. A report from the California State Auditor confirms that police departments in the state are not complying with existing law and recommends further regulation of these systems.

This bill implements some of the report's recommendations by mandating annual random audits of public agency operators and end-users to determine whether they have properly implemented the required usage and privacy policies. The bill requires more specific safeguards regarding employee access to ALPR systems and provides more authority for DOJ to oversee these systems. ALPR information cannot be retained by public agencies for longer than 30 days, except as specified. This bill is author-sponsored. It is supported by Oakland Privacy. The bill is opposed by a number of law enforcement agencies, including the Riverside Sheriffs' Association. This bill passed out of the Senate Transportation Committee on a vote of 9 to 3.

PROPOSED CHANGES TO THE LAW

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 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. (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. (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. (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 must 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.

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, that has been held for more than 30 days and does not match 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. ALPR systems and the privacy implications

The prevalence of ALPR systems and the ease with which license plate data can be gathered and aggregated have raised serious privacy concerns for years. Using large datasets of ALPR data gathered over time, it is possible to reconstruct the locational history of a vehicle and extrapolate certain details about the vehicle's driver. As an American Civil Liberties Union (ACLU) report explains:

> Tens of thousands of license plate readers are now deployed throughout the United States. Unfortunately, license plate readers are typically programmed to retain the location information and photograph of every vehicle that crosses their path, not simply those that generate a hit. The photographs and all other associated information are then retained in a database, and can be shared with others, such as law enforcement agencies, fusion centers, and private companies. Together these databases contain hundreds of millions of data points revealing the travel histories of millions of motorists who have committed no crime.[1]

The U.S. Supreme Court has examined the significant privacy concerns raised by locational tracking technology in *United States v. Jones* (2012) 565 U.S. 400. The *Jones* case considered whether the attachment of a Global Positioning System (GPS) tracking device to an individual's vehicle, and the subsequent use of that device to track the vehicle's movements on public streets, constituted a search within the meaning of the Fourth Amendment. In her concurring opinion, Justice Sonia Sotomayor made the following observations:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to

[1] ACLU, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* (July 2013) https://www.aclu.org/other/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements?redirect=technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record. All internet citations are current as of April 11, 2026.

> assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may alter the relationship between citizen and government in a way that is inimical to democratic society.
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.

(*United States v. Jones* (2012) 565 U.S. 400, 416 [internal citations and quotation marks omitted].)

As with GPS monitoring, the accumulation of ALPR locational data into databases that span both time and distance also threatens to undermine one's right to privacy. As with GPS monitoring, California residents may be less willing to exercise their associational and expressive freedoms if they know that their movements are being compiled into databases accessible not only to the government, but also to private industries and individuals. Without adequate regulations, the use of these systems threatens Californians' right to privacy, a right explicitly enshrined in the California Constitution.

2. Enhancing the law to ensure the legitimacy of ALPR systems and the security of their data

In 2015, SB 34 (Hill, Ch. 532, Stats. 2015) sought to address some of the concerns about the privacy of this information by placing certain protections around the operation of ALPR systems and the use of ALPR data. (*See* Civ. Code §§ 1798.90.51, 1798.90.53.)[2] The resulting statutes provided that both ALPR operators and ALPR end-users[3] were required 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. They were further required to implement usage and privacy policies in order to ensure that the collection, access, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties.

---

[2] SB 34 also included ALPR data within the definition of "personal information" for purposes of California's Data Breach Notification Law.

[3] The law defines an "ALPR operator" as a person that operates an ALPR system and an "ALPR end-user" as a person that accesses or uses an ALPR system, with certain exemptions. (Civ. Code § 1798.90.5.) Both definitions exclude a transportation agency when subject to Section 31490 of the Streets and Highways Code.

These policies are required to be made available to the public in writing and posted to the operator or end-user's internet website, if it exists. These policies are required to include at least the following:

- the authorized purposes for using the ALPR system, and collecting, accessing, and/or using ALPR information;
- a description of the job title or other designation of the employees and independent contractors who are authorized to access and use the ALPR system and its information, or to collect the ALPR information. It must also identify the necessary training requirements;
- a description of how the ALPR system will be monitored to ensure the security of the ALPR information, and compliance with all applicable privacy laws;
- a process for periodic system audits for end-users;
- the purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons;
- the title of the official custodian, or owner, of the ALPR information responsible for implementing the relevant practices and policies;
- a description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors; and
- the length of time ALPR information will be retained, and the process the ALPR operator or end-user will utilize to determine if and when to destroy retained ALPR information.

Unfortunately, the security and privacy concerns have only multiplied in the wake of SB 34. Many ALPR systems have been found to have weak security protections, leading to the leaking of sensitive ALPR data and easy access to potential hackers.[4] A 2018 Los Angeles Times editorial illustrates the concerns:

> When someone drives down a street or parks a car at a curb, there is no expectation of privacy — the driver, the car and the license plate are in public view. Yet most people would recoil if the government announced a program to scan those license plate numbers into a database it could use to determine whose car was parked where and when. It's an obnoxiously intrusive idea that sneaks over the line between a free society and Big Brother dystopia. The notion that the government could trace people's travels whenever it wishes undercuts our fundamental belief that, barring probable cause to suspect involvement in a crime, we should be able to move about freely without being tracked.
>
> But government agencies, from local police departments to Immigration and Customs Enforcement, are able to do just that. Some police agencies

[4] Zack Whittaker, *Police license plate readers are still exposed on the internet* (January 22, 2019) TechCrunch, https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/.

> — including the Los Angeles Police Department and the Los Angeles County Sheriff's Department — maintain their own databases of scanned plates, which is problematic enough without proper policies and controls in place. Many share with other agencies in broad networks. Some agencies contract with private vendors that build massive databases by merging feeds from automatic license plate readers. So while police must obtain a warrant before placing a tracking device on someone's car, they do not need a judge's permission to contract with a database — or build their own — and, theoretically, track a person's movements over time by consulting records of where his or her car has been spotted.
> . . .
> We have been concerned about the broad spread of license-plate scanners in recent years primarily because of the potential for ubiquitous monitoring. Clearly, a database that allows police to, in essence, go back in time and see what cars might have been parked outside a store as it was being robbed could be a useful investigative tool. But at what cost?
>
> Under this privatized system, government officials can enter a license plate and receive an alert as soon as it turns up on any of the nationwide army of scanners — in police cars, on utility poles, in cars driven by private citizens working with the vendors — that feed these databases. Because the data is not purged after a short amount of time, it also means police can plug in a license plate and find out where a car had traveled on any specific day going back years. Such an arrangement might pass constitutional muster, but it certainly violates our right and expectation to not have our daily activities collected and saved for retrieval by government agents.[5]

3. California State Auditor report uncovers disturbing lack of compliance, oversight

In response to the growing concerns with ALPR systems, the Joint Legislative Audit Committee tasked the California State Auditor with conducting an audit of law enforcement agencies' use of ALPR systems and data.

The 2020 report focused on four law enforcement agencies that have ALPR systems in place.[6] 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

---

[5] Los Angeles Times Editorial Board, *Private surveillance databases are just as intrusive as government ones* (February 3, 2018) Los Angeles Times, https://www.latimes.com/opinion/editorials/la-ed-license-plate-readers-privacy-congress-20180203-story.html.

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

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. All three failed to detail who had access to the systems and how it will monitor the use of the 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.

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. However, the lack of clear guidelines or auditing made it unclear exactly where information was coming from, who was accessing it, and what purposes it was being put to. The report does make clear that these agencies have "shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images." Increasing the vulnerability of such vast troves of sensitive data, the agencies' retention policies were uninformed and not tied to the usefulness of the data or the risks extended retention posed.

In fact, the Auditor had difficulty determining whether the agencies made informed decisions about sharing the ALPR data at all because of the deficient record keeping. It was discovered that two of the agencies reviewed approved sharing with hundreds of entities and one shared with over a thousand. The sharing occurred with most of the other 49 states and included public and private entities. However, the audit makes clear that ultimately it was impossible to verify the identity of each of these entities or their purpose for receiving this data.

Many of these agencies relied on Vigilant Solutions software and protocols rather than establishing their own protocols and safety measures. Vigilant is one of the largest private operators and end-users of ALPR systems, is also a provider of facial recognition technology, and provides for ALPR data storage that allows the date, time, and location information to be stored with plate images. Vigilant's parent company has since been acquired by Motorola Solutions. It operates many of the ALPR systems used by law enforcement, including 70 percent of the law enforcement users surveyed by the Auditor. However, the company indicates that it can also offer access to a data sharing network that includes over 2,650 agencies capable of data sharing and 72 billion detection records from agency and business partners.[7]

---

[7] Brochure, *Do more than just detect*, Motorola Solutions, *https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/lpr_brochure.pdf?_gl=1*mdv274*_up*MQ..*_ga*MTIzMDk5MjA4NS4xNzQ0MzUwNjc0*_ga_23THW5EV9N*MTc0NDM1MDY3NC4xLjEuMTc0NDM1MDg0NC42MC4wLjA*.*

The report indicates that for the agencies partnering with Vigilant, it was not even clear who owns the data being put into the Vigilant cloud. Serious security concerns were identified with these agencies, including the lack of contractual guarantees that the data will be stored in the United States or that adequate safeguards will be implemented. While LAPD contracts with another company, Palantir, for IT, they failed to provide an up-to-date contract with security provisions required by the FBI based on the type of data being collected.

Perhaps most disturbingly, some of these agencies have a history of sharing their ALPR information with U.S. Immigration and Customs Enforcement (ICE), and the audit reveals that they have continued to authorize "shares with entities with border patrol duties," including the San Diego Sector Border Patrol of U.S. Customs and Border Protection, Customs and Border Protection National Targeting Center, and with an unknown entity simply listed as the "California Border Patrol." The report concludes that "[a]ll of these entities' duties could potentially intersect with immigration enforcement."

Reports indicate that such sharing is not limited to the four agencies at the center of the Auditor's report. The Los Angeles Times reported that Pasadena police were found to have been sharing data from their Vigilant ALPR system directly with a Homeland Security division affiliated with ICE, and the Long Beach Police Department was found to have been sending ALPR data directly to ICE through Vigilant's "group approval" feature.[8]

While the report urges the Legislature to require DOJ to establish templates and best practices for a number of features of ALPR systems, the report indicated that their "guidelines for sharing data are particularly relevant in these cases." Despite the existence of these clear immigration-related guidelines for sharing data, "the agencies were either unaware of these guidelines or had not implemented them for their ALPR systems."

These concerns prompted Attorney General Rob Bonta to issue legal guidance to law enforcement agencies regarding their ALPR systems, emphasizing the applicable restrictions:

> SB 34 does not permit California LEAs to share ALPR information with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies. This prohibition applies to ALPR database(s) that LEAs access through private or public vendors who

[8] Suhauna Hussain & Johana Bhuiyan, *Police in Pasadena, Long Beach pledged not to send license plate data to ICE. They shared it anyway* (December 21, 2020) Los Angeles Times, https://www.latimes.com/business/technology/story/2020-12-21/pasadena-long-beach-police-ice-automated-license-plate-reader-data.

> maintain ALPR information collected from multiple databases and/or public agencies. California LEAs are encouraged to review their data user agreements to ensure that they comply with SB 34 and do not allow access to agencies other than state and local agencies, or permitted private entities for purposes of data hosting or towing services.[9]

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."

Some of the major companies intricately tied to California's ALPR systems are Flock and Palantir, in addition to Vigilant, discussed above. These companies either have direct ties to federal immigration agencies or, at the very least, have had their databases used for immigration enforcement purposes. In fact, a recent investigation found that "Vigilant Solutions provided ICE with step-by-step guides on how to get license plate data from other agencies, including local and state law enforcement agencies, and said it could give ICE access to millions more license plate scans."[10]

More recently, it was reported that a database containing, among other data, ALPR information was created by Palantir and "serves as the core law enforcement case management tool for ICE Homeland Security Investigations" and that it may be a major tool being used to help ICE in its series of increasing raids across the country.[11]

Just last Fall, CalMatters reported that state law was repeatedly violated by law enforcement agencies in Southern California:

> Law enforcement agencies across Southern California violated state law more than 100 times last month by sharing information from automated license plate readers with federal agents, records show.
>
> The Los Angeles Police Department and sheriff's departments in San Diego and Orange counties searched license plate readings on behalf of Immigration and Customs Enforcement and Customs and Border Protection, according to a database of queries obtained by anti-surveillance group Oakland Privacy and provided to CalMatters.…

---

[9] *California Automated License Plate Reader Data Guidance* (October 27, 2023) DOJ, https://oag.ca.gov/news/press-releases/attorney-general-bonta-advises-california-law-enforcement-legal-uses-and.
[10] Hussain, *supra*.
[11] Jason Koebler, *Inside a Powerful Database ICE Uses to Identify and Deport People* (April 9, 2025) 404 Media, https://www.404media.co/inside-a-powerful-database-ice-uses-to-identify-and-deport-people/.

> Among the 10 agencies that conducted searches on behalf of ICE, six are in Los Angeles County and nine are in Southern California. Two agencies, the sheriff's departments for Orange and San Diego counties, carried out searches on behalf of Customs and Border Protection or the Border Patrol.
>
> "This is a big deal, it's part of the problem, and we need the attorney general's office to start litigating," said Brian Hofer, former chair of the privacy commission for the City of Oakland.
>
> Hofer said cities can put all the sanctuary policies on the books that they want, but if they're not shutting down the data sharing between local authorities and federal agencies like ICE, those protections are meaningless.…
>
> Automated license plate readers in Riverside County are part of a system powered by Flock, a company that works with law enforcement agencies in thousands of communities nationwide. The records obtained by Privacy Oakland came from a Flock audit report generated by the Riverside County Sheriff's Office.
>
> Evidence of the sharing comes less than a week after President Trump ordered the deployment of Marines and the California National Guard to Los Angeles amid escalating protests there against deportations.[12]

Just last Fall, Attorney General Rob Bonta was forced to file a lawsuit against the City of El Cajon "over its refusal to comply with state law prohibiting the sharing of license plate data with federal and out-of-state law enforcement agencies." The practice continued even after being contacted by the Attorney General:

> After learning that the City of El Cajon was sharing ALPR data with numerous out-of-state law enforcement agencies, the Attorney General contacted the El Cajon Police Chief regarding the limitations on ALPR data-sharing in state law. Despite this and subsequent outreach, 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,

---

[12] Khari Johnson and Mohamed Al Elew, *California police are illegally sharing license plate data with ICE and Border Patrol* (June 13, 2025) CalMatters, https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/#:~:text=An%20annual%20surveillance%20report%20released,hypothetical%20anymore%2C%E2%80%9D%20she%20said.

North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Texas, Utah, Virginia, Washington, and Wisconsin.[13]

4. Responding to the lack of transparency, accountability, and security

The Auditor's report provides several recommendations for the Legislature "[t]o better protect individuals' privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use." They urge the Legislature to do the following:

- Require the California Department of Justice (DOJ) to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.
- Require DOJ to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
- Establish a maximum data retention period for ALPR images.
- Specify how frequently the ALPR system use must be audited and that the audits must include assessing user searches.

This bill attempts to implement several of these recommendations and applies them to a broader universe of ALPR operators and end-users.[14] The bill provides that all SB 34-mandated usage and privacy policies must indicate the purpose for which employees and contractors are authorized to use or access the ALPR systems. Currently, ALPR operators and end-users are required to maintain reasonable security measures and practices. This bill requires that this must include:

- 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.
- Requiring data security training and data privacy training for all employees who access ALPR information.

This works to ensure greater controls over ALPR system access and data sharing.

---

[13] Press Release, *Attorney General Bonta Sues El Cajon for Illegally Sharing License Plate Data with Out-of-State Law Enforcement* (October 3, 2025) California Department of Justice, https://oag.ca.gov/news/press-releases/attorney-general-bonta-sues-el-cajon-illegally-sharing-license-plate-data-out.

[14] The Brennan Center for Justice also put out a detailed report on ALPR systems in which they similarly recommend strict retention limits and regular auditing. *See* Angel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use* (September 10, 2020) Brennan Center for Justice, https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.

The bill requires DOJ to conduct random annual audits of public agency ALPR operators and end-users to determine whether they have implemented a compliant usage and privacy policy. This is contingent on appropriation, as provided.

For public agencies, the bill also establishes a 30-day retention period for ALPR information that does not match specified hot lists. This mirrors language in other bills that have been considered by the Legislature, including SB 210 (Wiener, 2021), which limited retention to 24 hours or less.

Moving forward, public agencies are 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.

These requirements work toward addressing the privacy and security concerns highlighted above. The bill is nearly identical to SB 274 (Cervantes, 2025), which was passed by the Legislature, but vetoed by Governor Newsom, who stated:

> 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.

5. Stakeholder positions

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 planning to use them in the future. Senate Bill 34 by Senator 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 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."

A coalition of law enforcement agencies, including the Palos Verdes Police Officers' Association, writes in opposition:

> **Existing Safeguards Already in Place**
> Law enforcement agencies already operate under strict policies governing ALPR use, including audit requirements, access controls, and compliance with state and federal privacy laws. Misuse of ALPR data is taken seriously and subject to disciplinary action and even criminal prosecution when warranted. SB 1013 imposes redundant and overly burdensome restrictions that do not meaningfully enhance privacy protections but will undermine legitimate law enforcement functions.
>
> **Unintended Consequences**
> The practical effect of SB 1013 would be to weaken law enforcement capabilities while providing a tactical advantage to criminals who are increasingly sophisticated and mobile. Reducing access to ALPR data will not deter criminal behavior—it will only make it more difficult to detect, investigate, and prevent it.

Writing in opposition, the California Police Chiefs Association (CPCA) argues for a different retention approach:

> CPCA has previously worked collaboratively with the Legislature on this issue and offered a balanced amendment framework in connection that

> would protect privacy while preserving the utility of ALPR systems. Specifically, CPCA proposed allowing data to be retained for up to two years, followed by "logical deletion," whereby the data is no longer accessible to general users and is flagged within the system. Under that approach, access to logically deleted data would be limited to administrators and permitted only for significant offenses and serious/violent felony investigations, including crimes such as human trafficking, witness intimidation, stalking, and organized theft, or pursuant to a court order. The proposal would also require permanent deletion after five years, except where the data is needed for prosecution or administrative proceedings. This framework ensures strong privacy protections, strict access controls, and accountability, while preserving the ability to investigate the most serious crimes.

Writing in support, Oakland Privacy asserts:

> To be clear, the leaks to immigration from California's law enforcement ALPR databases are happening in three different ways:
>
> a) By individual law enforcement officers in CA agencies running searches on behalf of federal agents, including Homeland Security Investigations (HSI-ICE) and Customs and Border Patrol (CBP).
> b) By some California law enforcement agencies continuing to share their ALPR scans out of state with law enforcement agencies that are in 287(g) agreements with ICE, as well as having state bans on reproductive and gender care in place, years after the CA Attorney General told them to stop. Recently identified ones include police departments in El Monte, El Cajon and Salinas. The Attorney General of California filed suit against the El Cajon Police Department when they refused to stop out of state sharing. We note that the existing statute from 2015 (Senate Bill 34) has been serially violated by dozens of California law enforcement agencies over the last decade. Opposition claims that existing state law is robust don't correspond with the facts.
> c) A secretive pilot program at Flock Safety gave access to over 80,000 cameras and millions of scans to Customs and Border Patrol for more than 3 months, exactly as that agency was terrorizing Southern California. The program did not stop until it was outed in the media by a leak inside the company. 8 Law enforcement agencies did not know CPB had access to their stored scans in the cloud.

Enraged communities in Colorado, Illinois and Texas have already convinced their local governments to entirely deactivate all of their their automated license plate readers. Cities in California including Mountain View, Santa Cruz and South Pasadena have decommissioned their equipment. If California wants to protect its large financial investment in license plate readers, it is absolutely necessary to take immediate steps to stop the leaks and tighten up the regulatory regime.

Automated license plate readers are high-speed cameras mounted to traffic poles or law enforcement vehicles that take high speed searchable images of license plates from passing cars and stamp them with the date, time and location they were captured. These images are then automatically uploaded to privately held vendor databases in the cloud that are accessed by thousands of law enforcement agencies nationwide. Scan data is shared in these cloud storage systems by providing query-based access to the agency's entire collection of automated license plate scan data. There are also some non-law enforcement entities (like transit agencies) that use ALPR systems as well as a private marketplace that includes HOA's, but law enforcement constitutes the largest sector of use.

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.

SUPPORT

Oakland Privacy

OPPOSITION

Arcadia Police Officers' Association
Brea Police Association
Burbank Police Officers' Association
California Narcotic Officers' Association
California Police Chiefs 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
League of California Cities
Murrieta Police Officers' Association
Newport Beach Police Association
Palos Verdes Police Officers Association
Placer County Deputy Sheriffs' Association
Pomona Police Officers' Association
Riverside Police Officers Association
Riverside Sheriffs' Association

RELATED LEGISLATION

SB 274 (Cervantes, 2025) *See* Comment 4.

AB 1355 (Ward, 2025) would have established the California Location Privacy Act. Among other things, it would prohibit covered entities from collecting or processing the location information, which includes ALPR data, of an individual unless doing so is necessary to provide goods or services requested by that individual, and only to the extent needed and only for as long as needed. AB 1355 would have prohibited selling, renting, trading, or leasing location information to third parties and made it unlawful for a covered entity or service provider to disclose location information to any federal, state, or local government agency or official, except as provided. AB 1355 died in the Assembly Appropriations Committee.

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. AB 1463 died in the Senate Judiciary Committee.

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) 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. It died in the Senate Appropriations Committee.

SB 34 (Hill, Ch. 532, Stats. 2015) *See* Comment 2.

PRIOR VOTES:

Senate Transportation Committee (Ayes 9, Noes 3)

****