Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

UNFINISHED BUSINESS

Bill No: SB 274
Author: Cervantes (D), et al.
Amended: 9/5/25 in Assembly
Vote: 21

SENATE JUDICIARY COMMITTEE: 10-2, 4/22/25
AYES: Umberg, Arreguín, Ashby, Caballero, Durazo, Laird, Stern, Wahab, Weber Pierson, Wiener
NOES: Niello, Valladares
NO VOTE RECORDED: Allen

SENATE PUBLIC SAFETY COMMITTEE: 5-1, 4/29/25
AYES: Arreguín, Caballero, Gonzalez, Pérez, Wiener
NOES: Seyarto

SENATE APPROPRIATIONS COMMITTEE: 5-1, 5/23/25
AYES: Caballero, Cabaldon, Grayson, Richardson, Wahab
NOES: Seyarto
NO VOTE RECORDED: Dahle

SENATE FLOOR: 26-10, 6/3/25
AYES: Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Cortese, Durazo, Gonzalez, Grayson, Laird, Limón, McGuire, McNerney, Menjivar, Padilla, Pérez, Richardson, Rubio, Smallwood-Cuevas, Umberg, Wahab, Weber Pierson, Wiener
NOES: Alvarado-Gil, Choi, Dahle, Grove, Jones, Niello, Ochoa Bogh, Seyarto, Strickland, Valladares
NO VOTE RECORDED: Allen, Hurtado, Reyes, Stern

SENATE FLOOR: 39-0, 6/3/25
AYES: Allen, Alvarado-Gil, Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Choi, Cortese, Dahle, Durazo, Gonzalez, Grayson, Grove, Hurtado, Jones, Laird, Limón, McGuire, McNerney, Menjivar, Niello, Ochoa Bogh, Padilla, Pérez, Richardson, Rubio, Seyarto, Smallwood-Cuevas, Stern, Strickland, Umberg, Valladares, Wahab, Weber Pierson, Wiener

NO VOTE RECORDED: Reyes

ASSEMBLY FLOOR: 41-28, 9/13/25 – Roll call vote not available.

---

**SUBJECT:** Automated license plate recognition systems

**SOURCE:** Author

---

**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 annually to ensure compliance with their usage and privacy policies, as provided. This bill places retention limits on ALPR data, with exceptions.

*Assembly Amendments* of 9/5/25 add exceptions and additional protections.

**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. Article. 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 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, as specified.
   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 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).)

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 60 days after the date of collection.

**Background**

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 providing for audits and requiring 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 60 days if it does not match information on a hot list.

This bill is author-sponsored. It is supported by the California Public Defenders Association. It is opposed by a coalition of law enforcement groups. For a more thorough assessment, please see the Senate Judiciary Committee analysis of this bill.

**Comment**

*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.[1] 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. 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.

According to the author:

> 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

[1] *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**.

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. 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 chill fundamental freedoms of speech. ICE's contract allowing access to ALPR databases has emerged at a critical moment when concerns are escalating regarding the implications of data collection and retention practices, as well as the ongoing operations of immigration enforcement. These developments threaten to undermine the foundational goals of sanctuary city laws meant to protect vulnerable immigrant communities within our state.

ALPR technology also poses a risk to individuals who frequent sensitive locations like health care facilities, immigration clinics, gun shops, labor union halls, protest sites, and places of worship. Using this technology to monitor and target vehicles in these areas can create a chilling effect, discouraging individuals from seeking necessary services or participating in civic engagement due to fear of being tracked or apprehended by immigration authorities. 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. Law enforcement agencies that do not have their own ALPR systems can access data collected by other agencies through regional sharing systems and networks operated by these private firms. Senate Bill 274 would prohibit public agencies from using ALPR systems to collect geolocation data at specific locations for immigration enforcement purposes and would limit the retention of ALPR information to no more than 30 days.

> The temptation to "collect it all" should never overshadow the critical responsibility to "protect it all." Senate Bill 274 is a significant legislative measure aimed at establishing robust safeguards and crucial oversight regarding the use of ALPR throughout our state. This bill is designed to ensure that the privacy of Californians is respected and preserved, while also maintaining compliance with existing sanctuary laws that safeguard vulnerable communities. Under this bill, public safety agencies will be required to collect only the data necessary for legitimate criminal investigations, thereby preventing any potential misuse of ALPR technology. Specifically, the legislation prohibits the use of ALPR information for immigration enforcement purposes, ensuring that local law enforcement agencies do not overreach or compromise the trust of the communities they serve. By implementing these measures, Senate Bill 274 aims to strike a balance between enhancing public safety and protecting individual privacy rights in our increasingly digitized world.

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

According to the Senate Appropriations Committee:

- Department of Justice (DOJ): Unknown, potentially significant workload costs pressures (General Fund) to the DOJ to audit any public agency that is an ALPR operator or ALPR end-user to determine whether they have implemented a usage and privacy policy.

State and Local Agencies: Unknown, potentially significant costs (General Fund, local funds) to state and local agencies, including any law enforcement agency that uses ALPRs. If the Commission on State Mandates determines these costs to constitute a reimbursable state mandate, the state may need to reimburse these local costs.

According to the Assembly Appropriations Committee:

1) Ongoing annual costs (General Fund) of an unknown but substantial amount, likely in the high hundreds of thousands of dollars annually, to DOJ to conduct annual random audits of each public agency that is an ALPR operator or end-user. The DOJ did not provide its estimate of costs, but affirmed it interprets the bill as requiring DOJ to conduct an annual in-person audit of each public agency that is an ALPR operator or end-user to determine whether the agency has complied with the requirements of state law and with the agency's own privacy policy.

2) Annual costs (various funds) of an unknown amount, but likely in the hundreds of thousands of dollars at least, to each state agency that operates ALPRs, such as the California Highway Patrol.

3) Potential annual costs (General Fund) of an unknown amount, but likely in the hundreds of thousands of dollars at least, to reimburse local public agency costs to comply with this bill. The state would incur these cost only if a local agency or agencies filed a claim with the Commission on State Mandates and the commission determined the state liable for reimbursement.

**SUPPORT:** (Verified 9/11/25)

California Public Defenders Association
Surveillance Technology Oversight Project

**OPPOSITION:** (Verified 9/11/25)

Arcadia Police Officers' Association
Brea Police Association
Burbank Police Officers' Association
California Association of School Police Chiefs
California Coalition of School Safety Professionals
California Narcotic Officers' Association
California Police Chiefs Association
California Reserve Peace Officers Association
California State Sheriffs' Association
City of Los Alamitos
City of Thousand Oaks
Claremont Police Officers Association
Corona Police Officers Association
Culver City Police Officers' Association
Electronic Frontier Foundation
Fullerton Police Officers' Association
Los Angeles School Police Management Association
Los Angeles School Police Officers Association
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

Sacramento County Sheriff Jim Cooper
Santa Ana Police Officers Association

**ARGUMENTS IN SUPPORT:** Surveillance Technology Oversight Project writes:

Fusion centers in California and across the nation routinely facilitate ICE's access to ALPR data, violating state and local protections for undocumented immigrants and allowing ICE to easily and efficiently intercept the individuals it targets. Cutting off ALPR data access is essential to blocking the mass deportation of Californians.

Senate Bill 274 will hold local law enforcement accountable if it shares ALPR data in violation of California's sanctuary laws, ending the current status quo, which allows that sharing without consequences. Beyond this, it is an important privacy measure for all Californians: SB 274 will eliminate the over-long storage of data that reveals all California drivers' life patterns, including where they live, work, socialize, and worship.

**ARGUMENTS IN OPPOSITION:** A coalition of law enforcement agencies, including the California Coalition of School Safety Professionals, writes:

While we appreciate the author's effort to permit law enforcement to access LPR data when the information is used as evidence or for all felonies being investigated, there is no way to know in advance when the LPR data will be used as evidence or for a felony that has not yet been committed.

Additionally, the restrictions imposed by SB 274 would prevent investigators from accessing the LPR data for misdemeanors, including violent misdemeanors.

As currently amended, SB 274 will significantly hamper the ability of law enforcement to effectively investigate crimes throughout the state by requiring the deletion of LPR data after 30 days, thereby preventing investigators from using the LPR data to investigate crimes which occurred more than 30 days ago.

Prepared by: Christian Kurpiewski / JUD. / (916) 651-4113
9/13/25 0:32:39

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