Date of Hearing: July 7, 2025

ASSEMBLY COMMITTEE ON TRANSPORTATION
Lori D. Wilson, Chair
SB 274 (Cervantes) – As Amended May 23, 2025

SENATE VOTE: 26-10

SUBJECT: Automated license plate recognition systems

SUMMARY: Prohibits a public agency from retaining automated license plate reader (ALPR) information that does not match information on a hot list for more than 60 days after the date of collection. Specifically, **this bill**:

1) Defines "hot list" as a list or lists of license plates of vehicles of interest against which the ALPR system is comparing vehicles on the roadways.

2) Requires an ALPR operator to institute 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.

3) Requires ALPR operators to require data security training and data privacy training for all employees that access ALPR information.

4) Requires the Department of Justice to conduct annual random audits on a public agency that is an ALPR operator or ALPR end-user to determine whether they have implemented a usage and privacy policy in compliance with the law.

EXISTING LAW:

1) Defines "automated license plate recognition system" or "ALPR system" to mean a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data. "ALPR information" means information or data collected through the use of an ALPR system. "ALPR operator" means a person that operates an ALPR system, except as specified. "ALPR end-user" means a person that accesses or uses an ALPR system, except as specified. The definitions for both ALPR operator and ALPR end-user exclude transportation agencies when subject to Section 31490 of the Streets and Highways Code. (Civil Code section (CIV) 1798.90.5.)

2) 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 1798.90.51

3) 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; and,
        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 1798.90.52)

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

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

6) 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 Code section (VEH) 2413(b))

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

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

9) 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 2413(e))

10) Establishes the data breach notification law, which requires any agency, person, or business that owns, licenses, or maintains data including personal information to disclose a breach, as provided. (CIV 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 1798.29(g), 1798.82(h)

FISCAL EFFECT: According to 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.

COMMENTS: According to the United States Department of Justice, the Police Scientific Development Branch in the United Kingdom (U.K.) invented ALPR technology in 1976. The technology rose to prominence after Provisional Irish Republican Army terrorist bombings in the City of London that resulted in the establishment of a surveillance and security network around the city referred to as the "ring of steel" in 1993.

ALPR systems are capable of capturing information on up to 1,800 plates per minute at speeds of 120-160 miles per hour. According to the Brennan Center for Justice, ALPR systems can be mounted on stationary poles, moving police cruisers, and handheld devices. The devices log pictures of the vehicles, and their GPS coordinates. This data can be compared against "hot lists" to find vehicles that have been stolen or help find an abducted child.

Law enforcement agencies use of ALPR was prevalent across the United States by the mid-2000s. The 2007 Law Enforcement Management and Administrative Statistics Survey indicated that as of 2007, 48% of law enforcement agencies with more than 1,000 sworn officers were regularly using ALPR readers, with 32% of agencies with greater than 500 officers, but less than 1,000.

California's use of ALPRs and legislative response: ACLU in a 2013 report indicated that law enforcement was collecting and storing ALPR images related to individuals not suspected of a crime, and that this data could be used inappropriately to monitor the movements of individuals such as ex-spouses, neighbors, and other associates. Such information could be used to locate places people regularly visit, to determine their acquaintances, and to blackmail them based on this information.

Out of increasing concern surrounding the privacy of individuals data collected through ALPR systems, SB 34 (Hill), Chapter 532, Statutes of 2015 was enacted. SB 34 imposed a range of privacy protections on ALPR data, including requiring ALPR operators to secure information collected by ALPR systems with reasonable operational, administrative, technical, and physical safeguards to ensure confidentiality and integrity. According to Senator Hill at the time, "California law has not kept up with the rapid adoption of the technology. Except for the California Highway Patrol and transportation agencies, current California law doesn't require

any privacy safeguards or establish any protocols for the use of ALPR systems. Not only has the law failed to keep up with the quick adoption of ALPR, but the entities using ALPR have also been slow in crafting their own internal policies. For example, according to the International Association of Chiefs of Police, only 48% of police agencies across the country have developed policies that govern ALPR use and privacy."

In 2019 the State Auditor reviewed four local law enforcement agencies use of ALPR and found that these agencies were accumulating massive amounts of data unrelated to criminal investigations. Also, the Auditor found that none of the agencies they reviewed were complying with the requirements set forth in SB 34, and that the Los Angeles Police Department (LAPD) had no ALPR policy at all. The other three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data. For example, of the 320 million images LAPD had collected, only 400,000 generated an immediate match against a hot list. In addition, the State auditor conducted a statewide survey of law enforcement agencies and found that 70% operate or plan to operate an ALPR system, and that 84% 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."

The State Auditor found that "ALPR systems should be accessible only to employees who need the data, and accounts should be promptly disabled otherwise. However, the agencies often neglected to limit ALPR system access and have allowed accounts that should be disabled to remain active longer than is prudent. To further ensure that individuals with access do not misuse the ALPR systems, the agencies should be auditing the license plate searches that users perform, along with conducting other monitoring activities. Instead, the agencies have conducted little to no auditing and monitoring and thus have no assurance that misuse has not occurred."

The State Auditor recommended that the Department of Justice (DOJ) draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies, and that DOJ 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. It also suggests the Legislature set a requirement for when law enforcement agencies should delete ALPR data. The State Auditor recommended that the Legislature should establish a maximum data retention period for ALPR images.

In October of 2023, the DOJ released two information bulletins providing guidance to California state and local law enforcement agencies regarding the governance of ALPRs. According to the guidance, the DOJ believes California law prohibits ALPR information from being shared with federal agencies or local agencies outside of the state of California. The bulletin included a template use policy that recommended law enforcement agencies maintain the data for 60 days to six months. Flock Securities, the ALPR company most prominently used in California, has a 30 day retention policy.

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 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 chill fundamental freedoms of speech."

The California Public Defenders Association, *writing in support of this bill*, argues "Limiting use of ALPR use which could be used for immigration enforcement at sensitive locations is a positive step towards protecting these important places. California is home to more immigrants than any other state in the country. Nearly half of working households in California include immigrants and over half of all California workers are either immigrants or the children of immigrants. Immigrants are an integral part of the fabric of Californian society, contributing to its economy, culture, and workforce, and bringing innovation, and enrichment to our workplaces, schools, faith communities, and neighborhoods. Now more than ever, it is imperative to protect our immigrant community members from the federal attack on noncitizen residents."

The California Police Chiefs Association (CPCA), *writing in opposition to this bill*, argue "CPCA understands the need to protect against unscrupulous searches and unwarranted invasion of individual privacy, which is why our ALPR operations are highly audited and regulated by existing law. These protections, however, still allow law enforcement to utilize the data collected by ALPRs in a manner that is critical to solving and preventing crime in our communities. The number one deterrent that prevents crime is creating a perception that perpetrators will be caught for unlawful acts, and ALPR systems only help increase that perception.

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."

CPCA has asked the Legislature to codify LAPD record retention policy as a statewide policy. LAPD keeps ALPR data for five years. After two years LAPD "logically" deletes the data so only a system administrator can access the data for a limited set of crimes.

Privacy rights organizations, like the Electronic Frontier Foundation, have removed their support from this bill after Senate amendments extended the record retention allowance from 30 days to 60 days.

Previous Legislation: SB 34 (Hill), Chapter 532, Statutes of 2015 established regulations on the privacy and usage of automatic license plate recognition (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 of 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 this Committee.

AB 2192 (Ramos of 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 the 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. That bill passed out of this committee and was taken up in Assembly Privacy and Consumer Protection for testimony only.

SB 210 (Wiener of 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 of 2020) was largely identical to AB 1463 and was held under submission in the Senate Transportation Committee.

AB 1782 (Chau of 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.

REGISTERED SUPPORT / OPPOSITION:

Support

California Public Defenders Association
Surveillance Technology Oversight Project

Opposition

Arcadia Police Officers' Association
Brea Police Association
Burbank Police Officers' Association
California Association of School Police Chiefs
California Coalition of School Safety Professionals
California Civil Liberties Advocacy (unless amended)
California Narcotic Officers' Association
California Police Chiefs Association
California Reserve Peace Officers Association
California State Sheriffs' Association
City of Thousand Oaks
Claremont Police Officers Association
Corona Police Officers Association
Culver City Police Officers' Association
Fullerton Police Officers' Association
Los Angeles County Sheriff's Department
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 County Sheriff's Office
Riverside Police Officers Association
Riverside Sheriffs' Association
San Diego Sheriff’s Office
Santa Ana Police Officers Association

Analysis Prepared by: David Sforza / TRANS. / (916) 319-2093