Date of Hearing: July 1, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 1013 (Cervantes) – As Amended June 15, 2026

SENATE VOTE: 28-9

SUBJECT: Automated license plate recognition systems

SYNOPSIS

Automated License Plate Recognition (ALPR) systems are searchable computerized databases resulting from the operation of one or more cameras combined with computer algorithms to capture and convert images of license 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.

Investigations, discussed in detail in Comments #4 and 5, have determined that law enforcement officers, including some in California, continue to misuse the data by sharing it with federal immigration officials, in direct violation of the law; sharing it with other states that are searching for people seeking abortion care, also in direct violation of the law; and, using it to surveil women they either have an interest in, are in a relationship with, or who are former partners. To curb further abuses by law enforcement associated with these systems, this bill provides additional restrictions related to the use of ALPR data and time frames for how long ALPR data may be kept by government entities unless the data is directly related to an active investigation or case.

This bill is supported by the California Initiative for Technology & Democracy (CITED) and Oakland Privacy. It is opposed by a number of law enforcement organizations and cities.

This bill was previously heard by the Transportation Committee, where it passed on an 11 – 4 vote.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

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

provisions of the Streets and Highways Code that apply to electronic toll collection. (Civ. Code § 1798.90.5.)

3) Requires an ALPR operator to maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. ALPR operators must implement usage and privacy policies in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. It further requires the policies to include, at a minimum, certain elements. (Civ. Code § 1798.90.51.)

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

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

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

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

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

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

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

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

12) Establishes the California Values Act, which prohibits state law enforcement from using state resources to assist in the enforcement of federal immigration law, except as specified. (Gov. Code § 7282 et seq.)

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

14) Establishes the Reproductive Privacy Act, which provides that the Legislature finds and declares that every individual possesses a fundamental right of privacy with respect to personal reproductive decisions, which entails the right to make and effectuate decisions about all matters relating to pregnancy, including prenatal care, childbirth, postpartum care, contraception, sterilization, abortion care, miscarriage management, and infertility care. Accordingly, it is the public policy of the State of California that:

    a. Every individual has the fundamental right to choose or refuse birth control.

    b. Every individual has the fundamental right to choose to bear a child or to choose to obtain an abortion, with specified limited exceptions.

    c. The state shall not deny or interfere with a person's fundamental right to choose to bear a child or to choose to obtain an abortion, except as specifically permitted. (Health & Saf. Code § 123462.)

15) Provides that the state may not deny or interfere with a person's right to choose or obtain an abortion prior to viability of the fetus or when the abortion is necessary to protect the life or health of the person. (Health & Saf. Code § 123466 (a).)

16) States that a person shall not be compelled in a state, county, city, or other local criminal, administrative, legislative, or other proceeding to identify or provide information that would identify or that is related to an individual who has sought or obtained an abortion if the information is being requested based on either another state's laws that interfere with a person's rights under subdivision (a) or a foreign penal civil action. (Health & Saf. Code § 123466(b).)

THIS BILL:

1) Defines the following terms:

    a. "Case file number" means a reference number pertaining to a specific law enforcement or public safety incident or investigation.

    b. "Hot list" means a list or lists of license plates of vehicles of interest against which the ALPR system is comparing vehicles on the roadways.

2) Limits authorized hot lists to the following:

a. The National Crime Information Center (NCIC) list.

b. The National Center for Missing and Exploited Children (NCMEC) list.

c. The Stolen Vehicle System (SVS).

d. California Department of Justice lists.

e. Official alerts, including AMBER, Silver, Feather, Blue, Yellow, Ebony, and any new alerts authorized by the Legislature.

f. Custom BOLO lists that pertain solely to missing and at-risk people, witness locations, burglaries, grand theft, and violent crimes.

3) 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.

4) Requires the 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.

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

6) 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.

7) 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.

8) 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.

9) 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.

10) 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.

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

12) Requires a public agency, as of January 1, 2027, to delete all ALPR information that has been held for more than 30 days, 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.

13) 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.

14) 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.

COMMENTS:

1) **Author's statement**. 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 10agencies 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 operators 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) **Background**. Automated License Plate Recognition (ALPR) systems are searchable computerized databases resulting from the operation of one or more cameras combined with computer algorithms to capture and convert images of license 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. These cameras continuously record the plates, color, and brand of vehicles passing in front of them. Law enforcement can then perform searches to see where exactly a vehicle, and by extension person, was at a certain time or map out their movements across a wide date range.[1] ALPR data can have legitimate uses, including for law

[1] Jason Koebler and Joseph Cox, "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows," *404 Media* (May 27, 2025) https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/.

enforcement purposes. While such systems may be useful, there are serious privacy concerns associated with the collection, storage, disclosure, sharing, and use of ALPR data.[2]

In 2015, SB 34 (Hill, Chap. 532, Stats. 2015) sought to address some of the concerns about the privacy of the information collected by these systems by placing certain protections around the operation of ALPR and the use of the data.[3] The resulting statutes provide that both ALPR operators and ALPR end-users are 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. These operators and end-users are 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.

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:

1. The authorized purposes for using the ALPR system, and collecting, accessing, and/or using ALPR information.

2. 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. Necessary training requirements must also be identified.

3. A description of how the ALPR system will be monitored to ensure (a) the security of the ALPR information, and (b) compliance with all applicable privacy laws.

4. A process for periodic system audits for end-users.

5. The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.

6. The title of the official custodian, or owner, of the ALPR information responsible for implementing the relevant practices and policies.

7. A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.

8. 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.

3) **California State Audit Report.** In response to the growing concerns with ALPR systems, the Joint Legislative Audit Committee in 2019 tasked the California State Auditor with conducting an audit of law enforcement agencies' use of ALPR systems and data.

---

[2] 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].
[3] See Civ. Code §§ 1798.90.51, 1798.90.53.

The resulting report, released in February 2020, focused on four law enforcement agencies that have ALPR systems in place. The report found that "the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use." In addition, the audit found that three of the four agencies failed to establish ALPR policies that included all of the elements required by SB 34. 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.[4]

The Auditor's report calls into question how these systems are being run, how their 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, illustrating 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 the information 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.[5]

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 data sharing with hundreds of entities and one shared data 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.[6]

The Auditor's report demonstrated that some law enforcement agencies are either accidentally or deliberately violating the state's privacy laws. This bill seeks to rein in that behavior.

4) **Law enforcement misuse of ALPR systems.** A 2025 investigation into the Flock Safety ALPR system by *404 Media*, an independent media company that specializes in technology, found more than 4,000 nation and statewide lookups by local and state police nationwide done either at the behest of the federal government or as an informal favor to federal law enforcement, or with a potential immigration focus.[7] According to the report:

> The fact that police almost never get a warrant to perform a Flock search means that there is not as much oversight into its use, which leads to local police either formally or informally helping the feds by doing lookups.

---

[4] State Auditor Report, *supra.*
[5] *Ibid.*
[6] *Ibid.*
[7] Koebler and Cox, *supra*.

> "Law enforcement really likes license plate readers because of the lack of restrictions on that data. They don't feel like they need a warrant. Oftentimes there are no restrictions whatsoever on what they search," Dave Maass, who studies border technology at the Electronic Frontier Foundation, told 404 Media. "It might be totally true that some of these searches are for people who have warrants or who are wanted for criminal activity. They might be looking for a terrorist, who knows. But that's kind of the point—we don't know."[8]

In an extension of their research, *404 Media* found that law enforcement authorities in Texas performed a nationwide search of over 83,000 Flock ALPR cameras in a search for a woman who they claim had a self-administered abortion. The article notes:

> The news shows in stark terms how police in one state are able to take the ALPR technology, made by a company called Flock and usually marketed to individual communities to stop carjackings or find missing people, and turn it into a tool for finding people who have had abortions. In this case, the sheriff told 404 Media the family was worried for the woman's safety and so authorities used Flock in an attempt to locate her. But health surveillance experts said they still had issues with the nationwide search.
>
> "You have this extraterritorial reach into other states, and Flock has decided to create a technology that breaks through the barriers, where police in one state can investigate what is a human right in another state because it is a crime in another," Kate Bertash of the Digital Defense Fund, who researches both ALPR systems and abortion surveillance, told 404 Media.[9]

The search by the officer logged the reason as "had an abortion, search for female."[10] Ashley Emery, senior policy analyst in reproductive health and rights at the National Partnership for Women & Families, told *404 Media*:

> The risks of this intrusive government monitoring cannot be overstated: law enforcement could deploy this surveillance technology to target and try to build cases against pregnant people who travel for abortion care and those who help them. This incident is undeniably a harbinger of more AI-enabled reproductive surveillance and investigations to come. Especially for women of color who are already over-surveilled and over-policed, the stakes couldn't be higher.[11]

As for California law enforcement activities, a suit was filed against the Marin County Sheriff in October 2021 alleging that despite laws against sharing ALPR data out of state and with the federal government, since 2010 the Sheriff's Office had been forwarding scans from ALPR cameras to out-of-state and federal agencies, including U.S. Immigration and Customs Enforcement, which has used the information to track and deport people who have immigrated to the United States.[12] In the June 2022 settlement agreement, the Sheriff agreed to start complying

---

[8] *Ibid*.
[9] Joseph Cox and Jason Koebler, "A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion," *404 Media* (May 29, 2025) https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/.
[10] *Ibid*.
[11] *Ibid*.
[12] Nikki Silverstein, "Marin Sheriff agrees to obey the law as part of legal settlement," *Pacific Sun* (June 8, 2022) https://pacificsun.com/marin-sheriff-settlement/.

with state laws and stop sharing the information.[13] The other example is the Vallejo police department, which captured over 400,000 license plates a month and had been sharing their data with law enforcement in Arizona and Texas, according to an October 2022 article in *The Guardian*.[14]

In 2025, a *CalMatters* report found that Southern California law enforcement agencies violated state law more than 100 times in one month by sharing information from automated license plate readers. 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.[15]

According to *CalMatters*:

> This log is where police searching Riverside County data revealed their cooperation with ICE, often using the term "HSI," referring to the agency's Homeland Security Investigations unit. The term "CBP" was also repeatedly listed as a search purpose.
>
> 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 the behalf of Customs and Border Protection or the Border Patrol.[16]

5) **The use of ALPR data by law enforcement to harass, stalk, and harm women.** A recent investigation by the Institute of Justice found that law enforcement officers throughout the country had been discovered tracking their romantic interests, including current and ex partners, and even strangers who unwittingly caught their eye in public.[17] While the investigation was only able to uncover 20 cases, the bulk of them had happened since 2024. The investigation also found that "Flock Safety and other ALPR providers emphasize that they have internal safeguards to prevent this kind of misuse. But only a few of the 20 analyzed cases were initially discovered through internal investigations, according to media reports. Most incidents came to light only after victims reported the officers' behavior to the police, typically in the context of a broader stalking allegation."[18]

As it relates to this subject, the author notes:

> We also face the unfortunate truth that access to ALPR data can be abused to perpetrate crimes including sexual harassment, domestic violence, and stalking. A 2016 investigation by the Associated Press found that law enforcement officers across the country have abused

---

[13] *Ibid.*
[14] Johana Bhuiyan, "How expanding web of license plate readers could be 'weaponized' against abortion," *The Guardian* (Oct. 6, 2022) https://www.theguardian.com/world/2022/oct/06/how-expanding-web-of-license-plate-readers-could-be-weaponized-against-abortion?ref=vallejosun.com.
[15] Khari Johnson and Mohamed Al Elew, "California police are illegally sharing license plate data with ICE and Border Patrol," *CalMatters* (Jun. 13, 2025) https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/.
[16] *Ibid*.
[17] Christopher Ingraham, "Police Have Reportedly Used License Plate Readers to Stalk Romantic Interests at Least 20 Times in Recent Years," *Institute for Justice* (April 27, 2026) https://ij.org/police-have-reportedly-used-license-plate-readers-to-stalk-romantic-interests-at-least-14-times-in-recent-years/.
[18] *Ibid.*

their ability to access databases with confidential information to illicitly track love interests, journalists, and business associates. In Shasta County, an officer used ALPR data to harass the ex-boyfriend of his fiancée and was charged with six misdemeanors after he used this data to have the ex-boyfriend's truck towed and impounded. In San Diego, investigators discovered that a sergeant in the San Diego Police Department had used ALPR data to obtain information on his ex-girlfriend's new boyfriend. He used this information to stalk both his ex and her boyfriend.

6) **What this bill would do.** The author introduced this bill to strengthen the regulations around the searching and amassing of ALPR data, particularly data that is not related to any criminal investigation. In order to do that, the bill makes several significant additions to the state's current ALPR laws:

- Requires that license plate data that does not match information contained on a "hot list" must be deleted within 30 days.

- Requires that within 14 days of enactment, public agencies must delete all of their stockpile of ALPR data that is more than 30 days old unless it is retained in the evidence file of an active investigation, criminal proceeding, or matches information on an authorized hot list.

- Requires an ALPR operator to institute safeguards for managing which employees can see the data from their systems.

- Requires data security training and data privacy training for all employees that access ALPR information.

- Requires an ALPR user to retain a record of all access, including a case file number that justifies the search. Prohibits the ALPR search without a valid and current case number.

- Requires the Department of Justice (DOJ) to conduct annual random audits of agencies using ALPR to determine whether they have implemented a usage and privacy policy and are complying with the law.

7) **Analysis of this bill.** The question before this Committee is whether this bill strikes the right balance between protecting people against excessive surveillance and ensuring law enforcement can do its job.

As discussed in this Committee's informational hearing on surveillance earlier this year, Californians have largely lost the ability to live their lives in private and there can be significant consequences due to that loss. As discussed in the hearing background paper:

> In the physical world, we cannot step out of our homes without being monitored and tracked. Cars collect location data everywhere we drive. Phones, our constant companions, collect location data everywhere we go. License plate readers and traffic cameras are at virtually every intersection, on freeways and toll roads, at the entrance of parking garages, and in store parking lots. These devices track the movement of every single car that passes by. Even if someone walks or rides a bicycle, security cameras on homes and business can capture their movements and their location. Our faces may not be captured by these cameras, but

> technological advancements can analyze a person's walk and movements using gait recognition technology and identify them.[19] In addition, most stores and businesses use security cameras and images from those cameras can easily be run through facial recognition systems to identify the people walking through their doors.[20]

This bill importantly puts limits on a significant surveillance tool being used by government agencies. Perhaps the most significant provision in the bill is the provision requiring agencies to purge data that has been held for more than 30 days and is not associated with an active investigation.

Under current law, there are no restrictions against law enforcement agencies amassing large stores of license plate data. As an example, the ALRP audit report found that in the Los Angeles ALPR database, "only 400,000 of the 320 million images it has accumulated over several years and stores in its database generated an immediate match against its hot lists. In other words, 99.9 percent of the ALPR images Los Angeles stores are for vehicles that were not on a hot list at the time the image was made."[21] Given the massive volume of images being stored in these databases, it makes the previous discussion related to the Marin County Sheriff's Department collecting data on perhaps millions of license plates as people drove on the highways through Marin County on their way to and from San Francisco and then repeatedly sharing that information with federal immigration authorities all the more alarming.

Much of the opposition argues that having to purge data not on a hot list after 30 days will hinder their ability to solve crimes. Many of them note, "What happens if we find a body on day 31?" However, the opposition has not provided any data on the number of older cases that have been solved due to the presence of old license plate data that has been amassed on people who have not been accused of committing any crimes.

Finally, nothing in this bill would prohibit the legitimate use of ALPR data to find suspects when a crime has been committed. The opposition provided several examples, in fact, where law enforcement agencies in California have found that ALPR data furthered their investigations. That use of the data would be able to continue uninterrupted.

8) **Governor's Veto.** This bill is similar to SB 274 (Cervantes) from 2025, which this Committee passed on a 9-4 vote. The Governor vetoed that bill, stating:

> This bill restricts the use and sharing of automated license plate reader (ALPR) data, including by placing a default 60-day limit on how long public entities may retain ALPR data.
>
> 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-

---

[19] *Gait recognition system: deep dive into this future tech,* recfaces.com blog post, https://recfaces.com/articles/what-is-gait-recognition

[20] The full background paper and a link to the video recording of the hearing can be found here: https://apcp.assembly.ca.gov/hearings/2025-26-informationaloversight-hearings.

[21] State Auditor Report, *supra*.

> 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.

As the Governor's veto message pertains to this reintroduced bill, the Governor repeats law enforcements' concerns about older "cold" cases. Arguably, one could justify creating an entire surveillance state around the idea that it could possibly help some sort of crime someday. This Committee, however, has prioritized protecting people's privacy unless there is a clear benefit that justifies the erosion of privacy rights. Without any data to support the Governor's theoretical statement, it is not unreasonable for the Committee to err on the side of protecting Californians' constitutional right to privacy.

While the veto message mentions the 60-day retention timeframe in the previous bill, the timeframe has been shortened to 30 days in this bill, which was the original number of days in SB 274 before it was extended in the Senate Appropriations Committee. 30 days is the retention period recommended by ALPR system providers such as Flock Safety.

As for the Governor's argument that restricting inter-jurisdiction sharing, nothing in this bill restricts the sharing of ALPR information across jurisdictions within California and with DOJ-led multijurisdictional task forces. Presumably, in a real-time pursuit law enforcement would simply communicate with the next jurisdiction to tell them the license plate number and make and model of the car that the suspect they are pursuing is driving. What the bill rightly would prohibit, however, is law enforcement from out of state sending a license plate to a California law enforcement agency and asking them to search their ALPR system for information on where the car has been.

In his veto, the Governor expressed concerns about restricting law enforcement's ability to use ALPR data to help locate missing persons. In order to address that concern, the author has added missing person alerts to the definition of a "hot list."

Finally, the Governor also expressed concerns about the cost in the previous bill. This bill addresses that concern by making implementation of the DOJ audit requirements contingent on an appropriation by the Legislature.

ARGUMENTS IN SUPPORT: the California Initiative for Technology & Democracy (CITED) writes in support:

> Every day, hundreds of thousands, if not millions, of Californians are covertly surveilled by an estimated 10,000 ALPRs across the state. These cameras have been sold to cities and

municipalities as tools to combat crime and track down perpetrators; however, they have created a panopticon that captures the movements of Californians and reveals intimate details of their lives.

This has become a documented problem on multiple fronts. Most prominently, ALPRs have been used to surveil and track undocumented Californians for immigration enforcement. During the final year of the Biden administration, California granted permits to Border Patrol to install ALPRs, meaning as many as 40 cameras are actively sending information to the Trump administration for use in immigration enforcement. El Cajon is currently under legal challenge from the Attorney General for unlawfully sharing ALPR data with out-of-state authorities, demonstrating that California law can be circumvented by law enforcement to aid immigration enforcement. Audits of San Francisco's Flock Safety ALPR network further revealed that outside regional intelligence and out-of-state agencies improperly accessed database queries — and while no evidence of ICE or DHS involvement was found, these findings underscore the systemic vulnerabilities of these systems.

ALPRs have also been weaponized for stalking and harassment. Because ALPR systems log detailed movement data and are accessible to any law enforcement officer with a login, they have proven ripe for personal misuse. More than a dozen law enforcement officers have been arrested, fired, or charged for using these platforms to stalk individuals. These cases typically only come to light after egregious conduct prompts a private citizen to request audit reports, suggesting the problem is significantly underreported and that departmental oversight is badly lacking.

These systems also pose a broader threat to state and national security. Flock Safety, one of America's largest ALPR providers, runs a surveillance network tracking vehicles and people for roughly 12,000 police departments and communities nationwide. According to a responsible disclosure report by an independent cybersecurity researcher, the company accidentally left a digital "master key" exposed in its publicly accessible code in 53 different places. A security researcher discovered that anyone who found this key could have accessed a live map showing patrol car locations, license plate detections, 911 call data, drone feeds, and the personal information of camera owners across the country. The vulnerability was eventually fixed, but not before sitting exposed long enough that a foreign government or bad actor could theoretically have monitored law enforcement movements on a national scale, all without anyone at Flock Safety noticing. If an independent researcher could uncover a flaw of this magnitude, it raises serious questions about how vulnerable these systems truly are, and whether foreign governments or other sophisticated actors may have already found similar weaknesses.

SB 1013 addresses these failures directly. The bill would require all ALPR contracts to be updated to prevent default access to national ALPR databases or other agencies, and would impose new requirements on data sharing between California law enforcement agencies. It would limit ALPR use to locating vehicles or persons reasonably suspected of involvement in a crime, or individuals reported missing. It would also prohibit public agencies from retaining ALPR data for more than 30 days unless it matches an authorized hot list or is part of an active investigation, and would require deletion of all data held beyond that threshold by January 1, 2027.

.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of a large number of law enforcement organizations argues:

> ALPR technology is an essential and widely used investigative tool that allows law enforcement agencies to identify vehicles associated with criminal activity, locate missing persons, and respond rapidly to active threats. The limitations proposed in SB 1013—particularly those restricting data retention, interagency sharing, and permissible uses—would severely diminish the effectiveness of this tool.
>
> **Impact on Criminal Investigations**
>
> ALPR data is often critical in solving violent crimes, including homicides, kidnappings, and organized retail theft. Investigations frequently rely on historical data to establish patterns, identify suspects, and corroborate witness statements. By imposing restrictive retention limits, SB 1013 would eliminate access to valuable evidence that may only become relevant days or weeks after a crime has occurred.
>
> **Officer and Community Safety Concerns**
>
> ALPR systems provide real-time alerts on stolen vehicles, wanted suspects, and vehicles linked to violent offenders. Restrictions on data access and sharing would delay or prevent timely alerts, increasing risks to officers and the communities they serve. When seconds matter—any delay in accessing accurate information can have life-threatening consequences.
>
> **Regional Collaboration and Crime Trends**
>
> Criminal activity does not respect jurisdictional boundaries. Law enforcement agencies rely heavily on regional data-sharing partnerships to track organized crime networks, human trafficking operations, and cross-county offenses. SB 1013 would disrupt these partnerships, creating investigative blind spots and enabling offenders to exploit jurisdictional gaps.
>
> **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.

REGISTERED SUPPORT / OPPOSITION:

Support

California Initiative for Technology & Democracy, a Project of California Common CAUSE
Oakland Privacy

Oppose

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 Los Alamitos
City of Sonora
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
Murrieta Police Officers' Association
Newport Beach Police Association
Newport Beach; City of
Palos Verdes Police Officers Association
Peace Officers Research Association of California (PORAC)
Placer County Deputy Sheriffs' Assocation
Pomona Police Officers' Association
Riverside County Sheriff's Office
Riverside Police Officers Association
Riverside Sheriffs' Association

Oppose Unless Amended

California Mobility and Parking Association
City of Buena Park
City of Gustine
City of Kerman, CA
City of LA Mirada
City of LA Palma
City of Lomita
City of Madera
City of Rancho Palos Verdes
City of Rancho Santa Margarita
City of San Luis Obispo
City of Sierra Madre
City of Stanton
City of Tustin
City of Vacaville
League of California Cities
Oceanside; City of
Security Industry Association

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200