Date of Hearing: July 16, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 274 (Cervantes) – As Amended May 23, 2025

SENATE VOTE: 26-10

PROPOSED AMENDMENTS

SUBJECT: Automated license plate recognition systems

SYNOPSIS

Automated License Plate Reader (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 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.

To curb potential abuses associated with these systems, this bill primarily does four things:

1. Requires that license plate data that does not match information contained on a "hot list" must be deleted within 60 days.

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

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

4. 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 in compliance with the law.

This bill is opposed by a number of law enforcement organizations and, after amendments taken in Senate Appropriations, no longer has any registered support.

The Committee amendments contained in Comment # 7 strengthen privacy protections in the bill by further restricting how the ALPR systems can be used and by whom. Among the amendments are the clarifying of the definition of a "hot list"; requiring a current case number to query the database; and clarifying that ALPR information may only be used for purposes of locating vehicles or persons when either are reasonably suspected of being involved in the commission of a public offense.

This bill was previously heard by the Transportation Committee, where it passed on a 12-4-0 vote.

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 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.

5) Prohibits an agency from retaining ALPR information that does not match a hot list for more than 60 days after the date of collection.

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).)

COMMENTS:

1) **Author's statement**. 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 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. It is imperative that we examine the implications of these practices alongside the ongoing operations of immigration enforcement in our state and nationwide.

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 limit the retention of ALPR information to no more than 60 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 laws that safeguard vulnerable communities. Senate Bill 274 mandates that operators and end users of ALPR systems strengthen safeguards of these systems, including requiring the Department of Justice to conduct random annual audits of public agency operators. The bill also requires that ALPR data must be retained for no longer than 60 days if on a hotlist. Senate Bill 274 strikes a balance between protecting public safety and ensuring individual privacy rights in our increasingly digital world.

2) **Background.** Automated License Plate Reader (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 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. 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 enforcement purposes. The majority of police and sheriff departments in California use an ALPR system. 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

---

[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/.
[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.

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) **Law enforcement misuse of ALPR systems.** A recent 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.[4] 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.
>
> "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

[4] Koebler and Cox, *supra*.

> 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."[5]

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.[6]

The search by the officer logged the reason as "had an abortion, search for female."[7] 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.[8]

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 2014 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 immigrants. In the June 2022 settlement agreement, the Sheriff agreed to start complying with state laws and stop sharing the information. The other example is the Vallejo police department, which captured over 400,000

---

[5] *Ibid.*
[6] 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/.
[7] *Ibid.*
[8] *Ibid.*

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*.[9]

More recently, 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.[10]

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.[11]

4) **Flock Safety and Vigilant Solutions.** Automated license plate readers have become ubiquitous in public spaces. This means even if a consumer takes steps to reduce their personal device use, they are not able to avoid near constant surveillance while interacting in public.

Specifically, the proliferation of both privately owned and publicly owned license plate readers track where people drive and park. Fixed and mobile license plate recognition cameras take photos of license plates, capturing the date, time, and GPS coordinates of where the photo was taken. Each plate image captured, along with the data for that image (date, time, location), is stored in a database as records that can be searched.

The largest vendor for ALPR systems, Flock Safety, has long presented themselves as the good actors in the surveillance space, stating that they do not sell access to data or access it themselves. They have argued in the past that the data in their system belongs to the law enforcement agencies they have contracts with. However, as the *404 Media* investigation found, their system is being used for intrusive surveillance of Americans. In addition, Flock recently announced the launch of their new product *Nova*, which is being promoted as being able to supplement license plate data with a wealth of personal information sourced from other companies and the wider web. The tool will potentially be able to link a vehicle passing by a camera to its owner and then more people connected to them, through marriage or other association. According to internal documents acquired by *404 Media*:

---

[9] 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.
[10] 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/.
[11] *Ibid*.

> "You're going to be able to access data and jump from LPR to person and understand what that context is, link to other people that are related to that person [...] marriage or through gang affiliation, et cetera," a Flock employee said during an internal company meeting, according to an audio recording. "There's very powerful linking." One Slack message said that Nova supports 20 different data sources that agencies can toggle on or off.
>
> [. . .]
>
> In the meeting audio obtained by 404 Media, the Flock employee described the sorts of information the company will supplement ALPR data with. The first is data breaches. One example the employee pointed to was a 2021 data breach impacting users of Park Mobile, an app that allows users to pay for parking without physically going to the parking meter or in some lots where meters no longer exist. That data included license plate numbers with their owners' associated email addresses, phone numbers, and in some cases mailing addresses. With regards to Flock, "Nova ingests that and is able to use that to contextualize the data. So we're now able to make that cognitive leap from LPR to person," the employee said.
>
> Over the last several years more surveillance and technology companies have packaged stolen or hacked data and then sold access to that information to law enforcement. The practice raises questions around the ethics of re-using such data for surveillance purposes; the legality of doing so; and the chain of custody of that information if it was ever used as part of a criminal investigation.
>
> The second was "commercially available data," with the employee explicitly naming credit bureaus Equifax and TransUnion. . . . [W]hen people open a credit card their personal information is sent to the credit bureaus in their role as monitoring peoples' credit. Some bureaus then repackage and sell this information to law enforcement or other data brokers. TransUnion has a data product called TLOxp. . . .
>
> The third is public records such as marriage licenses, property records, and campaign finance records, the employee said. The slides say that Nova will also pull data from law enforcement Records Management Systems (RMS), which are typically databases for storing information on cases, and Computer Aided Dispatch (CAD) systems, which manage responses to 911 calls.[12]

Another company, Vigilant Solutions, has amassed billions of license plate records throughout the county that allow law enforcement officials to monitor the movements of individuals. In their marketing materials, Vigilant claims:

> Vigilant Solutions creates highly innovative and essential tools for law enforcement – tools that ultimately saves lives. As an example, Vigilant Solutions' Automated License Plate Recognition (ALPR / LPR) product is the most comprehensive offering available, with over tens of thousands of users around the world and thousands of success stories.

---

[12] Joseph Cox, "Flock Is Building a Massive People Lookup Tool, Leak Shows," *404 Media* (May 14, 2025) https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/.

> Data is cumbersome; intelligence is actionable. Vigilant Solutions' products are designed to collect, organize and share data to credentialed law enforcement personnel, providing intelligence that is readily accessible and easy to use. This intelligence provides more efficient and effective law enforcement while enhancing officer safety.
>
> *Vigilant Solutions creates intelligence by merging previously disparate data sets such as fixed and mobile license plate recognition, privately collected LPR data, facial recognition, and more.*[13] Vigilant's LEARN Intelligence Network provides an easy to use and intuitive interface to all of this information for unmatched investigative capability in a secure, hosted environment to reduce demands on agency IT resources and to facilitate nationwide interoperability and data sharing.[14]

All of this tracking information, potentially tracking people to sensitive locations, is available to any paying law enforcement agency eliminating the need for them to obtain a court order, warrant, or subpoena. Vigilant boasts, "Even without [license plate reader] cameras, you can benefit by using our Commercial Data. We are the only [license plate reader] provider that can offer over 5 billion nationwide detections and over 150 million more added monthly. We believe the power of LPR is in the data and analytics. In addition to access to our commercial data, agencies can choose to share with other law enforcement agencies to gain access to another 1.5B detections nationwide."[15]

5) **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.

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.[16]

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

---

[13] Emphasis added.
[14] https://www.ra-comm.com/vigilant-solutions/
[15] https://induscom.com/motorola/vigilant/
[16] State Auditor Report, *supra.*

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.[17]

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.[18]

The Auditor's report and the examples in Comment # 4 demonstrate that some law enforcement agencies are either accidentally or deliberately violating the state's privacy laws. This bill seeks to rein in that dangerous behavior.

6) **Analysis of this bill.** The question before this Committee is whether or not this bill furthers its policy priorities, particularly protecting Californians who are being picked up in the street by immigration enforcement, regardless of their citizenship status. In addition, to protect all Californians, and those coming from out of state, are protected from punitive and discriminatory draconian laws attacking the LGBTQ+ community and criminalizing people seeking abortion and gender affirming care.

The author argues, "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." In order to address this concern, the bill does several things:

1. *Purges geolocation data not associated with a car that appears on a hot list after 60 days*. 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." 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.

   The more data collected and retained, the more vulnerable people become to having their daily movements tracked, regardless of whether or not they are suspected of having committed a crime.

---

[17] *Ibid.*
[18] *Ibid.*

Requiring that the data not related to ongoing investigations be purged every 60 days is significantly longer than in previous versions of the bill and longer than the retention time recommended by Flock Safety, which notes that 30 days is considered the best practice for protecting drivers' privacy. In addition, 30 days was generally in line with the CA State Auditor recommendation to limit retention to the shortest practicable time. Last session, AB 1463 (Lowenthal, 2023) would have required law enforcement agencies to delete the data within 30 days. Prior to that, SB 210 (Weiner, 2022), required law enforcement agencies to delete the data within 24 hours. SB 1143 (Wiener, 2020) was a similar bill that met a similar fate. Finally, AB 1782 (Chau, 2019) would have allowed the data to be retained for 60 days, but also required anonymization of the data.

The April 20th version of this bill included a 30 day retention period. However, the Senate Appropriations Committee amended the bill to double the time period to 60 days. By extending the retention period, this bill arguably increases the risk of misuse of the data. Committee amendments described in Comment 7 would enhance the restrictions related to the use of that data to help compensate for the increased risk.

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

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

4. *Requires that the DOJ conduct annual random audits agencies using ALPR to determine whether they have implemented a usage and privacy policy in compliance with the law.* This provision in the bill addresses a concern raised by the State Auditor. As discussed previously, 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, ultimately it was impossible to verify the identity of each of these entities or their purpose for receiving this data. As a result of this finding, the Auditor recommended the Legislature specify how frequently ALPR system use must be audited.

Given the finding in the audit report that law enforcement agencies were not assessing how their ALPR systems were being used and often could not provide the auditors with any information regarding how often or for what reasons they conducted ALPR searches, random DOJ audits appears to be a reasonable first step toward ensuring that the technology is used appropriately.

Privacy advocacy organizations, particularly Oakland Privacy, have pointed out the weakness in auditing whether or not law enforcement agencies maintain the required safety and security procedures. With a support if amended position on an earlier version of the bill, Oakland Privacy cautions:

> In SB 274, the bill language tells the Cal-DOJ to annually audit. . . agencies that use automated license plate readers. The language is described as auditing *whether* they have a compliant policy, which is certainly important, but does not ascertain whether the policy that exists is actually being followed by the agency, which is the gist of the concern.

> In addition, . . the bill language skirts the actual compliance problem - which is not non-compliant policies, but non-compliant operations. We prefer placing the burden of mandated auditing on the agencies themselves to demonstrate that they are, in fact, operating in compliance with their written policies.

Much of the opposition argues that having to purge data not on a hot list after 60 days will hinder their ability to solve crimes. Many of them note, "What happens if we find a body on day 61?" Unfortunately, what they fail to demonstrate is how their access to years and years of ALPR data help them solve serious crimes. As a primary example, Los Angeles County Sheriff, Robert Luna, details a recent crime in San Bernardino County where a woman went missing in 2023 and nine months later her body was found. The woman had been shot. He argues that if this bill is passed the ALPR data would have already been deleted by the time the woman was reported missing. However, Sheriff Luna does not actually state ALPR data had a role in capturing a suspect in the crime. He merely states that the data "might have helped in the case." He specifically states:

> Regardless of the means by which the woman's body was found or how the suspect was identified in this particular case, it should be easily understandable that in this case, or any case that may follow, ALPRS data may prove to be a critical piece of evidence in understanding what has happened.

In 2024, Flock Safety released a report that claimed that their ALPR system was responsible for solving 10% of the crimes in the United States. However, the report has been roundly criticized by researchers, including two who were credited as authors of the report. According to reporting based on email exchanges with one of the researchers:

> The Flock paper's data "was sourced from a survey of Flock Safety ALPR customers," meaning police departments, and the researchers "combine[d] agency-attributed ALPR crime clearances with historical FBI-reported crime data to calculate the portion of crime solved within each of the law enforcement jurisdictions with data of sufficient quality for inclusion."[19]

The piece goes on to note:

> Chris Gilliard, who studies surveillance and privacy at the Just Tech Social Science Research Council, told me "The study isn't published in a journal or vetted for accuracy in a traditional peer review process. Ultimately, it is a marketing document. The emails indicate the desire to prove the technology's effectiveness, which seems counter to how a rigorous study should be conducted."[20]

In 2019, one police department in Georgia attempted to test the impact of Flock's ALPR system. They placed 13 cameras along roads near a popular amusement park. The area was chosen because of the disproportionate amount of property crimes. During the first six months the "number of reported crimes like robbery and nonresidential burglary dropped over 50 percent

---

[19] Jason Koebler. "Let's Talk About the Flock Study That Says It Solves Crime," *404 Media* (Mar. 20, 2024) https://www.404media.co/researcher-who-oversaw-flock-surveillance-study-now-has-concerns-about-it/.
[20] *Ibid*.

apiece compared with the same period the year before."[21] Flock was quick to capitalize on the reduction in crime. The company "proudly touted the results of the Cobb County pilot in a press release it sent [out]. . . and advertises on its website that it solves 'up to five crimes an hour.'"[22]

However, researchers and police were not so convinced. According to an article in *Wired* magazine:

> But experts say it's not that simple, and that establishing a causal relationship between any given variable and fluctuating crime rates is no easy task. "I am not saying that the readers did not have an effect on crime—it is just that we cannot attribute any reduction in crime to the readers themselves," says Alex Piquero, a professor of criminology at the University of Texas, Dallas.
>
> Even police agree. "To make it very clear, we are not 100 percent positive that Flock cameras were the difference," notes VanHoozer. "What we did see, though, is an incredible decrease in crime, starting when we put these cameras down there."
>
> [. . .]
>
> Maria Cuellar, a professor of criminology at the University of Pennsylvania who researches the use of statistics in the law, says pilots like the one in Cobb County only provide before and after comparisons, which alone can't prove a causal relationship. "The problem with these is that so many things could have changed between the 'before' period and the 'after' period," she adds. That includes everything from the number of cars passing through the area to broader demographic changes. The study was also relatively short. "With such a small sample size in terms of time, any changes could likely be noise rather than an actual signal," says Cuellar.
>
> Wider trends too have to be taken into account. Police say crime is down overall in Cobb County, as well as in nearby Atlanta. "We do believe that there are other things we are doing that have attributed to the general decline in crime," says VanHoozer. He notes there are also social factors that might be contributing to the drop, like low unemployment.[23]

The lack of evidence, even from those who oppose the bill, arguably could suggest that after a decade of use, these systems may not be worth the significant erosion in privacy that comes with them. In addition, given the reports of misuse of the data, and the lackadaisical way that some local law enforcement agencies are monitoring the use of ALPR and failing to establish basic security protocols, if this surveillance system is going to continue to be used, it is prudent for the state to adopt policies to stop the data from being improperly shared. This bill presents a very modest step toward that goal.

However, as former supporters of the bill, Electronic Frontier Foundation, noted when removing their support for the bill, "[I]n light of the amendments taken in Senate Appropriations. Where a 30-day retention period is the outer limit of our comfort, the change to 60 days means we can no longer support the bill." As a result of that amendment, this bill currently has no registered

---

[21] Louise Matsakis. "Flock Safety Says Its License Plate Readers Reduce Crime. It's Not That Simple," *Wired* (Oct. 24, 2019) https://www.wired.com/story/flock-safety-license-plate-readers-crime/.
[22] *Ibid.*
[23] *Ibid.*

support, demonstrating that privacy experts are concerned that enshrining a 60-day retention period in state law could in fact do more harm than good.

7) Amendments. In order to further ensure ALPR technology is being used for the intended purpose, the author has agreed to the following amendments:

1798.90.5. The following definitions shall apply for purposes of this title:

(a) "Automated license plate recognition end-user" or "ALPR end-user" means a person that accesses or uses an ALPR system, but does not include any of the following:

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

(2) A person that is subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code and state or federal statutes or regulations implementing those sections, if the person is subject to compliance oversight by a state or federal regulatory agency with respect to those sections.

(3) A person, other than a law enforcement agency, to whom information may be disclosed as a permissible use pursuant to Section 2721 of Title 18 of the United States Code.

(b) "Automated license plate recognition information," or "ALPR information" means information or data collected through the use of an ALPR system.

(c) "Automated license plate recognition operator" or "ALPR operator" means a person that operates an ALPR system, but does not include a transportation agency when subject to Section 31490 of the Streets and Highways Code.

(d) "Automated license plate recognition system" or "ALPR system" means 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.

(e) "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. ***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 person, witness locates, burglaries, grand theft and violent crimes.***

(f) "Person" means any natural person, public agency, partnership, firm, association, corporation, limited liability company, or other legal entity.

(g) "Public agency" means the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including, but not limited to, a law enforcement agency***, but does not include a transportation agency when subject to Section 31490 of the Streets and Highways Code***.

1798.90.52. If an ALPR operator accesses or provides access to ALPR information, the ALPR operator shall do both of the following:

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

(1) The date and time the information is accessed.

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

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

(4) The ~~**purpose for accessing the information**~~ ***case file number that justifies the search query. No queries shall be allowed without a log entry with a valid and current case file number from the agency conducting the query.***

(b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51.

1798.90.54. (a) In addition to any other sanctions, penalties, or remedies provided by law, an individual who has been harmed by a violation of this title, including, but not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR system, may bring a civil action in any court of competent jurisdiction against a person who knowingly caused the harm.

(b) The court may award a combination of any one or more of the following:

(1) Actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500).

(2) Punitive damages upon proof of willful or reckless disregard of the law.

(3) Reasonable attorney's fees and other litigation costs reasonably incurred.

(4) Other preliminary and equitable relief as the court determines to be appropriate.

(c) The Department of Justice shall conduct annual random audits on a public agency that is an ALPR operator or ALPR end-user to determine whether they have implemented ***and are adhering to*** a usage and privacy policy in compliance with subdivision (b) of Section 1798.90.51 or subdivision (b) of Section 1798.90.53, as applicable.

1798.90.55. Notwithstanding any other law or regulation:

(a) A public agency that operates or intends to operate an ALPR system shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program.

(b) 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.

(c) 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.

1798.90.56. A public agency shall not retain ALPR information that does not match information on a***n authorized*** hot list for more than 60 days after the date of collection.

1798.90.57. ***As of January 1, 2026, a public agency shall, within 14 days, delete all ALPR information that has been held for more than 60 days and does not match information on an authorized hot list.***

The amendment to 1798.90.55(c) is in keeping with the ALPR restrictions imposed upon the Highway Patrol and can be found in Vehicle Code Section 2413(c), which states in part: "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."

ARGUMENTS IN OPPOSITION: In opposition to the bill, the California Police Chiefs Association argues:

CPCA understands the need to protect against unscrupulous searches and unwarranted invasion of individual privacy, especially during the current political climate, 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 ALPR's in a manner that is critical to solving and preventing crime in our communities. A significant deterrent to prevent crime is creating a perception that perpetrators will be caught for unlawful acts, and ALPR systems greatly 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. Setting a data retention limit such as 60 days in statute will significantly hinder the use of a valuable law enforcement tool.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Oppose

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 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
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
San Diego County Sheriff's Office

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