SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

AB 1463 (Lowenthal)
Version: July 3, 2023
Hearing Date: July 11, 2023
Fiscal: Yes
Urgency: No
CK

SUBJECT

Automated license plate recognition systems: retention and use of information

DIGEST

This bill requires operators and end-users of automated license plate recognition systems ("ALPR system") to conduct annual audits to review ALPR searches. If the operator or end-user is a public agency, the bill further requires them to destroy all ALPR information that does not match information on a hot list within 30 days. The bill places restrictions on accessing certain systems and sharing ALPR information.

EXECUTIVE SUMMARY

ALPR systems are searchable computerized databases resulting from the operation of one or more cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data. The cameras can be mobile, e.g. mounted on patrol cars, or fixed, e.g. mounted on light poles. ALPR systems allow for the widespread and systematic collection of license plate information. ALPR data can have legitimate uses, including for law enforcement purposes. Currently, at least 230 police and sheriff departments in California use an ALPR system, with at least three dozen more planning to use them. While such systems are useful, there are serious privacy concerns associated with the collection, storage, disclosure, sharing, and use of ALPR data.

Current law requires operators of these systems and those using the data to implement usage and privacy policies. However, concerns have remained about the widespread collection of this data and the wildly inconsistent and opaque ways the data is used, stored, and destroyed. A report from the California State Auditor confirms that police departments in the state are not complying with existing law and recommends further regulation of these systems.

This bill implements some of the report's recommendations by mandating audits of ALPR systems to provide a clear trail for what uses the information is being used for and by who, and requiring most public agencies to destroy ALPR data within 30 days if it does not match the information on a hot list.

This bill is sponsored by Oakland Privacy and supported by the Electronic Frontier Foundation. It is opposed by the City of Thousand Oaks and sheriffs associations.

PROPOSED CHANGES TO THE LAW

Existing law:

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

2) Defines "automated license plate recognition system" or "ALPR system" to mean a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data. "ALPR information" means information or data collected through the use of an ALPR system. "ALPR operator" means a person that operates an ALPR system, except as specified. "ALPR end-user" means a person that accesses or uses an ALPR system, except as specified. The definitions for both ALPR operator and ALPR end-user exclude transportation agencies when subject to Section 31490 of the Streets and Highways Code. (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 shall not be considered the sale, sharing, or transferring of ALPR information. (Civ. Code § 1798.90.55.)

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

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

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

9) Requires CHP to annually report the license plate reader practices and usage, including the number of license plate reader data disclosures, a record of the agencies to which data was disclosed and for what purpose, and any changes in policy that affect privacy concerns to the Legislature. (Veh. 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(a), (b), (c) and 1798.82(a), (b), (c).) Includes within the definition of "personal information," ALPR data when combined with an individual's first name or first initial and last name when either piece of data is not encrypted. (Civ. Code §§ 1798.29(g), 1798.82(h).)

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. & Hy. Code § 31490.)

This bill:

1) Requires ALPR operators and end-users to conduct annual audits to do the following:
    a. review and assess ALPR end-user searches during the previous year to determine if all searches were in compliance with the usage and privacy policy; and
    b. if the ALPR operator or end-user is a public agency assess whether all ALPR information that does not match information on a hot list has been purged no more than 30 days from the date of collection.

2) Provides that if the ALPR operator is a private corporation or limited liability company which provides an ALPR system to a public agency, the auditing requirements shall apply to the public agency and not to the private entity providing the ALPR system.

3) Provides that an ALPR operator or end-user that is a public agency must include a requirement in its usage and privacy policy that all ALPR information is to be purged within 30 days if it does not match information on a hot list.

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

5) Excludes airport authorities from the provisions of the bill applying to public agencies.

6) Prohibits ALPR operators and end-users that are public agencies from accessing ALPR information that is older than 60 days unless the data matches information on a hot list, has been entered into evidence in a criminal matter under California law, or the ALPR system is operated by an airport authority.

7) Prohibits a public agency from selling, sharing, or transferring ALPR information, except to another public agency, and only as otherwise permitted by California state law. Prohibits selling, sharing, or transferring ALPR information to out-of-state or federal agencies without a court order or warrant issued by a California court.

COMMENTS

1. ALPR systems and the privacy implications

The prevalence of ALPR systems and the ease with which license plate data can be gathered and aggregated have raised serious privacy concerns for years. Using large datasets of ALPR data gathered over time, it is possible to reconstruct the locational

history of a vehicle and extrapolate certain details about the vehicle's driver. As a 2013 American Civil Liberties Union (ACLU) report explains:

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

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

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

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

---

[1] ACLU, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* (July 2013) https://www.aclu.org/other/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements?redirect=technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record. All internet citations are current as of June 26, 2023.

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

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

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

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

- the authorized purposes for using the ALPR system, and collecting, accessing, and/or using ALPR information;
- a description of the job title or other designation of the employees and independent contractors who are authorized to access and use the ALPR system and its information, or to collect the ALPR information. It must also identify the necessary training requirements;
- a description of how the ALPR system will be monitored to ensure the security of the ALPR information, and compliance with all applicable privacy laws;
- a process for periodic system audits for end-users;
- the purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons;

[2] SB 34 also included ALPR data within the definition of "personal information" for purposes of California's Data Breach Notification Law.
[3] The law defines an "ALPR operator" as a person that operates an ALPR system and an "ALPR end-user" as a person that accesses or uses an ALPR system, with certain exemptions. (Civ. Code § 1798.90.5.) Both definitions exclude a transportation agency when subject to Section 31490 of the Streets and Highways Code.

- the title of the official custodian, or owner, of the ALPR information responsible for implementing the relevant practices and policies;
- a description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors; and
- the length of time ALPR information will be retained, and the process the ALPR operator or end-user will utilize to determine if and when to destroy retained ALPR information.

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

> When someone drives down a street or parks a car at a curb, there is no expectation of privacy — the driver, the car and the license plate are in public view. Yet most people would recoil if the government announced a program to scan those license plate numbers into a database it could use to determine whose car was parked where and when. It's an obnoxiously intrusive idea that sneaks over the line between a free society and Big Brother dystopia. The notion that the government could trace people's travels whenever it wishes undercuts our fundamental belief that, barring probable cause to suspect involvement in a crime, we should be able to move about freely without being tracked.
>
> But government agencies, from local police departments to Immigration and Customs Enforcement, are able to do just that. Some police agencies — including the Los Angeles Police Department and the Los Angeles County Sheriff's Department — maintain their own databases of scanned plates, which is problematic enough without proper policies and controls in place. Many share with other agencies in broad networks. Some agencies contract with private vendors that build massive databases by merging feeds from automatic license plate readers. So while police must obtain a warrant before placing a tracking device on someone's car, they do not need a judge's permission to contract with a database — or build their own — and, theoretically, track a person's movements over time by consulting records of where his or her car has been spotted.
>
> . . .
>
> We have been concerned about the broad spread of license-plate scanners in recent years primarily because of the potential for ubiquitous monitoring. Clearly, a database that allows police to, in essence, go back in

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

> time and see what cars might have been parked outside a store as it was being robbed could be a useful investigative tool. But at what cost?
>
> Under this privatized system, government officials can enter a license plate and receive an alert as soon as it turns up on any of the nationwide army of scanners — in police cars, on utility poles, in cars driven by private citizens working with the vendors — that feed these databases. Because the data is not purged after a short amount of time, it also means police can plug in a license plate and find out where a car had traveled on any specific day going back years. Such an arrangement might pass constitutional muster, but it certainly violates our right and expectation to not have our daily activities collected and saved for retrieval by government agents.[5]

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

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

The report focused on four law enforcement agencies that have ALPR systems in place.[6] The report found that "the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use." In addition, the audit found that three of the four agencies failed to establish ALPR policies that included all of the elements required by SB 34. All three failed to detail who had access to the systems and how it will monitor the use of the ALPR systems to ensure compliance with privacy laws. Other elements missing were related to restrictions on the sale of the data and the process for data destruction. The fourth entity, the Los Angeles Police Department did not even have an ALPR policy.

The Auditor's report calls into question how these systems are being run, how the data is being protected, and what is being done with the data. The report reveals that agencies commingled standard ALPR data with criminal justice information and other sensitive personal information about individuals, heightening the need for stronger security measures and more circumscribed access and use policies. However, the lack of clear guidelines or auditing made it unclear exactly where information was coming

---

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

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

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

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

Many of these agencies relied on Vigilant Solutions software and protocols rather than establishing their own protocols and safety measures. Vigilant is one of the largest private operators and end-users of ALPR systems and is also a provider of facial recognition technology and provides for ALPR data storage that allows the date, time, and location information to be stored with plate images. Vigilant's parent company has since been acquired by Motorola Solutions. Vigilant operates many of the ALPR systems used by law enforcement, including 70 percent of the law enforcement users surveyed by the Auditor. However, Vigilant indicates that it can also offer access to its private database of "over 5 billion nationwide detections and over 150 million more added monthly."[7] The company's website specifically advertises its ability to run advanced analytics across the vast troves of data it maintains.

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

Perhaps most disturbingly, some of these agencies have a history of sharing their ALPR information with ICE, and the audit reveals that they have continued to authorize "shares with entities with border patrol duties," including the San Diego Sector Border Patrol of U.S. Customs and Border Protection, Customs and Border Protection National Targeting Center, and with an unknown entity simply listed as the "California Border Patrol." The report concludes that "[a]ll of these entities' duties could potentially intersect with immigration enforcement." Reports indicate that such sharing is not

[7] *See* https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/.

limited to the four agencies at the center of the Auditor's report. The Los Angeles Times reported that Pasadena police were found to have been sharing data from their Vigilant ALPR system directly with a Homeland Security division affiliated with ICE, and the Long Beach Police Department was found to have been sending ALPR data directly to ICE through Vigilant's "group approval" feature.[8]

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

The major companies intricately tied to California's ALPR systems, Vigilant and Palantir, both have strong ties to ICE, and reports have indicated that ICE directly accesses the ALPR database run by Vigilant. In fact, a recent investigation found that "Vigilant Solutions provided ICE with step-by-step guides on how to get license plate data from other agencies, including local and state law enforcement agencies and said it could give ICE access to millions more license plate scans."[9]

While the report deeply investigated only four entities, it conducted a statewide survey of law enforcement agencies, revealing that 70 percent operate or plan to operate an ALPR system, and 84 percent of those operating a system shared their images. The report indicates that this "raises concerns that these agencies may share the deficiencies [they] identified at the four agencies [they] reviewed."

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

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

- Require the California Department of Justice (DOJ) to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.
- Require DOJ to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their

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

ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
- Establish a maximum data retention period for ALPR images.
- Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.

This bill implements several of these recommendations and applies them to a broader universe of ALPR operators and end-users.[10] It requires all ALPR operators and end-users to conduct annual audits to review and assess ALPR end-user searches during the previous year to determine if all searches were in compliance with the usage and privacy policy. Given the need for increased transparency, the author has agreed to amend the bill to require the audits be made publicly available.

For operators and end-users that are public agencies other than airport authorities, the bill establishes a strict retention period for ALPR information. It provides that their SB 34-mandated usage and privacy policies must require all such information be destroyed within 30 days if it does not match information on a hot list. The audits conducted by these public agency ALPR operators and end-users must also assess whether the ALPR information that does not match information on a hot list has been routinely destroyed in 30 days or less, as provided. Hot lists contain license plates of vehicles of interest against which the ALPR system is comparing vehicles on the roadways. The bill further provides that these public agency ALPR operators and end-users are prohibited from accessing an ALPR system that retains ALPR information that does not match a hot list for more than 60 days, except where the system is operated by an airport authority.

Currently, public agencies are prohibited from selling, sharing, or transferring ALPR information, except to another public agency, and only as otherwise permitted by law. This bill narrows that to only where permitted by *California* law. It goes further to prohibit any selling, sharing, or transferring to out-of-state or federal agencies without a court order or warrant issued by a California Court. As already discussed, there are very real concerns with this information getting into the hands of immigration enforcement officials. With the climate across the country in the wake of the *Dobbs* decision, there is also increased concern about law enforcement in other states using this data to further restrict or punish reproductive health care.[11]

---

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

[11] Press Release, *Civil Liberties Groups Demand California Police Stop Sharing Drivers' Location Data With Police In Anti-Abortion States* (May 25, 2023) ACLU Northern California, https://www.aclunc.org/news/civil-liberties-groups-demand-california-police-stop-sharing-drivers-location-data-police-anti ("California law enforcement's sharing of ALPR data with law enforcement in states that criminalize abortion also undermines California's extensive efforts to protect reproductive

These additional requirements work toward addressing the privacy and security concerns highlighted above. Specifically, these new guardrails will further protect against ALPR data falling into the wrong hands and being used for purposes contrary to California values, such as assisting in federal immigration enforcement or in the ongoing assault against reproductive rights.

5. Stakeholder positions

According to the author:

> ALPRs are just one of the many surveillance tools police departments and anti-abortion, groups have available to them, but and are becoming one of the most powerful tools available. As states start passing laws that put bounties on a woman's head for seeking abortions in abortion safe states and are trying to make it illegal [to] even make that trek, not to mention the number of states that are targeting Drag queens and the trans community, California must take all precautions to preserve the identities and whereabouts of seeking refuge in our state. AB 1463 is one measure that will prevent law enforcement in cooperating with states that seek to criminalizing people seeking medically safe abortions in California.

Writing in support, Oakland Privacy, the sponsor of the bill, explains the need for the bill:

> Queries into these large databases, mostly held in private hands like the LEARN system belonging to Vigilant Solutions, a division of Motorola Inc., the FALCON system belonging to Flock Safety, and some held in the state's homeland security fusion centers, do not require probable cause or reasonable suspicion to access sensitive geolocation data for any Californian and unless specifically restricted, red state law enforcement could locate vehicles in California from travelers they believe drove to California for reproductive or gender-affirming care and prepare to arrest them on their return.
>
> These large data repositories, like any huge trove of data, become subject to mistakes and errors the bigger and more aged they get. It is important to note that a license plate reader hit, whether erroneous or not, is justification under most California law enforcement agency policies for a felony traffic stop with guns drawn. License plate reader mistakes have led to erroneous and violent traffic stops that not only terrorize innocent drivers, but lead to expensive civil litigation that drains municipal coffers.

---

health privacy, specifically a 2022 law (AB 1242) prohibiting state and local agencies from providing abortion-related information to out-of-state agencies.").

> This is particularly a problem with rental cars that are reported stolen when returned late and then re-rented without clearing the previous stolen car alert. 8
>
> The California State Auditor observed that many agencies are not fully aware of all their sharing partners. Moreover, California's State Auditor also stated:
>
> *Three agencies (75% of the sample group) share their images with hundreds of entities across the U.S. but could not provide evidence that they had determined whether those entities have a right or a need to access the images.*
>
> As an example of the data-sharing practices in place, this printout of the Sacramento Sheriff's Department Vigilant LEARN sharing profile, secured by a public records request, shows the department routinely share d their ALPR data with more than 800 other agencies, the majority of them out of the state.
>
> Having reviewed dozens of similar public records responses from all over California, we can attest that the Sacramento Sheriff's Department practices are not an outlier, but a reflection of what have been standard practices. Just on the first of the thirteen pages of agencies with access, we can identify at least twenty that have no reason to be investigating the travel patterns of Sacramentans, including the police departments in Alapaha, GA (population 668), Bensalem Township, PA, Beaumont, TX, and the airport in Atlantic City, NJ.

The City of Thousand Oaks writes in opposition:

> ALPR is a valuable public safety tool used by the Thousand Oaks Police Department (TOPD). To clarify, ALPR simply takes images of license plates and does not take video images of motorists. ALPR serves as not only an investigatory tool but a crime deterrent. ALPRs are affixed to patrol cars, intersections and even on message board trailers. The system alerts officers immediately if a motorist associated with a missing person, stolen vehicle, or other crimes. TOPD has strict policy on the use of this tool, which is limited to searches related to criminal activity. By setting an arbitrary timeframe for the retention of ALPR data to 30 days, surveillance data needed to solve a crime or apprehend criminals could be potentially deleted. Investigations may require data older than 30 days. Creating a short retention schedule eliminates access to data that could help resolve a crime.

The California State Sheriffs' Association argues in opposition:

> 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. To set a data destruction timeline such as 30 days in statute will significantly hinder the use of a valuable law enforcement tool.

SUPPORT

Oakland Privacy (sponsor)
Electronic Frontier Foundation

OPPOSITION

California State Sheriffs' Association
City of Thousand Oaks
Los Angeles County Sheriff's Department

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

SB 210 (Wiener, 2021) would have provided greater transparency and accountability with respect to ALPR systems by requiring, similar hereto, ALPR operators and end-users to conduct annual audits to review ALPR searches. It would have further required an operator or end-user that is a public agency to destroy all ALPR data that does not match information on a hot list within 24 hours. It died in the Senate Appropriations Committee.

SB 1143 (Wiener, 2020) was largely identical to the current bill. It was held under submission in the Senate Transportation Committee.

AB 1782 (Chau, 2019) would have required those operating ALPR systems and those accessing or using ALPR data to have policies that include procedures to ensure nonanonymized ALPR information is timely destroyed, except as specified, and that all ALPR information that is shared is anonymized. The bill was subsequently gutted and amended to address a different topic. It died in the Senate Appropriations Committee.

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

PRIOR VOTES:

Assembly Floor (Ayes 48, Noes 15)
Assembly Appropriations Committee (Ayes 11, Noes 4)
Assembly Privacy and Consumer Protection Committee (Ayes 8, Noes 2)
Assembly Transportation Committee (Ayes 10, Noes 4)
****