SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

SB 210 (Wiener)
Version: March 15, 2021
Hearing Date: March 23, 2021
Fiscal: Yes
Urgency: No
CK

SUBJECT

Automated license plate recognition systems: use of data

DIGEST

This bill provides greater transparency and accountability with respect to automated license plate recognition systems ("ALPR system"). It requires ALPR operators and end-users 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 data that does not match information on a hot list within 24 hours.

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 recent 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 24 hours if it does not match the information on a hot list.

This bill is sponsored by Media Alliance and Electronic Frontier Foundation. It is supported by several privacy and civil rights/liberties advocacy groups, and opposed by various law enforcement 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 carry out two specific security procedures and practices, as part of the existing requirement to maintain such procedures and practices:
    a. conduct annual audits to review ALPR end-user searches during the previous year to assess user searches, determine if all searches were in compliance with the relevant usage and privacy policy, and, if the ALPR operator is a public agency, confirm that all ALPR data that does not match hot list information has been routinely destroyed in 24 hours or less; and
    b. where the operator is a public agency, destroy all ALPR data that does not match information on a hot list in 24 hours or less and include such a requirement in their own usage and privacy policy.

2) Requires these audits to be made available to the public in writing and posted on the operator's website, as specified.

3) Requires an ALPR operator or an ALPR end-user that accesses or provides access to ALPR information to conduct an annual audit to review ALPR end-user searches during the previous year to assess user searches, determine whether all searches were in compliance with the usage and privacy policy, and, if the ALPR operator or end-user is a public agency, confirm that all ALPR data that does not match hot list information has been routinely destroyed in 24 hours or less. It also requires ALPR end-users that access or provide access to ALPR information to maintain a record of that access and to require that ALPR information only be used for the purposes authorized in their usage and privacy policy.

4) 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 data is to be destroyed within 24 hours if it does not match hot list information.

5) 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.

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

7) Requires the California Department of Justice (DOJ), on or before July 1, 2022, to draft and make available on its internet website a policy template that public agencies may use as a model for their ALPR policies. It further requires them to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR database

systems. The guidance shall include, but not be limited to, the necessary security requirements agencies should follow to protect the data in their ALPR systems.

8) Prohibits ALPR operators and end-users that are public agencies from accessing an ALPR system that retains ALPR information for more than 24 hours that does not match a hot list.

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

[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 [as of Mar. 2, 2021].) All further internet citations are current as of March 2, 2021.

> 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].)

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:

---

[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 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;
- 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

[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/.

> 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 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.[6]

The report 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

---

[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 [as of Mar. 4, 2021].

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 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 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.

---

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

Perhaps most disturbingly, some of these agencies have a history of sharing their ALPR data 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 limited to the four agencies at the center of the Auditor's report. The Los Angeles Times recently 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:

---

[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*.

- Require Justice 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 Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. 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 ALPR end-user searches during the previous year to assess user searches and determine if all searches were in compliance with the usage and privacy policy. These audits must be made publicly available.

For operators and end-users that are public agencies, the bill establishes a strict retention period for ALPR data. It provides that their SB 34-mandated usage and privacy policies must require all such data be destroyed within 24 hours if the data does not match hot list information. The audits conducted by these public agency ALPR operators and end-users must also confirm that this information has been routinely destroyed in 24 hours 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 public agency ALPR operators and end-users are prohibited from accessing an ALPR system that retains ALPR information for more than 24 hours that does not match a hot list.

Currently, an ALPR operator that accesses or provides access to ALPR information must maintain a record of that access and it must require that ALPR information only be used for purposes authorized in its usage and privacy policy. The bill applies these provisions to ALPR end-users. It further requires ALPR operators and ALPR end-users that access or provide access to such information to conduct annual audits "to review ALPR end-user searches during the previous year to assess user searches, determine whether all searches were in compliance with the usage and privacy policy" and, where the ALPR operator or end-user is a public agency, to "confirm that all ALPR data that does not match hot list information has been routinely destroyed in 24 hours or less." This provision may be redundant but further emphasizes the duty to routinely audit any access to ALPR systems.

---

[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.

The bill also carries out a recommendation with particular emphasis in the Auditor's report. It requires DOJ to create and post on its internet website a model ALPR policy template that public agencies can use. DOJ is also required to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR database systems. This must include critical security requirements agencies should follow to adequately protect the data in their ALPR systems.

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.

5. Stakeholder positions

According to the author:

> Each year billions of license plate scans are taken throughout California, and in the case of 99.7% of these scans, the information attained has no connection with any criminal activity. Despite this, enormous quantities of this sensitive data, which shows detailed patterns of Californian's movement, is stored for years at a time violating the privacy of millions. This ALPR data has then been recklessly distributed to other law enforcement agencies around the country, including Immigration and Customs Enforcement, along with thousands of other organizations. Many of these organizations have not been vetted nor has a clear reasoning for allowing access to these organizations been presented. Further, much of this information is accessible by law enforcement officers through end-use searches of ALPR databases, and by private third-party ALPR vendors.
>
> This bill aligns with many of the recommendations in the State Auditor's report and will prevent sensitive ALPR data from being misused by law enforcement by requiring that ALPR operators delete any information unrelated to vehicles of interest on a 'hot list' within 24 hours of collecting said information. The bill also requires annual audits to ensure that any end-use searches of this data were not done maliciously, and will seek to restrict the ability of ALPR operators to share their data with immigration enforcement agencies.

The Electronic Frontier Foundation, a co-sponsor of the bill, write: "The results of the audit speak for themselves. The people of California need stronger guardrails on law enforcement use of ALPR data, and new rules to protect them from unnecessarily invasive data collection and use—and from having that information shared broadly for

no apparent reason." The California Immigrant Policy Center also supports the bill and highlights that "ALPR technology disproportionately impacts low-income communities of color, including immigrant communities."

Writing in opposition are a number of law enforcement associations who are further regulated by the bill. The Los Angeles County Sheriff's Department highlights successful uses of ALPR data and asserts it is "STRONGLY OPPOSED to the limitation on the amount of time local law enforcement can keep this information."

The California Narcotic Officers Association also writes in opposition:

> The restriction on ALPR data is based on a false assumption that privacy rights are harmed by the use of ALPR. In fact, there is no expectation of privacy in a publicly created and displayed license plate. On the contrary, the gravamen of a license plate is precisely to publicly display the plate to facilitate the identification of the vehicle and that vehicle's registered owner.

The California Association of Highway Patrolmen write:

> ALPR systems are valuable tools for law enforcement agencies to investigate vehicles of interest quickly and efficiently. ALPR systems help secure public events and venues, recover stolen vehicles, and aid officers when confronting and apprehending a dangerous criminal. The data collected in these systems can determine whether a vehicle has been at the scene of a crime, identify crime patterns, and help solve future, or even past, crimes. By limiting the use of ALPR systems, the safety of our communities is at risk.

It writes in an oppose-unless-amended position: "Rather than limit the storage of data to 24-hours, the CAHP respectfully requests that you consider amending it to 60-days instead, which is current protocol for the CHP now and has proven to be effective."

Common Sense writes in support of the bill:

> SB 210 seeks to address the violations of privacy and rampant misuse seen with ALPR systems by requiring certain public agencies delete their ALPR data that does not match a hot list within 24 hours. Further, ALPR operators and end-users must both conduct annual audits to ensure compliance with regulations on their data. These requirements will ensure that ALPR information can still be utilized for criminal activity when necessary, but that irrelevant yet detailed data is not being collected and stored for years at a time.

SUPPORT

Electronic Frontier Foundation (co-sponsor)
Media Alliance (co-sponsor)
Access Humboldt
Asian Americans Advancing Justice, California
California Immigrant Policy Center
Common Sense
Consumer Federation of America
National Lawyers Guild, San Francisco Chapter
Oakland Privacy
Privacy Rights Clearinghouse

OPPOSITION

California Association of Highway Patrolmen
California Narcotic Officers' Association
California Peace Officers' Association
California Police Chiefs Association
California State Sheriffs' Association
City of Fremont
Los Angeles County Sheriff's Department
Peace Officers Research Association of California

RELATED LEGISLATION

Pending Legislation: AB 1076 (Kiley, 2021) requires DOJ to draft and make available on its internet website an ALPR system policy template for local law enforcement agencies and to develop and issue guidance for local law enforcement agencies to help them identify and evaluate the types of data they are storing in their ALPR systems. This guidance must include the necessary security requirements agencies should follow to protect the data in their ALPR system. This bill is currently in the Assembly Transportation Committee.

Prior Legislation:

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.

****