Date of Hearing:

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 1463 (Lowenthal) – As Amended March 22, 2023

As Proposed to Amended

SUBJECT: Automated license plate recognition systems: retention and use of information

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 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.

Unfortunately, a 2019 audit by the State Auditor 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, 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 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 that extended retention posed.

This bill does three things:

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

2. *Prohibits law enforcement agencies from sharing the data with any federal or out of state entities unless they have a valid California court order or warrant.*

3. *Requires departments using ALPR systems to conduct annual compliance audits.*

The question before this Committee is whether or not this bill furthers its policy priorities, particularly ensuring that 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. Another priority of the Committee is ensuring that our laws protect our immigrant neighbors from federal policies that make them vulnerable to being separated from their families, imprisoned, and ultimately returned to countries that many were forced to flee for their own safety.

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 like the ones contained in this bill to stop the data from being improperly shared.

This bill is sponsored by Oakland Privacy and supported by Initiate Justice and the Electronic Frontier Foundation. The California State Sheriffs' Association and the California Association of Highway Patrolmen are opposed.

This bill previously passed the Transportation Agency on a 10-4-1 vote.

SUMMARY: Requires a local public agency end-user of an automated license plate reader (ALPR) to purge information that does not match information on a hot list, as defined, within 30 days and explicitly prohibits the selling, sharing or transferring of ALPR data with an out-of-state or federal agency without a valid California court order or warrant. Specifically, **this bill**:

1) 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.

2) Requires that a local public agency, other than an airport authority, purge any ALPR data that is not on a hotlist after 30 days.

3) Requires an ALPR operator to have reasonable security procedures and practices that include, but are not limited to, an annual audit to review and assess ALPR end-user searches during the previous year to determine if all searches were in compliance with the applicable usage and privacy policy. If the ALPR operator is a public agency other than an airport authority, the audit shall 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.

4) Explicitly prohibits ALPR information from being shared or transferred to out-of-state or federal agencies without a valid court order or warrant from a California court.

5) Prohibits an ALPR operator or ALPR end-user that is a local public agency, excluding an airport authority, from accessing an ALPR system that retains ALPR information that does not match information on a hot list for more than 30 days after the date of collection unless they are accessing an ALPR system operated by an airport authority.

6) States legislative findings and declarations.

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) Prohibits use of California state funds for travel to any state that is subject to a ban on state-funded and state-sponsored travel because that state enacted a law that voids or repeals, or has the effect of voiding or repealing, existing state or local protections against discrimination on the basis of sexual orientation, gender identity, or gender expression, or has enacted a law that authorizes or requires discrimination against same-sex couples or their families on the basis of sexual orientation, gender identity, or gender expression. (Gov. Code § 11139.8.)

15) 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.)

16) 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).)

17) 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).)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS:

1) **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 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. As of 2019, 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. (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), *available at* https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [State Auditor Report].)

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. (See Civ. Code §§ 1798.90.51, 1798.90.53.) The resulting statutes provide that both ALPR operators and ALPR end-users ae required to maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. These operators and end-users are further required to implement usage and privacy policies in order to ensure that the collection, access, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties.

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

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

2. A description of the job title or other designation of the employees and independent contractors who are authorized to access and use the ALPR system and its information, or to collect the ALPR information. Necessary training requirements must also be identified.

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

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

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

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

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

8. The length of time ALPR information will be retained, and the process the ALPR operator or end-user will utilize to determine if and when to destroy retained ALPR information.

Unfortunately, security and privacy concerns have only multiplied in the wake of SB 34 and it appears that law enforcement agencies may not have followed the requirements of the law. 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. In addition, since the passage of the bill in 2015, alarm over the overturning of *Roe v. Wade* and continued aggressive and punitive federal immigration policies have become a central concern for the Legislature and this Committee. This statute has not been updated to insure that proper protections are in place for people traveling from out of state seeking sanctuary in California for abortion and gender affirming care, protection from federal immigration authorities, or fleeing the large number of states that have introduced or passed anti-LBGTQ+ laws. This bill is an effort to put some of those protections in place.

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 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. (State Auditor Report, *supra*.)

The Auditor's report calls into question how these systems are being run, how their data is being protected, and what is being done with the data. The report reveals that agencies commingled standard ALPR data with criminal justice information and other sensitive personal information about individuals, illustrating the need for stronger security measures and more circumscribed access and use policies. However, the lack of clear guidelines or auditing made it unclear exactly where information was coming from, who was accessing it, and what purposes the information was being put to. The report does make clear that these agencies have "shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images." Increasing the vulnerability of such vast troves of sensitive data, the agencies' retention policies were uninformed and not tied to the usefulness of the data or the risks extended retention posed. (*Ibid.*)

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. (*Ibid*.)

Along with the Auditor's report, at least two other breaches have been reported in the news in the last year. First, 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 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*. (Bhuiyan, *How expanding web of license plate readers could be 'weaponized' against abortion*, The Guardian (Oct. 6, 2022) *available at* https://www.theguardian.com/world/2022/oct/06/how-expanding-web-of-license-plate-readers-could-be-weaponized-against-abortion?ref=vallejosun.com.)

The Auditor's report and the two examples above demonstrate that some law enforcement agencies are either accidentally or deliberately violating the state's privacy laws. This bill appears to be a reasonable first step in trying to rein in that dangerous behavior.

2) **Author's statement.** According to the author:

> ALPRs are just one of the many surveillance tools police departments and anti-abortion, groups have available to them, but are rapidly 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, along with a number of states that are targeting Drag queens and the trans community, California must take all precautions to preserve the identities and whereabouts of people 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.

3) **Committee amendments.** The amendments being taken in the Committee seek to align the bill with several data sanctuary laws passed last year to protect data that might be associated with seeking or obtaining reproductive medical care, including abortion services. The amendments are as follows:

> Section 1798.90.55 of the Civil Code is amended to read:
>
> 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.*** ALPR information shall not be sold, shared, or transferred to out-of-state or federal agencies without a ~~**valid subpoena,**~~ court order or warrant ***issued by a California court.*** 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.

4) **Analysis of this bill.** The question before this Committee is whether or not this bill furthers its policy priorities, particularly ensuring that 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. Another priority of the Committee is ensuring that our laws protect our immigrant neighbors from federal policies that make them vulnerable to being separated from their families, imprisoned, and ultimately returned to countries that many were often forced to flee from for their own safety.

As discussed previously, this bill is intended to address some of the concerns raised by the State Auditor and align this bill with previously-enacted bills designed to protect reproductive health data, including abortion care and gender affirming care. Toward that end, the bill essentially does three things:

1. *Purges geolocation data not associated with the investigation of any crime after 30 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.

As noted in *The Guardian* article mentioned previously:

> License plate readers, which are usually installed on streetlights, highway overpasses or police squad cars, capture the details of passing cars and help police keep track of the vehicles that pass through certain locations or neighborhoods. The information is collected in a database, which police can search to see where certain vehicles have been or what cars have been in a certain area during a specific time frame.

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.

Requiring that the data not related to ongoing investigations be purged every 30 days seems to be a sensible time-frame and is significantly longer than in previous versions of the bill. In the last session, SB 210 (Weiner, 2022), the most recent attempt to set limits on the use of ALPR data, required law enforcement agencies to delete the data within 24 hours. Prior to that, SB 1143 (Wiener, 2020), would have also limited data retention to 24 hours. AB 1782

(Chau, 2019) would have allowed the data to be retained for 60 days, but also required anonymization of the data.

According to the author, this bill recommends 30 days, which is what is recommended by the state's leading ALPR supplier, Flock Safety, which notes that 30 days is considered the best practice for protecting drivers' privacy. In addition, 30 days is in line with the CA State Auditor recommendation to limit retention to the shortest possible time.

2. *Forbids the sharing of geolocation data with out of state and federal agencies without a valid California court order or warrant.* This bill, as proposed to be amended, seeks to align the data sharing prohibitions with the suite of reproductive privacy bills that are either currently moving through the Legislature or were passed in the last session. Specifically, this bill prohibits the sharing of ALPR data with any other public agency if it is contrary to state law. In addition, law enforcement agencies from another state or a federal agency will be required to obtain a court order or warrant from a California court in order to obtain access to the data. This language is similar to other data sharing restrictions that have been put in place to protect the data of vulnerable populations. This provision significantly strengthens current law and the version of the bill currently in print.

3. *Requires public agencies operating ALPR systems to perform an annual compliance audit*. This provision in the bill, like the data retention provision, is based on a recommendation from 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.

Under this bill, local law enforcement agencies would be required to perform a compliance audit once a year. Specifically, they must include in their annual audit a review and assessment of all end-user searches during the previous year to determine if all searches were in compliance with their usage and privacy policies. In addition, the audit must also include an assessment of whether or not all ALPR information that does not match information on a hot list had been purged no more than 30 days from the date of collection.

Given the finding in the audit report that law enforcement agencies often 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, an annual compliance audit appears to be a reasonable first step toward ensuring that the technology is used appropriately.

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 like the ones contained in this bill to stop the data from being improperly shared.

On a final important note, the California Association of Highway Patrolmen have opposed this bill. However, the laws being amended by this bill apply only to local public entities, including

law enforcement agencies, and will not impact the CHP's use of this technology. In addition, the provisions of this bill specifically exclude airport authorities, which may have national security reasons for retaining the data for longer periods of time.

5) **Related legislation.** SB 34 (Hill. Chap. 532, Stats. 2015) established regulations on the privacy and usage of automatic license plate recognition data and expanded the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system.

AB 2192 (Ramos, 2022) would have authorized a public agency that uses an ALPR to share the data that it collects with a law enforcement agency of the federal government or another state if the ALPR information was being sold, shared, or transferred to locate a vehicle or person reasonably suspected of being involved in the commission of a public offense, except as specified. That bill was taken up in Assembly Privacy and Consumer Protection for testimony only.

SB 210 (Wiener, 2022) would have required ALPR operators and end-users to conduct annual audits to review ALPR searches and required most public ALPR operators and end-users to destroy all ALPR data *within 24 hours* if it did not match information on a "hot list." It also would have required the DOJ to make available model ALPR policies and issue guidance to local law enforcement agencies, as specified. That bill was held on suspense by the Senate Appropriations Committee.

AB 1076 (Kiley, 2021) would have required the Department of Justice to draft and make available on its internet website an ALPR system policy template for local law enforcement agencies and require that the guidance given include the necessary security requirements agencies should follow to protect the data in their ALPR systems. That bill was held on suspense by the Assembly Appropriations Committee.

SB 1143 (Wiener, 2020) was largely identical to SB 210. It was held by 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 included procedures to ensure non-anonymized ALPR information is destroyed within 60 days, except as specified, and that all ALPR information that is shared be anonymized. The bill was subsequently gutted and amended to address a different topic. It died in the Senate Appropriations Committee.

ARGUMENTS IN SUPPORT. The sponsor of this bill, Oakland Privacy, notes:

> Retention policies vary across the state, but on average are about a year. Some California agencies retain for longer periods of time than a year and a few retain indefinitely. These long periods of time that capture multiple scans of individual vehicles and record regularly repeated travel patterns can reveal residences, places of employment and ongoing associations with the assistance of other databases that law enforcement agencies can easily access.
>
> In fact, in 2015, Senator Hill [the author of SB 34] was dismayed to discover that a private investigator provided with his spouse's automobile license plate number was able to track his

spouse to a local gym by using license plate reader scan data to analyze the travel patterns of the vehicle.

Also in support of the bill, Initiate Justice, states:

> In just the last few years, public records requests from public interest groups showed that at least two California police departments, Pasadena and Long Beach, were sharing their license plate reader scans with Immigrations and Customs Enforcement (ICE) in the Vigilant LEARN database. After the sharing became public, both agencies stated it had been a "mistake" and would cease, but such mistakes can cause deportations that cannot be undone. The mistakes point to the lack of control over the geolocation data created by automated license plate readers by agencies. If it is so easy to share this data with federal immigration without an agency even knowing that it is doing it, then there are not sufficient safeguards and those lack of safeguards are putting Californians and visitors at risk.
>
> Since at least 99.8% of all automated license plate reader scans taken in the state are never of interest in any criminal or civil matter, but are simply records of vehicle locations being kept in cold storage just in case, AB 1463 restricts retention beyond a month to vehicle scans that are of no interest in a criminal or civil matter and prevents the location data of drivers from being shared willy-nilly across the country without a proper legal process.
>
> One of the safest states in the nation, New Hampshire, reduced its retention period for license plate reader scans that were not of interest in a criminal matter to three minutes in 2007. 16 years after enacting this policy, New Hampshire remains one of the safest states in the nation.

ARGUMENTS IN OPPOSITION. In opposition to this bill, the California State Sheriffs' Association argues:

> 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.

REGISTERED SUPPORT / OPPOSITION:

Support

Oakland Privacy (sponsor)
Electronic Frontier Foundation
Initiate Justice

Opposition

California Association of Highway Patrolmen
California State Sheriffs' Association

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