Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2192 (Ramos) – As Amended March 29, 2022

For presentation only

SUBJECT: Automated license plate recognition systems: information sharing

SUMMARY: This bill would authorize a public agency that uses an automated license plate reader (ALPR) to share the data that they collect with a law enforcement agency of the federal government or another state, as specified. Specifically, **this bill would**:

1) Authorize a public agency that uses an ALPR to share the data that they collect with a law enforcement agency of the federal government or another state if the ALPR information is 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.

2) Prohibit the sale of ALPR data to the federal government or to other states under any of the following circumstances:

- The sale, sharing or transferring of ALPR information would violate a provision of the California Values Act.

- ALPR information would be sold, shared, or transferred to a state that is subject to a ban on state-funded and state-sponsored travel because the 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; and,

- ALPR information would be shared, or transferred to a state that has enacted laws that deny or interfere with a woman'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 woman.

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, sec. 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 Sec. 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 Sec. 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 Sec. 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 Sec. 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 Sec. 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 Sec. 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 Sec. 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 Secs. 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 Secs. 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 Sec. 31490.)

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

13) Prohibits state funds for travel to a state that is subject to a ban on state-funded and state-sponsored travel because the 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 Sec. 11139.8.)

14) Prohibits the state of California from enacting a law that denies or interfere with a woman'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 woman. (Health & Saf. Code Sec. 123466.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to ensure that law enforcement may share ALPR information with out of state law enforcement agencies if the information is being shared to locate a vehicle or person suspected of a crime. This bill is sponsored by the California State Sheriffs Association.

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

> Existing law is ambiguous at best when it comes to sharing of law enforcement automated license plate reader (ALPR) data. Specifically, one interpretation of the restriction on sharing these data limits with what out-of-state or federal agencies California agencies could share ALPR data.
>
> AB 2192 allows California state and local law enforcement agencies to share ALPR data with out-of-state and federal law enforcement agencies to locate a vehicle or person reasonably suspected of being involved in the commission of a public offense. This change would remove ambiguity and clarify existing statute.

3) **Automated license plate readers**: An ALPR system is one or more mobile or fixed cameras combined with computer algorithms that can read and convert images of automobile registration plates, and the characters they contain, into computer-readable data showing the license plate itself, as well as the time, date, and place of the picture. ALPR systems can also provide a "contextual" photo of the car itself, making information about car make and model,

distinguishing features, state of registration, and individuals in the car available as well. ALPR systems operate by automatically scanning any license plate within range. Some ALPR systems can scan up to 2,000 license plates per minute. In the private sector, ALPR systems are used to monitor parking facilities and assist repossession companies in identifying vehicles. Some gated communities use ALPRs to monitor and regulate access.

When used by law enforcement, each scanned license plate is checked against a variety of databases, such as the federal AMBER Alert for missing children, or the National Crime Information Center, which aggregates 21 different databases tracking categories such as stolen property, sex offenders, gang affiliates, and known violent persons. If one of the license plates photographed by the system gets a hit based on a match with one of the databases or some other "hot list," the ALPR system can alert law enforcement in real time so they can take action.

Prior to 2015, ALPR data was not considered personal information (PI). SB 34 (Hill, Ch. 532, Stats. 2015) created obligations for ALPR data for operators and end-users, and included ALPR data in the definition of PI for the purposes of California's data breach notification law. SB 34 also provided that ALPR information may only be shared among "public agencies" defined as the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and *county, including, but not* limited to, a law enforcement agency. This bill would additionally authorize a law enforcement agency of the federal government or a state other than California, to receive ALPR information, if the ALPR information is being sold, shared, or transferred to locate a vehicle or person reasonably suspected of being involved in the commission of a public offense.

In support, a large coalition of law enforcement organizations from southern California write, "Ensuring law enforcement's ability to communicate and share resources toward the end of protecting the public is a paramount concern. AB 2192 clarifies the authority of local law enforcement agencies to share ALPR data when the sharing is tied to a person or vehicle that is suspected of being involved in a crime and mirrors the California Highway Patrol's authority to share ALPR data as it exists today."

A large coalition of organizations advocating for a wide range of civil liberties, privacy, and related rights including the ACLU California Action, Planned Parenthood Affiliates of California, and the National Center for Lesbian Rights argue in opposition:

> AB 2192 will facilitate the widespread sharing of driver information with other governments, including those that do not share California's values. Governments have long used surveillance – ranging from wiretaps to ALPR—to target disfavored and marginalized people. In New York City, the police have targeted Muslim Americans using information collected by ALPR systems near mosques. In Texas, police have used ALPR-obtained information to shake down Black and Brown motorists for outstanding traffic fines. In the United Kingdom, police pulled over an activist because his license plate was placed on a watch list after an anti-war protest. As marginalized populations across the country face increasing legislative attacks because of their identities or invocation of their rights, many of them may relocate to friendlier states, including California, for access to services or to live—and we must respond by preventing their

> information from getting into the wrong hands. Instead, AB 2192 would permit the widespread sharing of information with agencies who could use it to target Californians.
>
> These concerns are not hypothetical. Rather, as other states seek to criminalize abortions or gender-affirming care, AB 2192 may put those individuals at risk for coming to California for those medical needs. The Idaho House of Representatives, for example, recently passed a bill that would make it a felony to help transgender kids seek gender-affirming care out of state, in addition to making it a felony to provide gender affirming care to minors in Idaho. A bill in Missouri would criminalize assisting someone to leave the state to receive an abortion. The only California protection against sharing ALPR information for the enforcement of such anti-abortion and anti-trans laws would be erased by AB 2192. Even if AB 2192 were amended to allow sharing of ALPR information across state lines only for certain crimes, this sharing would still likely undermine California's status as a sanctuary state for abortion services and gender affirming care.

Staff additionally notes that there is ongoing litigation on whether existing law already permits law enforcement agencies to share ALPR data outside of the state. On October 14, 2021, the ACLU and the Electronic Frontier Foundation (EFF) filed a lawsuit against the Marin County Sheriff for sharing ALPR data with Immigration and Customs Enforcement (ICE), Customs and Boarder Protection, 18 other federal agencies, and 424 out-of-state law enforcement agencies. The ACLU is asking for injunctive relief to stop the sharing of ALPR data with out of state or federal agencies.

4) **Law enforcement use of ALPR systems**: ALPR systems can be used to serve four specific public safety goals: (1) crime analysis; (2) alert law enforcement officials that a license plate number on a "hot list" is nearby; (3) monitor the movements of vehicles operated by individuals with travel restrictions; and (4) identify criminal conduct that was otherwise unnoticed. Hot lists, are generally databases of "vehicles of interest," such as such as the plate numbers of stolen cars or cars suspected of being involved in crimes or gang activity. That way, police receive real time updates when particular vehicles are spotted by an ALPR camera. Hot lists may be compiled by the local law enforcement agency using the ALPR system or by other state or federal government agencies.

Law enforcement may also purchase ALPR data from private databases. As described in this Committee's analysis of SB 34, these private databases are also big business. One of the most well-known companies in this space, Livermore-based Vigilant Solutions, "has seen its appeal among law enforcement officers grow because it can offer police departments access to a trove of more than 2 billion scans, maintained by an affiliated company, Digital Recognition Network. That database is fed by cameras attached to vehicles driven by repossession agents roving the nation's roadways. The two companies have 160 employees. Vigilant reports having more than 3,500 law enforcement clients that either use the company's cameras or access its data. Digital Recognition Network has more than 250 customers. A Vigilant representative estimated that the entire industry brings in as much as $500 million a year."[1]

[1] Faturechi, *Use of license plate photo databases is raising privacy concerns*, LA Times, (May 16, 2014).

A 2011 transportation budget trailer bill regulated the use of ALPR technology by the CHP. Pursuant to AB 115 (Committee on Budget, Ch. 38, Stats. 2011), the CHP is only authorized to retain data captured by ALPR systems for 60 days, except where the data is being used for felony investigations or as evidence. The CHP is also prohibited from selling the data for any purpose or making the data available to an agency or person other than law enforcement agencies or officers. The data may only be used by law enforcement agencies for purposes of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense. The CHP is required to monitor the internal use of ALPR data to prevent unauthorized use, and to regularly report to the Legislature on its ALPR practices and uses.

As introduced, this bill would similarly permit other California public agencies to sell and share ALPR data with out-of-state law enforcement (both state and federal), so long as that information is being shared or sold to locate a vehicle or person reasonably suspected of being involved in the commission of a public offense. Amendments taken in the Assembly Transportation Committee would temper the sharing of ALPR data by prohibiting the transfer to any state that: 1) has laws that would violate the California Values Act; 2) a state that is subject to a ban on state-funded and state-sponsored travel because the state enacted a law that voids or repeals, existing protections against discrimination on the basis of sexual orientation, gender identity, or gender expression, as specified; or, a state that has enacted laws that deny or interfere with a woman’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 woman.

Oakland Privacy argues that these amendments, while intended to address policy concerns, make the bill operationally impossible. Oakland Privacy writes in opposition:

> [A]pproximately 60% of California's hundreds of law enforcement agencies currently use automated license plate readers and more adopt the technology every year. Each of those agencies shares their data agency-to-agency with anywhere from a few dozen to as many as 1,000+ agencies across the country. The California State Auditor observed in their 2019-2020 state audit of California's use of ALPR that many agencies are not fully aware of all their sharing partners.
>
> AB 2192 now proposes that each of California's hundreds of law enforcement agencies constantly monitor state and local laws across 50 other states and adjust their ALPR sharing every time a new state or local law is passed in any state limiting or restricting the right to an abortion. It's not even clear that full-time legislative analysts can be up to speed on legislation across 50 states, much less every police department in California. Each agency would not only need to identify the passage of laws, but then review their entire sharing list for individual agencies located in the state in question.
>
> […]
>
> There is no practical way for the state to ensure that every agency goes through this process every time a red state modifies their abortion laws, and no practical way to ensure that the sharing is in fact restricted by each agency in California to each agency in another particular state.

In support of this bill, a large coalition of law enforcement agencies have submitted letters in support. Those letters mirror the justification of the sponsor:

> ALPR data has proven to be a useful tool when it comes to investigating crimes and identifying or excluding suspects. Existing law governing the use of ALPR data attempts to strike a balance between ALPR's utility as a crime fighting measure and the desire to protect motorists' privacy.

5) **Auditor's report calls for more oversight with regard to law enforcement use of ALPR**: 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.[2]

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 they 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 PI about individuals, heightening the need for stronger security measures and more circumscribed access and use policies.

The Auditor additionally had difficulty determining whether the agencies made informed decisions about sharing the ALPR data at all because of deficient record keeping. Two of the agencies reviewed approved sharing ALPR data with hundreds of entities and one shared ALPR data with over a thousand. The sharing occurred with most of the other 49 states and included public and private entities.

For the most part, agencies relied on Vigilant Solutions software and protocols rather than establishing their own protocols and safety measures. The report indicates that for the agencies partnering with Vigilant, it was not clear who owns the data stored in the Vigilant cloud. In addition, 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.

[2] *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].

Because of the many issues identified by the Auditor related to law enforcement's deficient ALPR policies, the report recommended that the Legislature direct the DOJ to develop a policy template that local law enforcement agencies can use as a model for their ALPR policies. This bill would now codify that recommendation.

SB 210 (Wiener), co-sponsored by the Electronic Frontier Foundation and the Media Alliance sought to codify many of the Auditor's recommendations. That bill was held under submission by the Senate Appropriations Committee.

6) **Prior legislation**: SB 210 (Weiner, 2021) would have required ALPR operators and end-users to conduct annual audits to review ALPR searches and require most public ALPR operators and end-users to destroy all ALPR data within 24 hours that does not match information on a "hot list." It also would require the Department of Justice (DOJ) to make available model ALPR policies and issue guidance to local law enforcement agencies, as specified. That bill was held under submission by the Senate Appropriations Committee.

SB 34 (Hill, Ch. 532, Stats. 2015) established regulations on the privacy and usage of ALPR data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system.

AB 1076 (Kiley, 2021) would have required the DOJ to draft and make available on its internet website an ALPR system policy template for local law enforcement agencies and requires 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 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 include procedures to ensure non-anonymized 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.

7) **Double referral**: This bill was double referred to the Assembly Committee on Transportation where it was heard on April 4, 2022 and passed out 9-0.

REGISTERED SUPPORT / OPPOSITION:

Support

Arcadia Police Officers Association
Burbank Police Officers' Association
California Association of Highway Patrolmen
California Coalition of School Safety Professionals
California State Sheriffs' Association
Claremont Police Officers Association
Corona Police Officers Association
Culver City Police Officers' Association

Fullerton Police Officers' Association
Inglewood Police Officers Association
Los Angeles School Police Officers Association
Newport Beach Police Association
Palos Verdes Police Officers Association
Peace Officers Research Association of California (PORAC)
Placer County Deputy Sheriffs' Association
Pomona Police Officer Association
Riverside Police Officers Association
Riverside Sheriffs' Association
Santa Ana Police Officers Political Action Committee
Upland Police Officers Association

Opposition

Access Reproductive Justice
ACLU California Action
Alianza Sacramento
All Family Legal
Asian Americans Advancing Justice - California
Asian Law Alliance
California Church Impact
California Immigrant Policy Center
Consumer Federation of California
Council on American-islamic Relations, California
Electronic Frontier Foundation
Ice Out of Marin
Maternal and Child Health Access
Mpact Global Action
Mpact Global Action for Gay Men's Health and Human Rights
National Center for Lesbian Rights
National Center for Youth Law
Oakland Privacy
Planned Parenthood Affiliates of California
Privacy Rights Clearinghouse
Secure Justice
Teach
TGI Justice Project
The Translatin@ Coalition

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200