

Date of Hearing: April 4, 2022

ASSEMBLY COMMITTEE ON TRANSPORTATION

Laura Friedman, Chair

AB 2192 (Ramos) – As Amended March 29, 2022

SUBJECT: Automated license plate recognition systems: information sharing

SUMMARY: Authorizes 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 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. Specifically, **this bill:**

- 1) Prohibits the sale of ALPR data to the federal government or to other states under any of the following circumstances:
 - a) The sale, sharing or transferring of ALPR information would violation a provision of the California Values Act.
 - b) 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,
 - c) 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.
- 2) 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.
- 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.

- 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.
- 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.
- 6) Defines a "Public agency" to mean 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.
- 7) 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.
- 8) 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.
- 9) Defines a public offense as "A crime or public offense is an act committed or omitted in violation of a law forbidding or commanding it."
- 10) Requires CHP to monitor internal use of the license plate reader data to prevent unauthorized use.
- 11) 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.
- 12) 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.
- 13) 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.

- 14) 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.
- 15) Prohibits a law enforcement agency from using a departments moneys to investigate, interrogate, detain, detect, or arrest persons for immigration enforcement purposes, including the sharing of personal information.
- 16) Establishes the California Values Act, which prohibits state law enforcement from using state resources to assist in the enforcement of immigration, except as specified.
- 17) 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.
- 18) 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.

FISCAL EFFECT: Unknown

COMMENTS: According to the United States Department of Justice, the Police Scientific Development Branch in the United Kingdom (U.K) invented ALPR technology in 1976. The technology rose to prominence after Provisional Irish Republican Army terrorist bombings in the City of London that resulted in the establishment of a surveillance and security network around the city referred to as the "ring of steel" in 1993.

ALPR systems are capable of capturing up to 1,800 plates per minute at speeds of 120-160 miles per hour. According to the Brennan Center for Justice, ALPR systems can be mounted on stationary poles, moving police cruisers, and handheld devices. The devices log pictures of the vehicles, and their GPS coordinates. This data can be compared against "hot lists" to find vehicles that have been stolen or help find an abducted child.

Law enforcement agencies use of ALPR was prevalent across the United States by the mid 2000's. The 2007 Law Enforcement Management and Administrative Statistics Survey indicated that as of 2007, 48% of law enforcement agencies with more than 1,000 sworn officers were regularly using ALPR readers, with 32% of agencies with greater than 500 officers, but less than 1,000.

According to the California State Auditor (Auditor), out of the 391 law enforcement agencies in California, 230 police and sheriff departments in California currently use ALPR systems, with 36 more planning to do so. The American Civil Liberties Union (ACLU) in a 2013 report indicated that law enforcement is collecting and storing ALPR images related to individuals not suspected

of a crime, and that this data could be used inappropriately to monitor the movements individuals such as ex-spouses, neighbors, and other associates.

Out of increasing concern surrounding the privacy of individuals data collected through ALPR systems, the Legislature passed and the Governor signed SB 34 (Hill), Chapter 532, Statutes of 2015. According to Senator Hill at the time, "California law has not kept up with the rapid adoption of the technology. Except for the California Highway Patrol and transportation agencies, current California law doesn't require any privacy safeguards or establish any protocols for the use of ALPR systems. Not only has the law failed to keep up with the quick adoption of ALPR, but the entities using ALPR have also been slow in crafting their own internal policies. For example, according to the International Association of Chiefs of Police, only 48% of police agencies across the country have developed policies that govern ALPR use and privacy."

SB 34 imposed a range of privacy protections related to ALPR data. Including requiring ALPR operators to secure information collected by ALPR systems with reasonable operational, administrative, technical, and physical safeguards to ensure confidentiality and integrity. Security and privacy concerns surrounding ALPR systems have only grown since the passage of SB 34 and in 2019 the Auditor reviewed four local law enforcement agencies use of ALPR and found that these agencies were accumulating massive amounts of data that were unrelated to any criminal investigations. Also, the Auditor found that none of the agencies they reviewed were complying with the requirements set forth in SB 34, and that the Los Angeles Police Department (LAPD) had no ALPR policy at all. The other three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data. For example, of the 320 million images LAPD had collected, only 400,000 generated an immediate match against a hot list.

According to the Auditor, "The agencies we reviewed have few safeguards for the creation of ALPR user accounts and have also failed to audit the use of their ALPR systems. Instead of ensuring that only authorized users' access ALPR data for appropriate purposes, the agencies have left their systems open to abuse by neglecting to institute sufficient oversight. Over the years, the media has reported that some individuals within law enforcement used or could use data systems—and sometimes ALPR systems—to obtain information about individuals for their personal use, including to locate places they regularly visit, to determine their acquaintances, and to blackmail them based on this information. ALPR systems should be accessible only to employees who need the data, and accounts should be promptly disabled otherwise. However, the agencies often neglected to limit ALPR system access and have allowed accounts that should be disabled to remain active longer than is prudent. To further ensure that individuals with access do not misuse the ALPR systems, the agencies should be auditing the license plate searches that users perform, along with conducting other monitoring activities. Instead, the agencies have conducted little to no auditing and monitoring and thus have no assurance that misuse has not occurred."

The State Auditor recommended that DOJ draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies, and that DOJ 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. It also suggests the Legislature set a requirement for when law enforcement agencies should delete ALPR data.

This bill would expand the ability for law enforcement agencies to share ALPR data with law enforcement agencies, both federal and state, for the purposes of investigating any crime.

According to the author, “An ambiguity in California law governing which public agencies may use automated license plate reader (ALPR) data. As currently written, the law limits sharing to only public agencies, and it is unclear whether the definition of a public agency is limited to California agencies and thereby excludes out-of-state or federal agencies, even law enforcement agencies.

AB 2192 would clarify that local law enforcement agencies can share ALPR data with out-of-state or federal law enforcement agencies to locate a vehicle or person reasonably suspected of involvement in commission of a crime. The proposed change would conform to the statute that currently covers the California Highway Patrol’s ability to share ALPR data.

ALPR data has proven to be a useful and successful tool when it comes to investigating crimes. Existing law governing ALPR data use attempts to strike a balance between ALPR’s utility as an investigative tool and protection of motorists’ privacy. AB 2192 clarifies ambiguities and would ensure this common sense and balanced approach is used in all federal and out-of-state law enforcement requests for ALPR data.”

Under existing law for the purposes of ALPR data, a public agency means “the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including, but not limited to, a law enforcement agency.”

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 Border 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.

The ACLU, EFF, Access Reproductive Justice, the Consumer Federation and various other groups, writing in opposition, state “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. For example, carve outs from current law to allow sharing ALPR information across state lines in instances of kidnapping or murder inquiries could still implicate parents supportive of their trans kid who have been charged with kidnapping during contentious child custody cases or, in a post-*Roe* world, recipients of abortion care who live in states that define abortion as murder.”

To address some of the concerns raised by the opponents, the author amended the bill to prohibit the sharing of data with states that have restricted abortion prior to the viability of the fetus and States that are on California's “no fly list” because they have passed legislation discriminating against the lesbian, gay, bisexual, Transgender communities. In addition, the bill restates existing law placing restrictions on using state resources for immigration purposes.

The California State Sheriffs' Association, the sponsors of this bill, argue “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. 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.”

Double referral: Should this bill pass this committee it will be referred to the Committee on Housing and Community Development.

Previous Legislation: SB 34 (Hill), Chapter 532, Statutes of 2015, established regulations on the privacy and usage of automatic license plate recognition (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), of 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 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 210 (Weiner), of the current legislative session requires 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 DOJ to make available model ALPR policies and issue guidance

to local law enforcement agencies, as specified. That bill is pending before Senate Appropriations Committee.

SB 1143 (Wiener), of 2020 was largely identical to SB 210. It was held by the Senate Transportation Committee.

AB 1782 (Chau), of 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.

REGISTERED SUPPORT / OPPOSITION:

Support

California State Sheriffs' Association
Peace Officers Research Association of California (PORAC)

Oppose

Access Reproductive Justice
ACLU California Action
All Family Legal
Asian Law Alliance
California Church Impact
Consumer Federation of California
Electronic Frontier Foundation
Maternal and Child Health Access
Mpact Global Action for Gay Men's Health and Human Rights
National Center for Lesbian Rights
National Center for Youth Law
Oakland Privacy
Privacy Rights Clearinghouse
Secure Justice
Teach
Tgi Justice Project
The Translatin@ Coalition

Analysis Prepared by: David Sforza / TRANS. / (916) 319-2093