Date of Hearing: March 27, 2023

ASSEMBLY COMMITTEE ON TRANSPORTATION
Laura Friedman, Chair
AB 1463 (Lowenthal) – As Amended March 9, 2023

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

SUMMARY: Requires a 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 subpoena, 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 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 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.

3) Explicitly prohibits that ALPR information shall not be sold, shared or transferred to out-of-state or federal agencies without a valid subpoena, court-order, or warrant.

4) Prohibits an ALPR operator or ALPR end-user that is a 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 60 days after the date of collection unless they are accessing an ALPR system operated by an airport authority.

EXISTING LAW:

1) Defines 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. (Civil Code (CIV) 1798.90.5)

2) 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 1798.90.51)

3) 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 1798.90.53)

4) 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. (CIV 1798.90.55)

5) 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. (CIV 1798.90.5)

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. (Vehicle Code (VEH) 2413)

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 2413)

8) Requires CHP to monitor internal use of the license plate reader data to prevent unauthorized use. (VEH 2413)

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 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 1798.29 and 1798.82)

FISCAL EFFECT: Unknown

COMMENTS:

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

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 information on 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-2000s. 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.

California's use of ALPRs and Legislative response: According to a 2019 Auditor report, 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. 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 on 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 unrelated to 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.

California State Audit on ALPR users: According to the Auditor's 2019 report, "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 the Department of Justice (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.

The California State Sheriffs Association, writing in opposition to this bill, argue " 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."

Oakland Privacy, writing in support of this bill, argues "Assembly Bill 1463 is both timely, and somewhat overdue. In 2015, the Legislature unanimously passed AB 34 from Senator Jerry Hill which imposed policy transparency requirements and attempted to restrict out of state sharing, although it did not end the practice. In 2019, then Assembly-privacy chair Ed Chau of Monterey Park wrote a bill to purge non-evidentiary license plate scans from databases after 60 days. AB 1782 was voted out of the Assembly Judiciary and Privacy committees and passed by the full

Assembly in May of 2019.3 AB 1782 was delayed in the Senate due to Senator Scott Weiner's request to the JLAC for the California State Auditor to review ALPR use in California. The auditor's report was released in February of 2020.

Senator Weiner's SB 210 attempted to replicate New Hampshire's state policy of immediate purges, and Assemblymember James Ramos' AB 2192 attempted to explicitly authorize out of state sharing of ALPR scans. Neither bill advanced out of their respective houses. So three years after the California State Auditor declared that legislative action is necessary to protect Californian's privacy rights, nothing has happened, and new out of state laws focused on out of state visitors seeking reproductive and gender-affirming medical care have made restrictions on sharing geolocation data critical to California's safety net.

In just the last three 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. 10 After the sharing became public, both agencies stated it had been a "mistake" and would cease, but such mistakes can cause deportations and family separations that cannot be undone and are in direct contradiction to Legislature's policies regarding immigration enforcement and local and state law enforcement agencies. 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.

Assembly Bill 1463 addresses these problems by minimizing the amount of geolocation data available to be mishandled."

Committee Comments: This bill seeks to implement the California State Auditor's (Auditor) 2019 recommendation that the Legislature set a date in which law enforcement has to delete ALPR data. It also seeks to prevent California agencies from selling or sharing ALPR data with out-of-state agencies, something the sponsors of this bill contend is existing law, but needs clarification because various law enforcement agencies have violated this provision. For example, last year the Marin County Sheriff settled a lawsuit with the American Civil Liberties Union (ACLU) for sharing information with out-of-state and federal agencies.

Double referral: Should this bill pass this committee it will be referred to the Committee on Privacy and Consumer Protection.

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 2192 (Ramos of 2022) would have authorized 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. That bill passed out of this committee and was taken up in Assembly Privacy and Consumer Protection for testimony only.

SB 210 (Weiner of 2022) 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 DOJ to make available model ALPR policies and issue guidance to local law enforcement agencies, as specified. That bill was held on suspense by Senate Appropriations Committee.

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 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

Oakland Privacy

Opposition

California State Sheriff's Association

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