Date of Hearing: April 19, 2021

ASSEMBLY COMMITTEE ON TRANSPORTATION
Laura Friedman, Chair
AB 1076 (Kiley) – As Introduced February 18, 2021

SUBJECT: Automated license plate recognition systems: model policy

SUMMARY: Requires the Department of Justice (DOJ) to draft and make available on its internet website an Automated License Plate Reader (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.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy.

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.

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) 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.

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.

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

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.

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.

11) 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.

12) 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.

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 1000.

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 California State 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 requires DOJ to make available on its website a policy template, but is silent on the recommendation to require law enforcement agencies to delete data.

According to the author, "Although current law requires agencies to have a policy to protect data in ALPRs, the State Auditor found that agencies either did not have a policy for ALPR usage, or the policy was deficient. AB 1076 requires the Department of Justice to create a template of policy regulations that comply with current law pertaining to ALPR data storage. This template shall be made available on Justice's website for the use or reference of law enforcement."

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

Related Legislation:

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.

Prior 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.

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

Peace Officers Research Association of California (PORAC)

Opposition

None on file

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