SENATE COMMITTEE ON APPROPRIATIONS
Senator Anthony Portantino, Chair
2021 - 2022 Regular Session

SB 210 (Wiener) - Automated license plate recognition systems: use of data

Version: March 15, 2021
Urgency: No
Hearing Date: April 5, 2021
Policy Vote: JUD. 9 - 1
Mandate: No
Consultant: Shaun Naidu

Bill Summary: SB 210 would require automated license plate recognition system (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 issues guidance to local law enforcement agencies, as specified.

Fiscal Impact:

- DOJ: The department reports costs of $323,000 (and 3.0 PY) in FY 2021-2022, $576,000 (and 3.0 PY) in FY 2022-2023, $506,000 (and 3.0 PY) in FY 2023-2024, and $433,000 (and 2.0 PY) annually thereafter to make available on its website a model ALPR policy template for public agencies, to develop and issue guidance to help local law enforcement agencies to identify and evaluate the data that currently is stored in their ALPR databases. (General Fund)

- Department of Corrections and Rehabilitation: Unknown costs to the Division of Adult Parole Operation, which uses ALPR in its California Parole Apprehension Team. (General Fund)

- California Highway Patrol (CHP): The department reports minor and absorbable costs associated with this measure.

Background: According to the analysis of this bill by the Senate Committee on Judiciary:

> In 2015, SB 34 (Hill, Ch. 532, Stats. 2015) sought to address some of the concerns about the privacy of [ALPR] information by placing certain protections around the operation of ALPR systems and the use of ALPR data. (*See* Civ. Code §§ 1798.90.51, 1798.90.53.) The resulting statutes provided that both ALPR operators and ALPR end-users were 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. They were 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:

- the authorized purposes for using the ALPR system, and collecting, accessing, and/or using ALPR information;
- 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. It must also identify the necessary training requirements;
- a description of how the ALPR system will be monitored to ensure the security of the ALPR information, and compliance with all applicable privacy laws;
- a process for periodic system audits for end-users;
- the purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons;
- the title of the official custodian, or owner, of the ALPR information responsible for implementing the relevant practices and policies;
- a description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors; and
- 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.

Additionally, existing law allows CHP to retain license plate data captured by license plate reader technology (LPR), which is another term for an ALPR, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. The department is prohibited from selling LPR data for any purpose and cannot make the data available to a non-law enforcement agency or officer. A law enforcement agency may use the data only for purposes of locating vehicles or persons when either are reasonably suspected of being involved in the commission of a public offense. Existing law also requires CHP to, as a part of the annual automobile theft report submitted to the Legislature, report the LPR practices and usage, including the number of LPR 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.

Proposed Law: This bill would:

- Require ALPR operators and end-users to carry out two specific security procedures and practices, as part of the existing requirement to maintain such procedures and practices:
  - Conduct annual audits to review ALPR end-user searches during the previous year to assess user searches, determine if all searches were in compliance with the relevant usage and privacy policy, and, if the ALPR operator is a public agency that is not an airport authority, confirm that all ALPR data that does not match hot list information has been routinely destroyed in 24 hours or less; and
  - Where the operator is a non-airport authority public agency, destroy all ALPR data that does not match information on a hot list in 24 hours or less and include such a requirement in their own usage and privacy policy.

- Require the audits to be made available to the public in writing and posted on the operator's website, as specified.
- Require an ALPR operator or an ALPR end-user that accesses or provides access to ALPR information to conduct an annual audit to review ALPR end-user searches during the previous year to assess user searches, determine whether all searches were in compliance with the usage and privacy policy, and, if the ALPR operator or end-user is a public agency that is not an airport authority, confirm that all ALPR data that does not match hot list information has been routinely destroyed in 24 hours or less. It also would require ALPR end-users that access or provide access to ALPR information to maintain a record of that access and to require that ALPR information be used only for the purposes authorized in their usage and privacy policy.
- Require an ALPR operator or end-user that is a public agency that is not an airport authority to include a requirement in its usage and privacy policy that all ALPR data is to be destroyed within 24 hours if it does not match hot list information.
- Define "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.
- Require DOJ, by July 1, 2022, to draft and make available on its website a policy template that public agencies may use as a model for their ALPR policies.
- Require DOJ to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they currently are storing in their ALPR database. The guidance must include, but not be limited to, the necessary security requirements agencies should follow to protect the data in their ALPR.
- Prohibit ALPR operators and end-users that are non-airport authority public agencies from accessing an ALPR that retains ALPR information for more than 24 hours that does not match a hot list.

Related Legislation: AB 1782 (Chau, 2019-2020 Reg. Sess.) would have required those operating, accessing, or using ALPR or its 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. AB 1782 was amended to replace this content and address a different topic. It was held on the Suspense File of this Committee.

SB 1143 (Wiener, 2019-2020 Reg. Sess.) was substantially similar to this bill. SB 1143 was never heard in the Senate Committee on Transportation.

SB 34 (Hill, Ch. 532, Stats. 2015) established the existing requirements on ALPR operators and end-users.

Staff Comments: Existing law sets a retention period for ALPR data only for CHP, which, as discussed in Background, above, is allowed to retain data for up to 60 days unless it is being used as evidence or in a felony investigation. SB 210 would require all public agencies, that are not airport authorities, that operate or use ALPR to destroy ALPR data within 24 hours unless it matches hot list information. This bill does not strike or alter the provision of law that provides CHP the ability to retain ALPR data for, generally, up to 60 days, but the 24-hour ALPR data destruction requirement would appear to apply to CHP, as it is a non-airport authority public agency. Generally, where there is a conflict between statutory provisions, the provision enacted "later in time"

would control. In an attempt to harmonize the law, however, a canon of statutory instruction provides that when there are conflicting statutory provisions, one general and one specific, the more specific provision would apply as an exception to the general provision. Consequently, it appears that CHP would be able to maintain ALPR data for up to 60 days despite the generally-applicable 24-hour destruction requirement in SB 210 if it is enacted.

-- END --