



**SB-210 Automated license plate recognition systems: use of data.** (2021-2022)

SHARE THIS:



Date Published: 03/15/2021 02:00 PM

AMENDED IN SENATE MARCH 15, 2021

AMENDED IN SENATE MARCH 05, 2021

CALIFORNIA LEGISLATURE— 2021–2022 REGULAR SESSION

**SENATE BILL**

**NO. 210**

**Introduced by Senator Wiener**  
**(Coauthor: Senator Wieckowski)**  
**(Coauthors: Assembly Members ~~Stone~~ Chiu, Stone, and Ting)**

**January 12, 2021**

An act to amend Sections 1798.90.51, 1798.90.52, and 1798.90.53 of, and to add Sections 1798.90.56 and 1798.90.57 to, the Civil Code, relating to personal information.

**LEGISLATIVE COUNSEL'S DIGEST**

SB 210, as amended, Wiener. Automated license plate recognition systems: use of data.

Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate reader technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law authorizes the department to share that data with law enforcement agencies for specified purposes and requires both an ALPR operator and an ALPR end-user, as those terms are defined, to implement a usage and privacy policy regarding that ALPR information, as specified. Existing law requires that the usage and privacy policy implemented by an ALPR operator or an ALPR end-user include the length of time ALPR information will be retained and the process the ALPR operator and ALPR end-user will utilize to determine if and when to destroy retained ALPR information.

This bill would include in those usage and privacy policies a requirement that, if the ALPR operator or ALPR end-user is a public agency and not ~~subject to a specified provision relating to electronic toll collection and electronic transit fare collection systems, an airport authority,~~ ALPR data that does not match a hot list be destroyed within 24 hours.

Existing law requires an ALPR operator and an ALPR end-user to maintain reasonable security procedures and practices. Under existing law, the reasonable security procedures and practices must include operational, administrative, technical, and physical safeguards to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.

This bill would additionally require those procedures and practices to include an annual audit to review ALPR end-user searches during the previous year and, where the ALPR operator or ALPR end-user is a public agency and not ~~subject to a specified provision relating to electronic toll collection and electronic transit fare collection systems, an airport authority~~, the destruction of all ALPR information that does not match information on a hot list within 24 hours. The bill would also ~~prohibit, except as specified, prohibit~~ an ALPR operator or an ALPR end-user that is a public agency *and not an airport authority* from accessing an ALPR system that ~~contains ALPR information that is more than 24 hours old, retains ALPR information for more than 24 hours that does not match a hot list.~~

Existing law requires an ALPR operator that accesses or provides access to ALPR information to maintain a record of that access and require that ALPR information only be used for the authorized purposes described in the usage and privacy policy.

This bill would extend the requirement to keep a record of access to ALPR information to an ALPR end-user. The bill would additionally 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 and to confirm that, if the ALPR operator or ALPR end-user is a public agency and not ~~subject to a specified provision relating to electronic toll collection and electronic transit fare collection systems, an airport authority~~, all ALPR information that does not match a hot list is routinely destroyed in 24 hours or less. The bill would require these annual audits be made available to the public in writing, and, if the ALPR operator or ALPR end-user has an internet website, would require the annual audits be posted conspicuously on that internet website.

This bill would require the Department of Justice, on or before July 1, 2022, to draft and make available on its internet website a policy template and would permit local law enforcement agencies to use the template as a model for their ALPR policies. The bill would also require the Department of Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR database systems.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

## THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

### SECTION 1. The Legislature finds and declares all of the following:

- (a) It is well documented that agencies engaged in federal immigration enforcement are exploiting automated license plate reader (ALPR) databases containing the locations of immigrant drivers as part of their efforts to locate and deport Californians.
- (b) The selling, sharing, or transferring of ALPR information by a California state or local public agency with an out-of-state or federal agency is prohibited under subdivision (b) of Section 1798.90.55 of the Civil Code.
- (c) Despite existing law, public agencies in California share ALPR information with agencies engaged in federal immigration enforcement.
- (d) Further legislation is needed to ensure that ALPR information is retained only for immediate comparison with a hot list and avoids being retained and used for purposes of federal immigration enforcement.

### SEC. 2. Section 1798.90.51 of the Civil Code is amended to read:

#### **1798.90.51.** An ALPR operator shall do all of the following:

(a) 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. These reasonable security procedures and practices shall include, but are not limited to, the following:

(1) An annual audit to review ALPR end-user searches during the previous ~~year, year to assess user searches, determine if all searches were in compliance with the usage and privacy policy, and, if the ALPR operator is a public agency and 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.~~

(2) If the ALPR operator is a public agency and not ~~subject to Section 31490 of the Streets and Highways Code, an airport authority~~, destruction of all ALPR information that does not match information on a hot list in 24 hours or less.

(b) (1) Implement a usage and privacy policy 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. The

usage and privacy policy and annual audits shall be available to the public in writing, and, if the ALPR operator has an internet website, the usage and privacy policy and annual audits shall be posted conspicuously on that internet website.

(2) The usage and privacy policy shall, at a minimum, include all of the following:

(A) The authorized purposes for using the ALPR system and collecting ALPR information.

(B) A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

(C) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

(D) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.

(E) The title of the official custodian, or owner, of the ALPR system responsible for implementing this section.

(F) A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.

(G) The length of time ALPR information will be retained, and the process the ALPR operator will utilize to determine if and when to destroy ALPR information. If the ALPR operator is a public agency and not ~~subject to Section 31490 of the Streets and Highways Code,~~ *an airport authority*, the policy shall require destruction of ALPR data that does not match hot list information in 24 hours or less.

(c) For purposes of this title, "hot list" means a list or lists of license plates of vehicles of interest against which the ALPR system is comparing vehicles on the roadways.

**SEC. 3.** Section 1798.90.52 of the Civil Code is amended to read:

**1798.90.52.** If an ALPR operator or an ALPR end-user accesses or provides access to ALPR information, the ALPR operator or ALPR end-user shall do all of the following:

(a) Maintain a record of that access. At a minimum, the record shall include all of the following:

(1) The date and time the information is accessed.

(2) The license plate number or other data elements used to query the ALPR system.

(3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

(4) The purpose for accessing the information.

(b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51.

(c) Conduct an annual audit to review ALPR end-user searches during the previous year to assess user searches, determine if all searches were in compliance with the usage and privacy policy, and, if the ALPR operator or ALPR end-user is a public agency and not ~~subject to Section 31490 of the Streets and Highways Code,~~ *an airport authority*, confirm that all ALPR data that does not match hot list information has been routinely destroyed in 24 hours or less.

**SEC. 4.** Section 1798.90.53 of the Civil Code is amended to read:

**1798.90.53.** An ALPR end-user shall do all of the following:

(a) 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. *These reasonable security procedures and practices shall include, but not be limited to, an annual audit to review ALPR end-user searches during the previous year to assess user searches, determine if all searches were in compliance with the usage and privacy policy, and, if the ALPR end-user is a public agency and 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.*

(b) (1) Implement a usage and privacy policy in order to ensure that the access, use, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. The usage and privacy policy and annual audits shall be available to the public in writing, and, if the ALPR end-user has an internet website, the usage and privacy policy and annual audits shall be posted conspicuously on that internet website.

(2) The usage and privacy policy shall, at a minimum, include all of the following:

(A) The authorized purposes for accessing and using ALPR information.

(B) A description of the job title or other designation of the employees and independent contractors who are authorized to access and use ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

(C) A description of how the ALPR system will be monitored to ensure the security of the information accessed or used, and compliance with all applicable privacy laws and a process for periodic system audits.

(D) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.

(E) The title of the official custodian, or owner, of the ALPR information responsible for implementing this section.

(F) A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.

(G) The length of time ALPR information will be retained, and the process the ALPR end-user will utilize to determine if and when to destroy ALPR information. If the ALPR end-user is a public agency and not ~~subject to Section 31490 of the Streets and Highways Code,~~ *an airport authority*, the policy shall require destruction of ALPR data that does not match hot list information in 24 hours or less.

**SEC. 5.** Section 1798.90.56 is added to the Civil Code, immediately following Section 1798.90.55, to read:

**1798.90.56.** (a) On or before July 1, 2022, the Department of Justice shall draft and make available on its internet website a policy template that public agencies may use as a model for their ALPR policies.

(b) The Department of Justice shall develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR database systems. The guidance shall include, but not be limited to, the necessary security requirements agencies should follow to protect the data in their ALPR systems.

**SEC. 6.** Section 1798.90.57 is added to the Civil Code, immediately following Section 1798.90.56, to read:

**1798.90.57.** An ALPR operator ~~that is a public agency, and an ALPR end-user that is a public agency, shall not access an ALPR system that contains ALPR information that is more than 24 hours old except to access ALPR information that matches hot list information.~~ *or ALPR end-user that is a public agency and is not an airport authority shall not access an ALPR system that retains ALPR information for more than 24 hours that does not match a hot list.*