COMMITMENT
INTEGRITY
LEADERSHIP

February 13, 2020
Report 2019-118

FACT SHEET

Elaine M. Howle *State Auditor*

CONTACT: *Margarita Fernández* | *(916) 445-0255 x 343* | *MargaritaF@auditor.ca.gov*

Automated License Plate Readers

To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects

Background

Many law enforcement agencies throughout California use automated license plate reader (ALPR) cameras—either fixed or mobile—to capture images of license plates within their field of view. Software extracts the license plate numbers from the images and stores the images, plate numbers, dates, times, and locations of the image captured in a searchable database. When the system identifies a license plate number in an image, it compares the number to stored lists of vehicles of interest—*hot lists*—and alerts law enforcement when it finds a match. An ALPR system is both a real-time tool for law enforcement agencies and an archive of historical information. Our audit focused on the extent to which four local law enforcement agencies are complying with existing law regarding the use of ALPR systems.

Key Recommendations

The Legislature should do the following to better protect individuals' privacy:

- Require the Department of Justice to create a policy template to serve as a model for agencies' ALPR policies, and develop guidance for identifying and evaluating types of data stored in ALPR systems and the security requirements needed.
- Establish a maximum data retention period for ALPR images, and specify how frequently ALPR data searches must be audited.

The agencies we reviewed should do the following:

- Improve their ALPR policies and practices, including those related to data security, establishing data retention periods, granting and managing user accounts, and overseeing the ALPR system.
- Update their vendor contracts with needed data safeguards, and ensure that they share ALPR images appropriately.

Key Findings

- Although each of the agencies has been using ALPR as far back as 2007, the agencies either do not have ALPR policies or their policies are deficient and their practices do not adequately consider the individual's privacy when handling or retaining the ALPR images and associated data.
- The agencies may not be adequately protecting sensitive data that agency personnel upload or enter into their ALPR systems, such as personal and criminal justice information; without sufficient security, the systems are at risk of misuse or data breaches.
  - » Three of the agencies have agreed to share their images widely with little knowledge of the receiving entities' rights or needs to access the images.
  - » Three agencies using a cloud vendor may not be protecting ALPR data in conformity with best practices based on federal policies for criminal justice information—the agencies do not have enough data security safeguards in their contracts and two have not updated their contract terms for several years.
  - » All four agencies have different retention periods for ALPR images—from one to five years—but did not consider the usefulness of the images over time and may be retaining images longer than needed.
- Instead of ensuring that only authorized users access their ALPR data for appropriate purposes, the agencies have few safeguards for creating user accounts and have not audited user searches of the data—some agencies did not disable accounts as necessary.

The Agencies' ALPR Policies Are Missing Required Key Elements