



Automated License Plate Readers

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

February 2020

REPORT 2019-118





CALIFORNIA STATE AUDITOR

621 Capitol Mall, Suite 1200 | Sacramento | CA | 95814



916.445.0255 | TTY **916.445.0033**



For complaints of state employee misconduct,
contact us through the **Whistleblower Hotline:**

1.800.952.5665

Don't want to miss any of our reports? Subscribe to our email list at

auditor.ca.gov





February 13, 2020
2019-118

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

As directed by the Joint Legislative Audit Committee, my office conducted an audit of local law enforcement agencies' use of automated license plate readers (ALPR); the following report details the audit's findings and conclusions. In general, we determined that the law enforcement agencies we reviewed must better protect individuals' privacy through ensuring that their policies reflect state law. In addition, we found that these agencies must improve their ALPR data security, make more informed decisions about sharing their ALPR data, and expand their oversight of ALPR users.

We reviewed four agencies in detail that operate ALPR systems—Fresno Police Department, Los Angeles Police Department, Marin County Sheriff's Office, and Sacramento County Sheriff's Office. An ALPR system collects and stores license plate images of vehicles passing in its view and enables law enforcement to track a vehicle's movements over time; such a system raises privacy concerns. State law helps address these concerns by requiring agencies to have policies and safeguards in place to protect their ALPR systems from misuse. However, the agencies we reviewed either did not have ALPR policies or their policies were deficient, and they had not implemented sufficient safeguards. For example, none had audited searches of the ALPR images by their staff and thus had no assurance that the searches were appropriate. Furthermore, three of the four agencies have shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images. The statewide survey of law enforcement agencies we conducted found that 70 percent operate or plan to operate an ALPR system, and this raises concerns that these agencies may share the deficiencies we identified at the four agencies we reviewed. Because many of the issues we identified link to the agencies' deficient ALPR policies we recommend that the Legislature direct the California Department of Justice to develop a policy template that local law enforcement agencies can use as a model for their ALPR policies.

Our statewide survey also showed that the period of time law enforcement agencies retain ALPR images varies widely. However, among the four agencies we reviewed none had considered the usefulness of the ALPR images to investigators over time when determining their retention periods. We recommend that the Legislature amend state law to specify a maximum retention period for ALPR images.

Respectfully submitted,

A handwritten signature in black ink that reads "Elaine M. Howle". The signature is written in a cursive, flowing style.

ELAINE M. HOWLE, CPA
California State Auditor

Selected Abbreviations Used in This Report

ACLU	American Civil Liberties Union
ALPR	Automated license plate reader
CHP	California Highway Patrol
CJIS	Criminal Justice Information Services Division
CLETS	California Law Enforcement Telecommunications System
FBI	Federal Bureau of Investigation
GPS	Global positioning system
ICE	U.S. Immigration and Customs Enforcement
IT	Information technology
OECD	Organization for Economic Cooperation and Development

Contents

Summary	1
Introduction	7
Audit Results	
The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy	15
The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk	18
The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts	32
Other Areas We Reviewed	39
Recommendations	40
Appendix A	
Summary of ALPR Survey Responses	45
Appendix B	
Scope and Methodology	49
Responses to the Audit	
Department of Justice	53
Fresno Police Department	55
Los Angeles Police Department	59
California State Auditor's Comments on the Response From the Los Angeles Police Department	61
Marin County Sheriff's Office	63
California State Auditor's Comments on the Response From the Marin County Sheriff's Office	67
Sacramento County Department of Human Assistance	71
Sacramento County Sheriff's Office	73
California State Auditor's Comments on the Response From the Sacramento County Sheriff's Office	77

Blank page inserted for reproduction purposes only.

Summary

Results in Brief

To better protect the privacy of residents, local law enforcement agencies must improve their policies, procedures, and monitoring for the use and retention of license plate images and corresponding data. The majority of California law enforcement agencies (agencies) collect and use images captured by automated license plate reader (ALPR) cameras. The ALPR system is both a real-time tool for these agencies and an archive of historical images. Fixed cameras mounted to stationary objects, such as light poles, and mobile cameras mounted to law enforcement vehicles, capture ALPR images. Software extracts the license plate number from the image and stores it, with the date, time, and location of the scan and sometimes a partial image of the vehicle, in a searchable database. The software also automatically compares the plate number to stored lists of vehicles of interest, called *hot lists* then issues alerts, called *hits* if the plate number matches an entry on the hot list. Agencies compile these hot lists based on vehicles sought in crime investigations and vehicles connected to people of interest—for example, a list of stolen vehicles or of missing persons. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists.

Because an ALPR system stores the plate number and image in a database even if the plate number does not match one on a hot list, the American Civil Liberties Union (ACLU) raised concerns in a 2013 report about law enforcement collecting and storing ALPR images related to individuals not suspected of crimes. The ACLU noted that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates—actions that do not respect individuals' privacy. Although ALPR supporters contend that the images are collected in public places where there is no reasonable expectation of privacy, state law has made privacy a consideration when operating or using an ALPR system. Nonetheless, we found that the handling and retention of ALPR images and associated data did not always follow practices that adequately consider an individual's privacy.

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The four local law enforcement agencies we reviewed—Fresno Police Department (Fresno), Los Angeles Police Department (Los Angeles), Marin County Sheriff's Office (Marin), and Sacramento County Sheriff's Office (Sacramento)—have accumulated a large number of images in their ALPR systems, yet most of these images are unrelated to their criminal investigations.

Audit Highlights . . .

Our audit of the use of automated license plate readers (ALPR) at four local law enforcement agencies highlighted the following:

- » *Local law enforcement agencies did not always follow practices that adequately consider the individual's privacy in handling and retaining the ALPR images and associated data.*
- » *All four agencies have accumulated a large number of images in their ALPR systems, yet most of the images do not relate to their criminal investigations—99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a hot list when the image was made.*
 - *None of the agencies have an ALPR usage and privacy policy that implements all the legally mandated—since 2016—requirements.*
 - *Three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data, and the remaining agency has not developed a policy at all.*
 - *Two of the agencies add and store names, addresses, dates of birth, and criminal charges to their systems—some of these data may be categorized as criminal justice information and may originate from a system maintained and protected by the Department of Justice.*

continued on next page . . .

- *Three agencies use a cloud storage vendor to hold their many images and associated data, yet the agencies lack contract guarantees that the cloud vendor will appropriately protect the data.*
 - *Three agencies share their images with hundreds of entities across the U.S. but could not provide evidence that they had determined whether those entities have a right or a need to access the images.*
- » *Agencies may be retaining the images longer than necessary and thus increasing the risk to individuals' privacy.*
- » *The agencies have few safeguards for creating ALPR user accounts and have not audited the use of their systems.*

For example, at Los Angeles only 400,000 of the 320 million images it has accumulated over several years and stores in its database generated an immediate match against its hot lists. In other words, 99.9 percent of the ALPR images Los Angeles stores are for vehicles that were not on a hot list at the time the image was made. Nevertheless, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to determine the vehicles present at particular locations and to track vehicles' movements at particular times in order to gather or resolve leads in investigations.

Technology gives governments the ability to accumulate volumes of information about people, raising a reasonable question: How is an individual's privacy to be preserved? Effective in 2016 the California Legislature addressed privacy with respect to ALPR systems through Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34) by establishing requirements for these systems, including requiring detailed usage and privacy policies that describe the system's purpose, who may use it, how the agency will share data, how the agency will protect and monitor the system, and how long the agency will keep the data. Yet the agencies we reviewed have not implemented all of the requirements in that law.

Law enforcement agencies must first create policies that set clear guidelines for how they will use ALPR data. Setting certain expectations in writing through an ALPR usage and privacy policy helps ensure that agencies operate their ALPR programs in a manner that better protects individuals' privacy. However, none of the four agencies have an ALPR policy that contains all of the required information. In fact, Los Angeles has not developed an 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. Their poorly developed and incomplete policies contributed to the agencies' failure to implement ALPR programs that reflect the privacy principles in SB 34.

ALPR systems may contain data beyond license plate images. For example, we found that Sacramento and Los Angeles are adding names, addresses, dates of birth, and criminal charges to their ALPR systems, which are then stored in those systems. Some of these data may be categorized as criminal justice information; in addition, the data may originate from the California Law Enforcement Telecommunications System (CLETS), which the California Department of Justice (Justice) maintains. These various types of data require different levels of protection under the law. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. In addition, we believe that policy from the Criminal Justice Information Services

Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI) models reasonable security measures for law enforcement agencies' ALPR data. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of the areas specified in state law.

Fresno, Marin, and Sacramento use a cloud storage solution to hold their many ALPR images and associated data. Although the three agencies told us their systems comply with CJIS policy, none of them could demonstrate the vetting they performed to confirm that their cloud storage vendor did, in fact, meet the CJIS policy standards. Moreover, none of the contracts these three agencies have with their cloud storage vendors include all necessary data security safeguards. Thus, the agencies lack guarantees that the cloud vendor will provide appropriate protection of their data.

Law enforcement agencies of all types may benefit from guidance to improve their policies and data security practices. We surveyed 391 police and sheriff departments statewide, and of those using an ALPR system, 96 percent stated that they have ALPR policies, and nearly all reported that their ALPR data storage solution complies with CJIS policy. However, it is likely that many of the survey respondents have the same problems we identified at the four agencies we visited. Justice has experience guiding law enforcement agencies to help them adhere to state law and to improve their administrative practices. By developing guidance for local agencies on needed ALPR policy elements, Justice could help them improve the quality and completeness of their policies.

State law allows law enforcement agencies to share ALPR images only with public agencies, and it requires such sharing to be consistent with respect for individuals' privacy. Three of the reviewed agencies share their ALPR images widely using features in the ALPR systems that enable convenient sharing of images with minimal effort. Fresno and Marin have each arranged to share their ALPR images with hundreds of entities and Sacramento with over a thousand entities across the United States. However, we did not find evidence that the agencies had always determined whether an entity receiving shared images had a right and a need to access the images or even that the entity was a public agency. We are concerned that unless an agency conducts verifying research, it will not know who is actually using the ALPR images and for what purpose.

In addition, the agencies have not based their decisions regarding how long to retain their ALPR images on the documented usefulness of those images to investigators, and they may be retaining the images longer than necessary, increasing the risk to individuals' privacy. Fresno's policy is to retain ALPR images for

one year; Sacramento's and Marin's policies specify two years. Los Angeles does not have an ALPR policy, and the lieutenant who administers the ALPR program stated that its protocol is to retain the images for at least five years. However, when we reviewed the agencies' ALPR searches over a six-month period in 2019, we found that personnel for three of the four agencies typically searched for images zero to six months old. Nonetheless, the agencies keep the images far longer.

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.

Recommendations

Legislature

To better protect individuals' privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:

- Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.

- Require 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 systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
- Establish a maximum data retention period for ALPR images.
- Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.

Law Enforcement Agencies

To address the shortcomings this audit identified, Fresno, Los Angeles, Marin, and Sacramento should do the following:

- Improve their ALPR policies.
- Implement needed ALPR data security.
- Update vendor contracts with necessary data safeguards.
- Ensure that sharing of ALPR images is done appropriately.
- Evaluate and reestablish data retention periods.
- Develop and implement procedures for granting and managing user accounts.
- Develop and implement ALPR system oversight.

Agency Comments

The four law enforcement agencies we reviewed responded to the draft audit report. Fresno responded that it will use the audit to work to achieve its goal of building trust in its community. Los Angeles responded that it respects individuals' privacy and believes it has policies in place to safeguard information. Nonetheless, it is working on an ALPR policy as required by state law and will perform periodic audits of users' searches. Marin stated it is committed to improvement and will consider the recommendations we made, although it disagreed with several of them. Sacramento stated that it had already begun implementing many of the recommendations, but that it did not agree with how we characterized some of the findings. Justice and the Sacramento County Department of Human Assistance also responded by acknowledging the draft report, although we did not have recommendations directed to either entity.

Blank page inserted for reproduction purposes only.

Introduction

Background

An automated license plate reader (ALPR) is a camera that captures color images of license plates within its field of view. Fixed cameras are mounted on stationary objects, such as light poles, while mobile cameras are mounted on moving objects, such as patrol cars. Software extracts the license plate numbers from the images and stores the images, plate numbers, and dates, times, and locations of the image captures in a searchable database. An *ALPR* system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data. Although the primary focus of each image is the license plate, the image may also show part of the vehicle itself, including individuals within the vehicle, depending on the camera’s position. ALPR technology has existed since the 1970s, yet widespread adoption by U.S. law enforcement agencies began only in the mid-2000s. Law enforcement agencies generally view ALPR technology as a valuable tool in achieving their missions.

We conducted a statewide survey of 391 police and sheriff departments, and the survey confirmed that ALPR use is widespread in California: 230 police and sheriff departments currently use an ALPR system, and 36 plan to use one. Table 1 provides an overview of the ALPR systems of the four law enforcement agencies we reviewed as part of this audit.

Table 1
ALPR Systems of Four Audited Law Enforcement Agencies

LAW ENFORCEMENT AGENCY	NUMBER OF AGENCY PERSONNEL WITH ACCESS TO ALPR DATA	NUMBER OF CAMERA SYSTEMS		CURRENT ALPR VENDOR	DATE AGENCY BEGAN USING CURRENT ALPR VENDOR
		FIXED	MOBILE		
Fresno	231	0	8	Vigilant Solutions, LLC	2016
Los Angeles	13,000	3	393	PIPS Technology*	2007
Marin	38	0	3	Vigilant Solutions, LLC	2010
Sacramento	539	33	27	Vigilant Solutions, LLC	2012

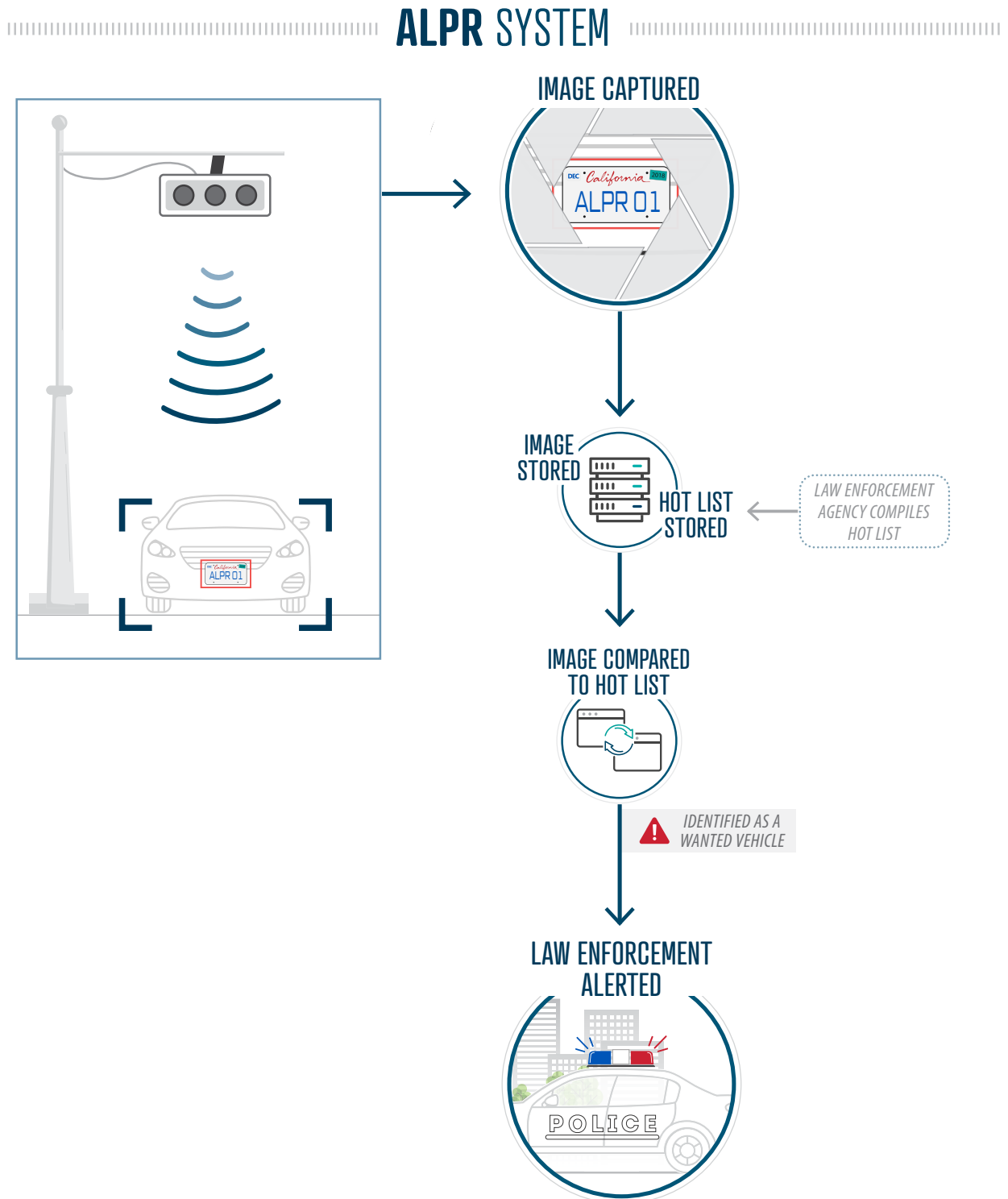
Source: Analysis of reports on ALPR systems as of 2019 and the agencies’ survey responses.

* Los Angeles uses PIPS Technology cameras and a user interface from Palantir Technologies, Inc.

An ALPR system is both a real-time tool for law enforcement agencies and an archive of historical information. After the ALPR system identifies a license plate number in an image, it compares the plate number to stored lists of license plate numbers from vehicles of interest, called *hot lists*. Figure 1 shows how an ALPR system uses hot lists to search stored images. Local law enforcement agencies create their own hot lists and also obtain hot lists from state and federal agencies. For example, the California Department of Justice (Justice) provides hot lists to local agencies that include license plate numbers associated with missing persons, gang members, and suspected terrorists. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists. Regardless of whether a license plate number matches a plate on a hot list (a *hit*), an ALPR system stores the plate image in a database, creating a searchable archive. Officers may search the database in various ways. For example, they may search for a full license plate number to locate a specific vehicle, search for a partial license plate number to locate a group of vehicles, or search for all vehicles recorded at a particular location at specific times.

Law enforcement agencies can share ALPR data with other public agencies. In the ALPR systems we observed, the agency could choose to share ALPR images only, to share hot lists only, or to share both. Accessing ALPR images shared from other jurisdictions enables agencies to search a broader area, such as across county and state lines. In addition, even if an agency does not operate ALPR cameras itself, it can, through sharing agreements, access ALPR images other agencies collect. Our statewide survey showed that among agencies that operate ALPR systems, roughly 84 percent share their images. Sharing hot lists also enables broader search coverage. For example, an agency could share a hot list that provides license plates linked to wanted individuals with other entities in the region. These entities would then receive hit alerts if their cameras detected those plates.

Figure 1
How ALPR Systems Work



Source: Analysis of David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, International Association of Chiefs of Police, Washington, D.C., 2012.

ALPR Vendors Most Commonly Used in California

Law enforcement agencies typically contract with a third-party vendor for an ALPR system. In our statewide survey, most—70 percent—of those that have an ALPR system reported using a company called Vigilant Solutions, LLC (Vigilant). Figure A.1 in Appendix A summarizes these responses. Three of the agencies we reviewed—the Fresno Police Department (Fresno), Marin County Sheriff’s Office (Marin), and Sacramento County Sheriff’s Office (Sacramento)—contract with Vigilant. The Vigilant ALPR system provides a user interface to search license plates and the option to share ALPR images and hot lists with other agencies through the Vigilant system. Fresno, Marin, and Sacramento all store their ALPR images on Vigilant’s server, which is a cloud service, and share their images with other agencies that subscribe to Vigilant’s services. Roughly 22 percent of the survey respondents that have ALPR systems use a company called PIPS Technology. One of the agencies we audited in depth, the Los Angeles Police Department (Los Angeles), purchased its cameras from PIPS Technology, but it stores the images on its own server. Los Angeles uses a software platform called Palantir for the user interface that allows for

searches of its ALPR images, and it shares its ALPR images with other agencies in the region that use the Palantir user interface.

Key Elements Law Enforcement Agencies Must Include in Their ALPR Usage and Privacy Policy

- The authorized purpose for using the ALPR system and collecting, accessing, or using ALPR data.
- 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 data.
- The training requirements for those employees and independent contractors authorized to use or access the ALPR system, or to collect ALPR data.
- A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- The purposes of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time ALPR data will be retained, and the process for determining if and when to destroy retained ALPR data.

Source: Analysis of state law.

State Laws Governing ALPR Systems and Data Sharing

With few exceptions, California law requires public agencies that operate and use ALPR systems to implement a usage and privacy policy. The Legislature passed Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34), effective January 1, 2016, to establish requirements regarding the operation and use of ALPR systems. This law generally requires public agencies, including law enforcement agencies, that operate or use an ALPR system to maintain reasonable security procedures and practices to protect ALPR data, to implement a usage and privacy policy, to make that policy available to the public, and to post that policy on its website should the agency have one, among other provisions. The text box describes required elements of an agency’s ALPR usage and privacy policy.

SB 34 does not specify retention periods for ALPR data, although another state law limits the California Highway Patrol (CHP) to retaining its ALPR images for no more than 60 days, unless those images are being used for felony investigations or as evidence. Agencies implementing ALPR programs after January 1, 2016, must also provide an opportunity for public comment before implementing the program.

In 2018 another state law took effect that limits the information law enforcement agencies can share for immigration enforcement purposes and requires Justice to issue guidance to state and local law enforcement agencies regarding these limitations as they apply to law enforcement databases. In October 2018 Justice issued this guidance, which can also serve as best practices for law enforcement agencies on how to lawfully share ALPR images. The guidance encourages law enforcement agencies that maintain databases to inquire about the purpose for which the other law enforcement agency intends to use the information contained in the database. If a law enforcement agency intends to use the information for immigration enforcement purposes, Justice states that law enforcement agencies should require, as a condition of accessing the database, an agreement that stipulates that access will be made only in cases involving individuals with criminal histories, or for information regarding the immigration or citizenship status of an individual. Beyond this guidance and the hot lists Justice provides to local law enforcement agencies, as we describe earlier, Justice plays no other role in ALPR programs.

State law requires law enforcement agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. These requirements mean that ALPR data are sensitive. For comparison purposes, the California Department of Technology Office of Information Security defines *sensitive data* for state agencies as information that requires special precautions to protect it from unauthorized use, access, disclosure, modification, loss, or deletion. In addition to ALPR images and hot lists, a law enforcement agency can enter other information into its ALPR system, such as personal information and criminal justice information. *Personal information* is information that identifies or describes an individual, including name or physical description. SB 34—whose purpose was, in part, to institute reasonable privacy standards for the operation of ALPR systems—requires that ALPR data be protected with reasonable operational, administrative, technical, and physical safeguards to ensure their confidentiality. Thus, personal information in an ALPR system also requires appropriate and reasonable safeguards. *Criminal justice information*, as defined by the Criminal Justice Information Services Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI), refers to data necessary

for law enforcement and civil agencies to perform their missions. This includes information about vehicles associated with crimes, when accompanied by personal information.

When CJIS provides criminal justice information to law enforcement agencies, it requires those agencies to comply with a minimum set of information technology (IT) security requirements to protect the information, and these requirements can serve as best practices for agencies to follow. Because an agency can enter personal information and criminal justice information into its ALPR system, either as part of a hot list or as a comment added as part of a license plate search, all ALPR data are sensitive and require appropriate safeguards.

Privacy Concerns Related to ALPR Systems

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The agencies we reviewed accumulate a large number of images in their ALPR systems. For example, Sacramento recorded 1.7 million images in one week, and Los Angeles currently has more than 320 million images in its ALPR database that it has accumulated over several years. The majority of these images do not generate hit alerts. For example, data from the Los Angeles system show that at the time of our review only 400,000 (0.1 percent) of the 320 million images Los Angeles has stored generated an immediate match against its hot lists for vehicles associated with car thefts, felonies, or warrants. However, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to target the whereabouts of vehicles at particular times or locations. This storage, retention, and searching of the images, although valuable to law enforcement, has the potential to infringe on individuals' privacy.

Organizations such as the American Civil Liberties Union (ACLU) have criticized law enforcement agencies' collection of ALPR images because of the risks it poses to privacy. The ACLU stated that increasing numbers of cameras, long data retention periods, and sharing of ALPR images among law enforcement agencies allow agencies to track individuals' movements in detail, and it has voiced concerns that such constant monitoring can inhibit the exercise of free speech and association. The ACLU has also raised concerns that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates. There have been occurrences of officers misusing law enforcement databases like those that contain ALPR images. In 2016 the Associated Press conducted a review that found more than

325 instances between 2013 and 2015 in which law enforcement officers who misused databases were fired, suspended, or resigned, and more than 250 instances of reprimands or lesser discipline related to such misuse. For example, the Associated Press reported on a police sergeant in Ohio who pleaded guilty to stalking his ex-girlfriend after he searched law enforcement databases for personal information about her and also the woman's mother, her close male friends, and students from a course she taught.

Law enforcement has recognized the privacy concerns posed by the operation of ALPR systems, yet it has also pointed to the usefulness of the systems. For example, the Police Executive Research Forum (police research forum) and the Mesa Police Department (Mesa) in Arizona conducted a study of the effectiveness of ALPR systems for Mesa's auto theft unit in 2011. They found that officers got nearly three times as many stolen vehicle hits and made about twice as many vehicle recoveries when using an ALPR system, compared to officers performing manual license plate checks. Law enforcement has also found ALPR systems useful for investigations. For example, the assistant chief of the Minneapolis Police Department told the police research forum in 2012 that the department located a vehicle associated with a domestic kidnapping case by searching ALPR images. With regard to the retention of ALPR images, the International Association of Chiefs of Police (chiefs' association) acknowledged the tension between long retention periods and privacy. The chiefs' association noted that a reluctance to destroy records may stem from investigators' experience that seemingly irrelevant or untimely information may acquire new significance as an investigation brings further details to light. However, the chiefs' association also recognized the privacy risks of ALPR images. In a 2009 report, it stated that mobile ALPR cameras could record license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, and staging areas for political protests. The chiefs' association argued that establishing policies regulating ALPR programs could mitigate privacy concerns, and it produced a report in 2012 offering guidance on developing such policies.

Federal Guidance on Privacy Protection

As far back as 1973, the federal government acknowledged that individuals' privacy needs to be protected from arbitrary and abusive record-keeping practices. The U.S. Department of Health, Education, and Welfare, as it was then known, identified principles for the fair collection, use, storage, and dissemination of personal information by electronic information systems. Over time the principles were adapted into information practices. According to the U.S. Government Accountability Office, a revised version of the information practices was published in 1980 by

the Organization for Economic Cooperation and Development (OECD)—an international organization that works with governments, policymakers, and citizens on social, economic, and environmental challenges—and with some variation, these practices form the basis of privacy laws in the United States and around the world. The OECD updated its eight information practices in 2013, and California’s lawmakers included many of these information practices in SB 34. For example, the OECD’s information practices describe the importance of an organization specifying the purposes for which it is collecting and using data; keeping data reasonably safe from the risk of unauthorized access, destruction, use, modification, and disclosure; being open about policies involving data; and being accountable for complying with the information practices.

The U.S. Supreme Court (court) has not directly decided a case that we could find addressing ALPR images, although it has decided cases involving other electronic surveillance. Because license plates are in plain view, the collection of license plate images by law enforcement is not a per se violation of the Fourth Amendment’s prohibition against unreasonable searches and seizures. However, the court has found that certain electronic data that reveal individuals’ movements over an extended period of time, if gathered, do at some point impinge on privacy. The court has specifically addressed these issues with respect to the use of global positioning system (GPS) data and cell-site location information, which is location information linked to cellphone use. Cell-site location information—similar to ALPR images—provides data on an individual’s continuous movements over a potentially unlimited period of time. In a 2018 case involving cell-site location information, the court stated that “[a] person does not surrender all [privacy] protections by venturing into the public sphere.” The court continued, “With access to [cell-site location information], the Government can now travel back in time to retrace a person’s whereabouts,” and noted that the information was collected on everyone, not only “persons who might happen to come under investigation.” Thus, even though case law on electronic data that enable tracking of individuals’ movements over an extended period of time is still evolving, the court has recognized that privacy implications exist for such data, which can include ALPR images.

Audit Results

The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy

California's lawmakers drafted current ALPR law to institute reasonable privacy standards for the operation of ALPR systems. As we discuss in the Introduction, technology gives governments the ability to accumulate significant amounts of information about people, raising the question of how individuals' privacy is to be preserved, and the federal and state governments and courts have issued laws and guidance—including, in the case of California, SB 34—related to the use of such information.

Yet local law enforcement agencies—specifically the four agencies we reviewed—have not done all they could to respect individuals' privacy by incorporating the requirements and concepts in SB 34 into their operations. With few exceptions, SB 34 requires a public agency that operates or uses an ALPR system to implement a usage and privacy policy that describes how the system will be used and monitored to ensure the security of the ALPR data accessed or used. The agencies we reviewed have mature ALPR programs—they have been using their current ALPR vendors since as far back as 2007. However, as we discuss later, we found that the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use.

State law requires law enforcement agencies to administer ALPR programs in ways that respect individual's privacy and protect ALPR data. The law also requires the agencies to have a written usage and privacy policy that sets forth how they will operate and use their ALPR systems. These usage and privacy policies must include the following elements:

- Authorized purposes for using the ALPR system and collecting the data.
- A description of the job title or other designation of individuals who are authorized to use or access the ALPR system.
- Training requirements for the authorized individuals who will use or access the ALPR system.
- A description of how the agency will monitor the ALPR system to ensure the security of the data and compliance with privacy laws.

- The purpose of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time the ALPR data will be retained and the process used to determine if and when to destroy retained ALPR data.

Agencies may expand on these required elements as needed to ensure that their collection, use, maintenance, sharing, and dissemination of ALPR data are consistent with respect for individuals’ privacy.

None of the four agencies we reviewed have an ALPR policy that contains all of the required information, thereby contributing to the agencies’ failure to implement programs that reflect the privacy principles in SB 34. Los Angeles has not developed an ALPR policy, and the policies of the other three agencies are deficient in various ways, as Figure 2 shows. For example, all have failed to fully address how they will monitor system use to ensure compliance with applicable privacy laws, which likely contributed to their failure to institute regular audits of user searches. The agencies could have avoided concerns such as those shown in Figure 2, which we describe later in this report if they had developed more thorough policies. Clear policies that define the purposes and procedures for monitoring ALPR systems help agencies meet their goals.

Figure 2
The Agencies’ ALPR Policies Are Missing Required Key Elements for Respecting Individuals’ Privacy



Source: State law and the agencies’ ALPR policies as well as interviews with the agencies’ management.

As a result of our audit, each of the four agencies is making or considering changes to its policies. The ALPR administrators at Fresno, Marin, and Sacramento agreed that their policies did not contain one or more elements required by state law. They also explained that they did not include certain policy requirements they believed did not apply to their use of ALPR data. For example, Sacramento's ALPR policy does not describe ALPR data-selling restrictions because, according to the ALPR administrator, Sacramento does not currently sell ALPR data. However, because their policies are incomplete and do not specify what personnel cannot do when interacting with their ALPR systems, these three agencies left out critical guidance to staff and increased the risk that staff would use the ALPR system inappropriately. The program administrators at Fresno, Marin, and Sacramento told us that they will consider changes to their policies subsequent to our audit. Although the lieutenant who serves as Los Angeles' program administrator initially believed that the agency's many IT policies covered the ALPR program, when we brought the deficiencies in oversight to his attention, he acknowledged the need for Los Angeles to have an ALPR policy and began drafting one in October 2019.

We are concerned that the policy deficiencies we found are not limited to the agencies we reviewed, and thus law enforcement agencies of all types may benefit from guidance to improve their policies. We surveyed 391 police and sheriff departments statewide about their ALPR programs, and many stated that they have ALPR policies and that these policies are publicly available. Because state law requires each agency that operates or uses an ALPR system to implement a usage and privacy policy, and to make the policy available to the public in writing and post it conspicuously on the agency's website, we inquired about how agencies throughout the State were adhering to these requirements. Of the law enforcement agencies using an ALPR system, 96 percent responded that they have ALPR policies. Of this group, at least 70 percent stated that they have posted their policy to their website. A breakdown of the law enforcement agencies' responses to our survey can be found at <http://auditor.ca.gov/reports/2019-118/supplemental.html>. However, we believe it is likely that many of the survey respondents will have the same problems with the quality and completeness of their policies as the four agencies we visited. As we discuss in the Introduction, Justice has issued guidance to law enforcement agencies to help them understand how to adhere to state law regarding the sharing of information for immigration enforcement purposes. Given Justice's experience and broad reach in the law enforcement community, developing guidance for local law enforcement agencies on needed policy elements could improve the quality and completeness of their policies.

Fresno, Marin, and Sacramento have incomplete ALPR policies, which increases the risk that staff will use the ALPR systems inappropriately.

The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk

Administering ALPR programs in ways that respect individuals' privacy requires a thoughtful and considered approach to data management that the agencies we reviewed have not always taken. Specifically, three of the agencies have agreed to share their images widely with little knowledge of the receiving entities and their need for the images. Moreover, the agencies have not based their decisions regarding retention of images on their actual usefulness to investigators and may be retaining the images longer than necessary, increasing the risk to individuals' privacy.

The Agencies May Not Be Adequately Protecting Their Sensitive ALPR Data

Law enforcement agency personnel can upload or enter sensitive information into their ALPR systems, which may require specific safeguards. As we discuss in the Introduction, this sensitive information could include personal information and criminal justice information. In addition, these data may originate from the California Law Enforcement Telecommunications System (CLETS)—a system that allows law enforcement agencies to obtain information from federal and state databases, such as arrests and fingerprint records from Justice. In reviewing multiple agencies' ALPR policies, we found several that stated that their ALPR systems may contain information obtained through CLETS. Additionally, in a security and compliance memorandum, Vigilant acknowledged that law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

Law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

For example, in addition to license plate images, Sacramento and Los Angeles add data to their systems such as criminal charges and warrant information, in combination with personal information such as names, addresses, dates of birth, and physical descriptions. The added data can be in the form of hot lists that agencies use to search for license plates of interest, as shown in Figure 1 in the Introduction, or they can be data that are entered into open text fields. By running an automated function each day, Sacramento extracts information from several databases and uploads the information as hot lists to its ALPR system. Los Angeles does not create its own hot lists, but it regularly downloads hot lists from Justice and the Los Angeles County Sheriff's Department, then uploads the hot lists to its ALPR system. Another way that information in addition to license plate images gets into an ALPR system is by users adding it to open text fields. Data entered into open text fields are generally associated with license plate searches.

When conducting a search, staff are prompted to enter a case number and the purpose of the search, and they may do so by typing in text. The ALPR systems store this open text in their audit logs, which detail user activity and the reasons for the activity.

In contrast to Sacramento and Los Angeles, Marin and Fresno occasionally upload hot lists into their ALPR systems. With regard to open text fields, we reviewed the audit logs for Marin and Fresno and did not find personal information in combination with other sensitive information in the six months of search records we studied. However, the possibility exists that law enforcement personnel could enter sensitive information into open text fields during ALPR searches.

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches. Systems containing personal information and criminal justice information must have adequate protections to assure individuals' privacy. However, as discussed in the Introduction, ALPR data can originate from different sources, and the source of the information may drive some of the required IT security protocols. On one hand, CJIS developed a policy that dictates the minimum standards that law enforcement agencies must follow to protect criminal justice information they obtain from the FBI (CJIS policy). On the other hand, users of Justice's CLETS system must follow the protections outlined in the CLETS *Policies, Practices and Procedures* document, which describes formal security measures law enforcement agencies must follow to access and protect CLETS information in addition to the CJIS policy requirements.

Further, it can be difficult to know what protections to apply to data from different sources. For example, an individual's address obtained by searching the Department of Motor Vehicles database through CLETS would be subject to Justice's data security requirements, but the same information obtained from a local law enforcement agency database would not. Moreover, the personal information Los Angeles and Sacramento have entered into their ALPR search records does not include its origin, making the required level of protection unclear.

Given these issues and the need to identify a standard that can be uniformly applied to ALPR data regardless of their source, we believe that CJIS policy provides reasonable security measures for law enforcement agencies to protect all of their ALPR data. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of these areas. For example, CJIS policy

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches.

We are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards.

requires agencies to ensure that their sensitive data are encrypted, and it limits physical access to specific personnel authorized to access the data. Nearly all of the 230 agencies that reported using ALPR systems in response to our statewide survey—including Fresno, Los Angeles, Marin, and Sacramento—reported that their ALPR data storage solution complies with CJIS policy.

Nevertheless, we are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards. Fresno, Marin, and Sacramento store their ALPR data in Vigilant's cloud database, and CJIS policy requires agencies to ensure that the cloud vendors that store and process their criminal justice information comply with its security requirements. Such requirements include controlling physical access to sensitive data, encrypting the data, and conducting background checks and training for employees with access to criminal justice information. In addition, before providing sensitive data to a vendor, CJIS requires law enforcement agencies to identify necessary authentication and monitoring controls, such as two-factor authentication and activity logging. Because the Vigilant software is by default accessible via the Internet, an officer may be able to access it using his or her personal device. The ability to access ALPR data in this manner bypasses the agencies' network security safeguards and violates CJIS policy requiring agencies to monitor and control access to the data.

One way to prevent users from signing in to the Vigilant system using personal devices would be to implement authentication controls, such as two-factor authentication. Two-factor authentication involves a second level of verification, such as a passcode sent to a specific device, and allows agencies to require that the passcode be sent only to department-issued devices. Although Vigilant offers two-factor authentication, Marin, Fresno, and Sacramento do not use it. CJIS policy requires two-factor authentication only for systems that directly access federal systems. However, this requirement recognizes that two-factor authentication is more secure than a basic username and password login for systems like Vigilant that are accessible over the Internet. Thus, two-factor authentication could serve as a best practice for agencies to prevent inappropriate access to their ALPR systems.

In addition, monitoring the activity logs can alert program administrators to unauthorized access of their ALPR systems. CJIS policy requires agencies to monitor access to systems that contain criminal justice information. Vigilant provides its clients with logs of network addresses that have accessed their ALPR systems, and although Marin's ALPR program administrator stated that he reviews these logs, administrators from Sacramento and Fresno confirmed that they do not. Reviewing the logs of system access

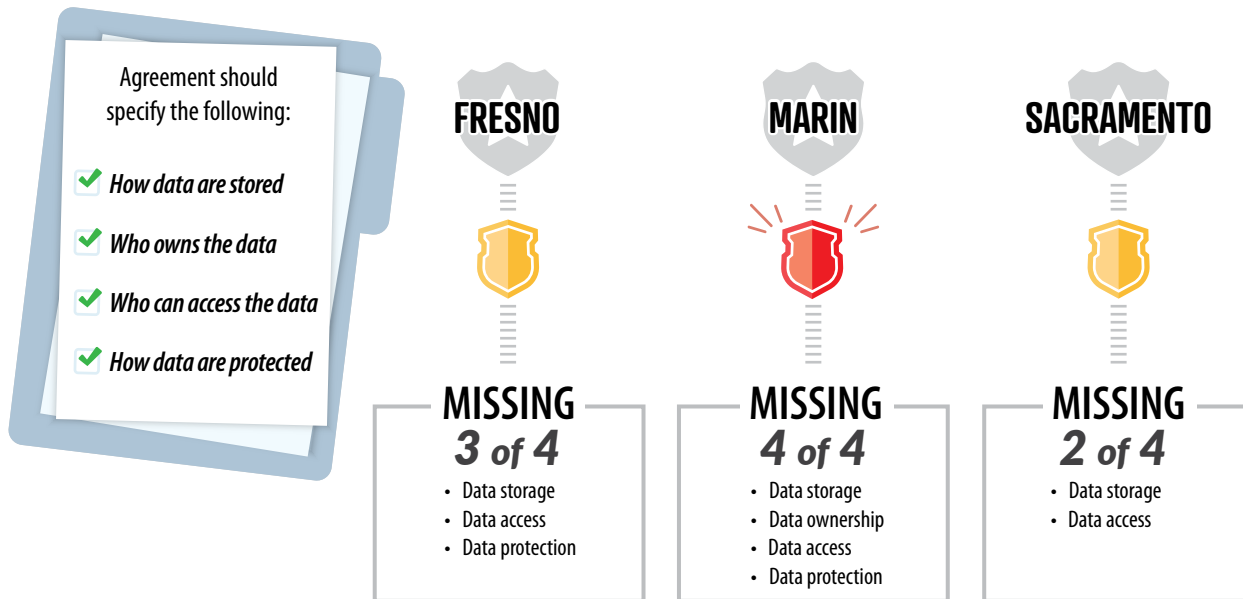
could help the agencies monitor access to their ALPR systems and detect whether someone accesses the ALPR system from an unrecognized network address.

When law enforcement agencies provide sensitive information to ALPR vendors, their contracts should provide assurance that the vendor will adequately protect that information. CJIS policy recommends several provisions that law enforcement agencies should consider including in their contracts to ensure that cloud vendors adequately protect criminal justice information. For example, a contract that protects a law enforcement agency's data would make clear that the agency owns the data it uploads into the ALPR system, that the agency's data will not be stored outside of the United States or Canada, and that employees at the cloud vendor who have access to unencrypted criminal justice information will undergo training and background checks. Without these contract provisions, agencies lack guarantees that the cloud vendor will implement appropriate protections of their data.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts. As Figure 3 shows, none of the agencies' contracts with Vigilant meet all of the CJIS data security requirements. For example, the agencies' contracts do not state that Vigilant will store their data in the United States or Canada. Marin's contract does not make clear that Marin owns the data it adds to the ALPR system. It is important to note that Vigilant claims to implement data security measures that comply with CJIS policy. In a security and compliance memorandum, Vigilant lists steps it takes to encrypt data that may contain criminal justice information, as well as physical and network security safeguards it has in place to prevent unauthorized access to its ALPR cloud. We have no basis to dispute Vigilant's claims, but without strong contract provisions requiring CJIS safeguards, the three agencies have no guarantee that Vigilant will protect their data. As CJIS policy states, ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts.

Figure 3
The Agencies' Existing Agreements With Vigilant Do Not Contain Adequate Data Security Measures



Source: Agencies' agreements with Vigilant and CJS policy requirements.

A lack of IT department involvement and outdated contracts likely contributed to the data security weaknesses we observed. Fresno, Marin, and Sacramento have IT units that administer their systems and ensure compliance with Justice's data security requirements. However, at Fresno and Marin, the IT units are responsible for network security and have little oversight of the ALPR systems' data security. According to Fresno's IT manager, Fresno's main IT unit does not manage user accounts or monitor access to the ALPR system. Fresno has an IT analyst separate from the main IT unit who currently helps administer user accounts and provides technical support for the ALPR system; however, his background is not in network security. A deputy in Marin's auto theft unit manages Marin's entire ALPR system—including user accounts and training. This arrangement is not ideal, since individuals outside of an agency's IT department may lack the expertise necessary to implement adequate data security safeguards. According to Sacramento's ALPR administrator, Sacramento's IT unit recently assumed responsibility for the ALPR system, but before about April 2019, an officer outside of the IT unit administered the ALPR system.

In addition, with the exception of Sacramento, the agencies have not updated their contract terms with Vigilant for several years. The agencies' contracts renew each year when the agencies pay a service fee to Vigilant. As a result, Fresno has not updated its contract for three years, and Marin for nine years. Sacramento updated

its contract terms with Vigilant in September 2019, after using its previous agreement for seven years. Agreements that are not kept current may reflect outdated practices or omit needed assurances, increasing the risk that data are not protected.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access. Los Angeles stores its ALPR data in a city-controlled data center rather than in a vendor cloud like the agencies that use Vigilant. Nevertheless, Los Angeles contracts with Palantir for IT support, and the FBI's 2017 audit of Los Angeles' data security practices identified Palantir as an entity with access to criminal justice information; thus we expected Los Angeles' agreement with Palantir to meet CJIS policy requirements. CJIS policy requires agencies to enter into agreements with vendors that access their criminal justice information. The agreements are to include an FBI-drafted security addendum that outlines specific safeguards a vendor agrees to put in place to comply with CJIS policy and an acknowledgment by the vendor of the great harm that may arise from misusing sensitive data. However, in response to our request for its agreement with Palantir, Los Angeles produced two expired contracts and a 2018 commodities agreement extending its licensing and support for Palantir software. None of these documents contained the FBI-drafted security addendum. Thus Los Angeles was not able to demonstrate that its agreement with Palantir contains appropriate data protections to ensure that Palantir employees with access to Los Angeles' ALPR data will not use the data for unauthorized purposes.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access.

The Agencies Have Not Made Informed ALPR Image-Sharing Decisions

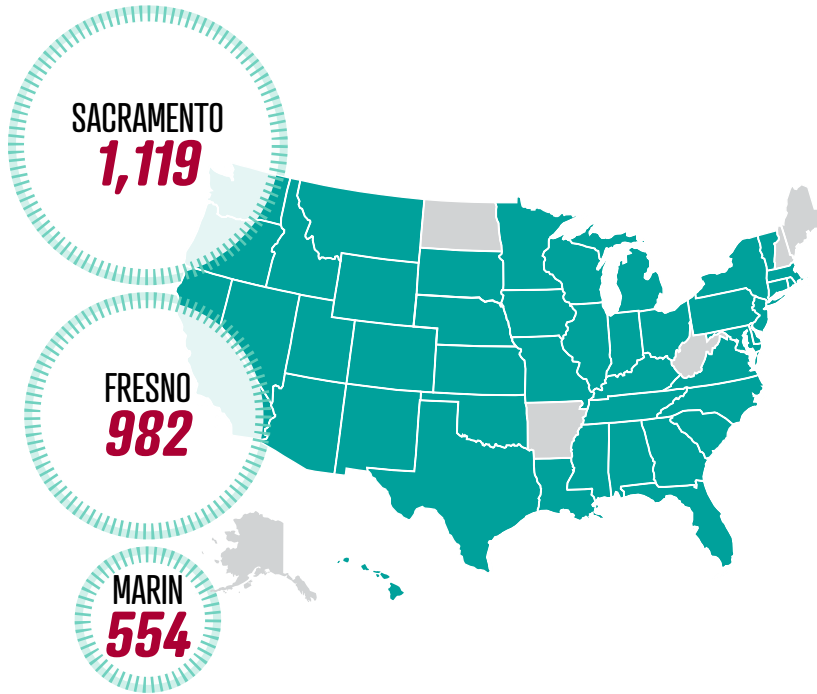
A significant feature of ALPR systems is their ability to share information with users across other organizations. A variety of requirements and guidance exist regarding how law enforcement agencies should share ALPR data, including images. ALPR images contain the date, time, and location of the scanned license plate and largely relate to vehicles that are not linked to crimes. The risk that the images will be misused rises as the images are more widely distributed, and there are numerous examples of law enforcement officers misusing their access to various databases. For example, an Associated Press article from 2016 reported a case from the state of Georgia in which an officer accepted a bribe to search for a woman's license plate number to see whether she was an undercover officer. Although such an example of misconduct is not representative of all law enforcement personnel, it illustrates the need for appropriate safeguards over law enforcement tools. Once a license plate is tied to an individual's identity, which is easy for a law enforcement officer to do, ALPR images may make it possible to track that individual's movements.

State law allows local law enforcement agencies to share ALPR images only with public agencies and requires sharing to be consistent with respect for individuals' privacy. Further, guidance that Justice issued in October 2018 addresses the agencies' governance of databases in relation to immigration enforcement, and this guidance provides a best practice for sharing in general. In the guidance, Justice encourages law enforcement agencies to inquire regarding the purpose for which an agency seeking access to their database intends to use the information and then, as a condition for accessing the database, to require agreements ensuring appropriate use of the data if its purpose includes immigration enforcement. The chiefs' association also recommends that law enforcement agencies maintain ALPR image-sharing records that include information on how the requester intends to use the images. The four agencies we reviewed asserted that they share ALPR images with others on the principle that these entities have a right and need to know the information. Because following state law necessitates establishing an agency's identity, i.e., the right to know, and Justice's guidance suggests establishing the purpose, i.e., the need to know, for which an agency intends to use the images, the agencies' position seems consistent with state law and Justice's guidance.

We could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency.

However, we had difficulty determining whether the reviewed agencies have actually made informed decisions about sharing their ALPR images. Fresno and Marin have each approved sharing their ALPR images with hundreds of entities, and Sacramento with over a thousand. Many of these entities are within California, but they also span most of the other 49 states. Figure 4 shows the entities' locations, illustrating how widely distributed access to these ALPR images is. In addition, we could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency. We reviewed the lists of entities and found one that appeared to be a non-public entity and others that were unidentifiable because they were listed only by initials. For example, Fresno, Marin, and Sacramento all approved an entity listed as the Missouri Police Chiefs Association (Missouri Association); however, this is not a public agency but rather a professional organization that provides training opportunities and advocates for pro-law enforcement legislation. However, none of the agencies could demonstrate that they had evaluated the Missouri Association before sharing images, nor could they tell us why the Missouri Association had a right to those images. When we inquired with Vigilant, an official explained that despite the name, it is the Missouri State Highway Patrol—a law enforcement agency—that uses the account. The lists contain many other entities whose identities and law enforcement purposes are not immediately evident. Unless a law enforcement agency verifies each entity's identity and its right to view the ALPR images, the agency cannot know who is actually using them. Although the three agencies reviewed their sharing arrangements to varying degrees during our audit, none could demonstrate that they perform this kind of verification before sharing their ALPR images.

Figure 4
Three Agencies Have Authorized Sharing With Entities Located in States Across the Nation



Source: Analysis of data-sharing reports from the Vigilant system.

Similarly, even when an entity is a verified public agency, it is not always evident that agencies are making informed decisions by establishing the entity’s need for the ALPR images. Fresno, Marin, and Sacramento all authorized sharing with the Honolulu Police Department, but given the distance between California and Hawaii and the limited instances of cars traveling between the two states, it is uncertain whether the Honolulu Police Department has a persuasive need for these ALPR images. Fresno’s ALPR administrator agreed that not a great deal of thought went into its decision to share with the Honolulu Police Department, and he believes that it probably authorized the share because the entity was a law enforcement agency. In contrast, Marin’s ALPR administrator believes that sharing ALPR images widely is important because the more information available to law enforcement, the more successful it can be in its mission. However, sharing decisions should also consider the importance of protecting individuals’ privacy. Each authorized share exposes the ALPR images to greater risk of misuse; therefore, the agencies should approach each sharing request individually based on the requester’s actual need for the images.

The three agencies have also relied on features in Vigilant's software rather than establishing their own practices for sharing their ALPR images. A sound approach to sharing would include establishing each requesting entity's need to know and right to know and keeping records of the assessment and resulting decision. However, none of these agencies maintain records outside of the Vigilant user interface of when or why they agreed to share with particular entities, and neither Marin nor Sacramento includes a process for approving sharing requests in their ALPR policies as state law requires. Fresno has outlined procedures that incorporate these elements, but it has not followed them. Fresno's ALPR administrator explained that its procedures require more information than an entity requesting a share provides in the Vigilant user interface, and there has been frequent turnover in the position responsible for approving sharing requests.

Current administrators at the three agencies have difficulty understanding when and how sharing occurred because the information the Vigilant user interface displays has changed over time. The status of a sharing relationship in the Vigilant system depends on whether the involved entities' accounts are *active* or *inactive*. Active entities have a current account with Vigilant while inactive entities do not. An agency may agree to share with an active entity that later becomes inactive. Images cannot be shared between active and inactive entities. However, unless an agency deliberately removes a sharing relationship with an inactive entity, that sharing relationship remains and would become operational if an inactive entity decided to renew its account with Vigilant and become active once more. Previously, Vigilant had structured its user interface so that inactive entities did not appear in the sharing report that shows a list of entities with whom an agency had agreed to share. Recently, Vigilant changed its interface to make inactive entities visible. Whether an entity is active is not apparent from the sharing report alone.

A change in the vendor's user interface and not keeping records of authorized shares made it difficult for ALPR administrators to track current sharing relationships.

This change in the user interface and the fact that agencies kept no records of the shares they have authorized made it difficult for ALPR administrators at the agencies to know the status of current sharing relationships. For example, in 2014 a prior ALPR administrator for Marin had agreed to share images with three U.S. Immigration and Customs Enforcement (ICE) agencies. In December 2018, Marin's current ALPR administrator used the Vigilant user interface to review the sharing report and noted that the report included no ICE agencies. However, when he reviewed the report again in August 2019—at our request—three ICE agencies appeared on the list. We discussed this discrepancy with Vigilant, which explained that the three ICE agencies were currently inactive. When Marin's ALPR administrator reviewed the sharing report in December 2018, inactive agencies did not appear on the report, but Vigilant subsequently changed its user interface so that inactive

agencies did appear. Although the ICE agencies could not access Marin's ALPR images because they were inactive, to effectively end the share, Marin needed to remove the authorization for sharing with the ICE agencies, which Marin has since done.

According to Marin's ALPR administrator, it is now the department's position that it will not share images with ICE, but if it had remained unaware that the sharing relationships existed and the ICE agencies had become active again, it would have been sharing its ALPR images with them without knowing it was doing so. Had Marin kept its own records of the sharing to which it had agreed, it would have been aware that it had agreed to share with ICE in the past, and it would have been able to remove those shares promptly. Sacramento had also authorized sharing to ICE agencies in the past. When the current ALPR administrator reviewed the list of entities with which it shared images with in response to our audit, he removed those shares as well. In contrast, Fresno had never authorized any sharing relationship with an ICE agency.

Although none of the agencies using Vigilant currently share with ICE agencies, all three had authorized shares with entities with border patrol duties. Despite not having implemented any agreements related to this sharing since Justice issued its guidance in October 2018, the three agencies were all sharing with the San Diego Sector Border Patrol of U.S. Customs and Border Protection at the start of our audit. During our audit, Sacramento removed the share to this agency. Marin and Sacramento had also authorized sharing with an agency listed as "California Border Patrol," and although Sacramento removed this share at the same time it removed the shares to ICE, Marin continues to share with this entity. Fresno continues to share with the Customs and Border Protection National Targeting Center. Although Sacramento had also authorized a share to this entity, it removed this share during our audit. All of these entities' duties could potentially intersect with immigration enforcement. Justice's guidelines for sharing data are particularly relevant in these cases, yet the agencies were either unaware of these guidelines or had not implemented them for their ALPR systems.

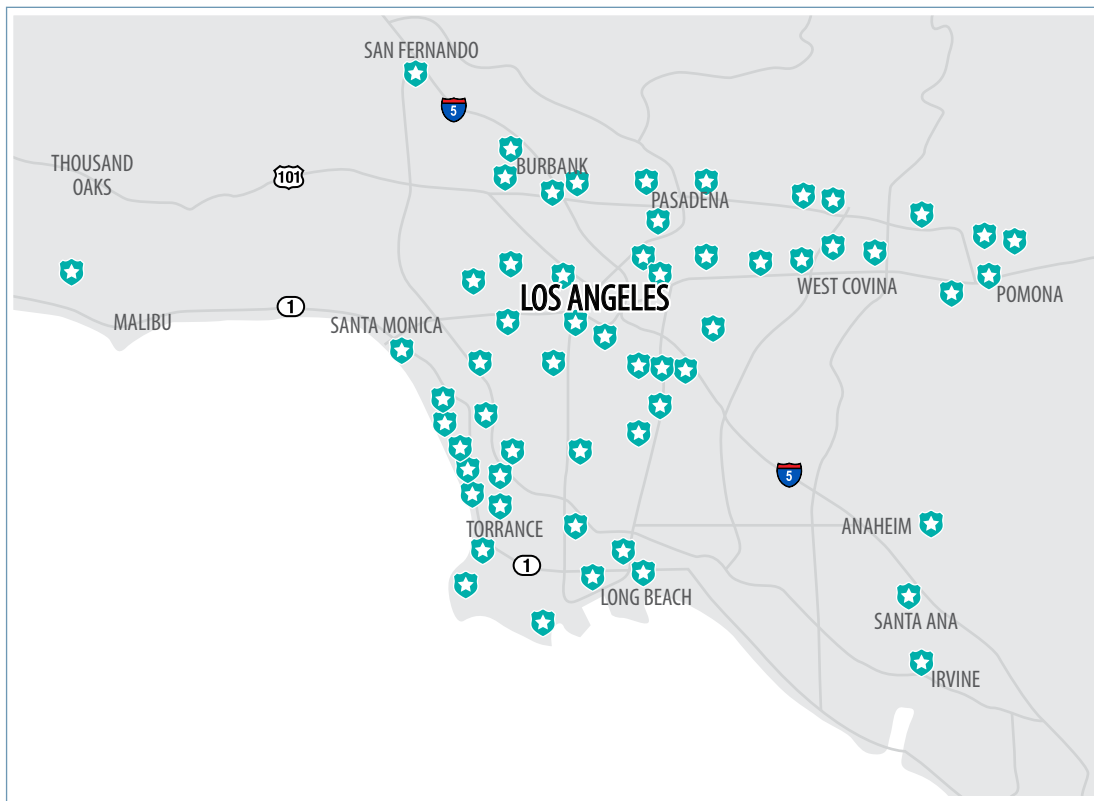
Of the four agencies we reviewed, only Fresno and Sacramento share hot lists they create, and they do so through a more controlled process than for sharing ALPR images. Vigilant's user interface enables hot-list sharing in addition to sharing ALPR images. In contrast to its wide sharing of ALPR images, Fresno shares the hot lists it occasionally uploads with only three law enforcement agencies in the nearby region. Sacramento has agreed to share six hot lists with eight law enforcement agencies in California. With each agency, Sacramento took the additional step of developing a memorandum of understanding providing guidelines for sharing the hot lists and the signature of the chief official at each agency.

Justice's guidelines for sharing data are particularly relevant, yet Fresno, Marin, and Sacramento were either unaware of these guidelines or had not implemented them for their ALPR systems.

Although the memorandum does not specify which hot lists Sacramento will share, it does provide a record of the entities with which hot-list sharing occurred, unlike its sharing of ALPR images for which no independent records exist outside the Vigilant user interface.

In contrast with the other reviewed agencies, Los Angeles has limited its sharing of ALPR images to entities within a regional structure established for its ALPR program through a federal grant that helped fund its ALPR program. As Figure 5 shows, Los Angeles shares ALPR images with 58 other law enforcement agencies in the region. It does not have agreements to share its ALPR images with any federal agencies, including ICE. According to the lieutenant who administers the ALPR program, Los Angeles decided to share images only with entities using the same software so that it could maintain greater control over its ALPR images. It has a formal agreement with each agency, which provides a record of its sharing decisions.

Figure 5
Los Angeles Shares Images With 58 Law Enforcement Agencies



Source: Analysis of data-sharing memorandums of agreement.

The Agencies' Image Retention Decisions Are Unrelated to How They Use the Images

The four agencies we reviewed retain ALPR images for varying periods of time. Our review determined that with the exception of CHP, state law does not mandate a specific retention period for ALPR images collected, accessed, or used by public agencies, nor does state law delineate the factors public agencies should use in determining those periods. Instead, state law requires that public agencies other than CHP that use or operate ALPR systems specify, in the agency's usage and privacy policy, the length of time ALPR data will be retained and the process that the agency will use to determine if and when to destroy retained ALPR data. Fresno's policy is to retain ALPR images for a minimum of one year, Sacramento's policy is to retain ALPR images for a minimum of two years, and Marin's policy is to retain images for two years. Although the agencies' policies describe their retention periods as minimums, in practice the agencies have configured their ALPR systems to delete images older than their specified retention periods. Fresno and Sacramento each download and retain images for longer than their prescribed retention policies if the images are relevant to investigations. Los Angeles does not have an ALPR policy, but the lieutenant who administers the ALPR program stated that it adheres to the city's Administrative Code, which requires data to be retained for a minimum of five years.

None of the agencies considered the images' utility over time when establishing their retention periods. Fresno based its ALPR image retention period on state law, which allows some cities to destroy certain video monitoring records after one year. Marin did not cite state law in its policy; its former ALPR administrator stated that when setting a two-year retention period, he considered other agencies' retention periods and the retention requirements for litigation related to investigations. Both Marin's and Fresno's ALPR administrators stated that they were not aware of any studies of how useful older images in their ALPR systems were to their personnel. In its ALPR policy, Sacramento cited a general state law that prohibits some cities from destroying records less than two years old. The lieutenant who oversees Sacramento's ALPR program acknowledged that the agency has not conducted any statistical analysis to determine how long it needs to retain ALPR images. However, he stated that, although he was not involved in drafting the original policy, two years made sense considering federal regulations, which permit retention of criminal intelligence information for no longer than five years. The lieutenant cited those federal regulations as a best practice for retaining sensitive data, connecting the ALPR images to a tenet of federal regulations that law enforcement agencies should keep criminal intelligence information as long as it is useful, even though ALPR data are not criminal intelligence.

None of the agencies considered the images' utility over time when establishing their retention periods.

To develop a retention policy that better protects individuals' privacy, an agency might begin by considering the time period during which ALPR data are most useful to law enforcement. To assess the usefulness of these images over time, we reviewed the four agencies' ALPR searches over a six-month period—between late January and September 2019, depending on when we visited the agencies—and found that personnel at three of the four agencies typically searched for ALPR images zero to six months old. When searching ALPR systems, investigators can enter search dates to target specific periods of interest. For example, on March 29, 2019, a Sacramento investigator searched for ALPR images from six days earlier—March 23—indicating that images less than one week old were relevant to that search. As Table 2 shows, we found that the searches agency personnel at the three agencies performed infrequently included older images. In fact, when investigators at Fresno, Marin, and Sacramento specified date ranges, most searches were of ALPR images that were less than six months old. In contrast, Los Angeles had a relatively even distribution of searches between those less than one year and those more than one year old. The Vigilant system defaults to showing the 50 most recent records when investigators do not specify a search date range. We analyzed 46,000 records for searches that did not specify a date range and found that investigators for Marin, Fresno, and Sacramento frequently did not seek further than the 50 default records, indicating that they generally were not interested in older ALPR images.

Table 2
The Agencies Usually Search for ALPR Images That Are Six Months Old or Less

	RETENTION PERIOD	TOTAL SEARCHES OVER 6-MONTH PERIOD ANALYZED	PERCENTAGE OF SEARCHES FOR IMAGES OF A SPECIFIED AGE			
			0 TO 6 MONTHS	6+ MONTHS TO 1 YEAR	1+ TO 2 YEARS	MORE THAN 2 YEARS
Fresno*	1 year	850	92%	6%	1%	1%
Los Angeles	5 years	28,874	42	8	29	21
Marin*	2 years	26	88	8	0	4
Sacramento*	2 years	4,262	84	4	11	1

Source: Analysis of search records from the agencies' ALPR systems between late January and September 2019, depending on when we visited the agency.

* The percentage of searches listed in this table beyond an agency's retention period are likely from their personnel searching data belonging to other agencies with longer retention periods.

Other states have established retention periods that are generally shorter than the lengths of time California's local law enforcement agencies are retaining ALPR images. The National Conference of State Legislatures identified at least 13 states that mandate maximum ALPR image retention periods. As the text box shows, these vary widely, from three minutes in New Hampshire to three years in Florida. Nevertheless, the majority of these states have retention periods that do not exceed six months.

In contrast, 230 California agencies responding to our survey reported that they use ALPR systems, and nearly 80 percent of these—180 agencies—stated that they retain their ALPR images for more than six months. About 20 of those agencies indicated that they retain ALPR images for more than five years. Figure A.2 in Appendix A summarizes these responses.

The length of time law enforcement agencies need to retain ALPR images will vary depending on how they use the images. Narrow use—for one purpose only, such as locating stolen cars—could dictate a short retention window. Personnel we interviewed at each of the four agencies stated that investigators rely primarily on recent images to investigate some types of crimes, such as auto theft. In contrast, using ALPR images to solve complex crimes could necessitate a longer retention window. For example, first-degree murder can be prosecuted at any time; therefore, a homicide investigator may be able to use ALPR images of any age to help solve a case. The four agencies we reviewed have access to information they can use to evaluate whether their ALPR retention periods are reasonable. Their systems record each time personnel search ALPR images, and these search records show the date of the search and the parameters used to narrow the search, such as location, date, and time. Agency administrators can analyze these activity logs to understand the images personnel are searching for and their relative ages.

Marin and Sacramento have allowed expired hot lists to remain in their ALPR systems for far longer than their specified retention periods. Unlike ALPR images, hot lists cannot be automatically deleted by the Vigilant system. Instead, the agencies define a period after which the hot list becomes inactive—meaning the ALPR system no longer generates alerts from the list—but the list remains stored in Vigilant’s servers until the agency deletes it. We found that Marin and Sacramento are retaining hot lists longer than necessary because their administrators were unaware of the need to manually delete them. They assumed that their Vigilant system would automatically delete inactive hot lists according to the designated purge schedule, as it does ALPR images. For example, Marin retained an inactive hot list of sex offenders for five years—three years longer than its two-year retention period for ALPR images. Sacramento has retained multiple hot lists for as long as six years—four years longer than its retention period for ALPR images. The types of lists ranged from a hot list of Sacramento County sex offenders to a warrants hot list. When we brought the inactive hot lists to the agencies’ attention,

ALPR Image Retention Periods for 13 States

New Hampshire	3 minutes
Maine	21 days
Minnesota	60 days
Montana	90 days
North Carolina	90 days
Tennessee	90 days
Arkansas	150 days
Nebraska	180 days
----- LONGER THAN SIX MONTHS -----	
Utah	270 days
Colorado	365 days
Vermont	540 days
Georgia	900 days
Florida	3 years

Source: National Conference of State Legislatures, *Automated License Plate Readers: State Statutes*, March 15, 2019, and review of the listed states’ ALPR laws and guidelines.

Note: These states allow retention for longer periods for specific reasons, such as data used in investigations.

the administrators at Marin and Sacramento acknowledged that the age of the hot lists exceeded the agency's retention period, and they were willing to delete the hot lists.

Law enforcement agencies should consider both the usefulness of the ALPR images and individuals' privacy when deciding how long to retain the images. Cost, however, is not a factor. According to the lieutenant who oversees Los Angeles' ALPR program, the images are useful to investigators and the cost of storing ALPR images is not a significant factor in determining how long to store them. Nevertheless, two studies by a consultant to the National Institute of Justice and the chiefs' association concluded that law enforcement agencies must consider the trade-offs between privacy concerns and the utility of retaining the ALPR images they capture and store.

The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts

Instead of ensuring that only authorized users access their ALPR data for appropriate purposes, the agencies we reviewed have made abuse possible by neglecting to institute sufficient monitoring. ALPR systems should be accessible only to employees who need the data and who have been trained in using the system. However, the agencies often neglected to limit ALPR system access, to provide appropriate training to individuals with access, or to monitor accounts. Similarly, to ensure that individuals with access do not misuse the system, the agencies should audit the license plate searches users perform. Instead, the agencies conduct little to no auditing and thus have no assurance that misuse has not occurred.

Best Practice Safeguards for Establishing and Managing User Accounts

Account Setup

- Supervisor approval is a prerequisite for account access.
- ALPR training is a prerequisite for account access.

Account Maintenance

- Accounts defined as *inactive* are suspended.
- ALPR training is required for users linked to inactive accounts to regain active status.
- Accounts are deleted when employees separate from the agency.

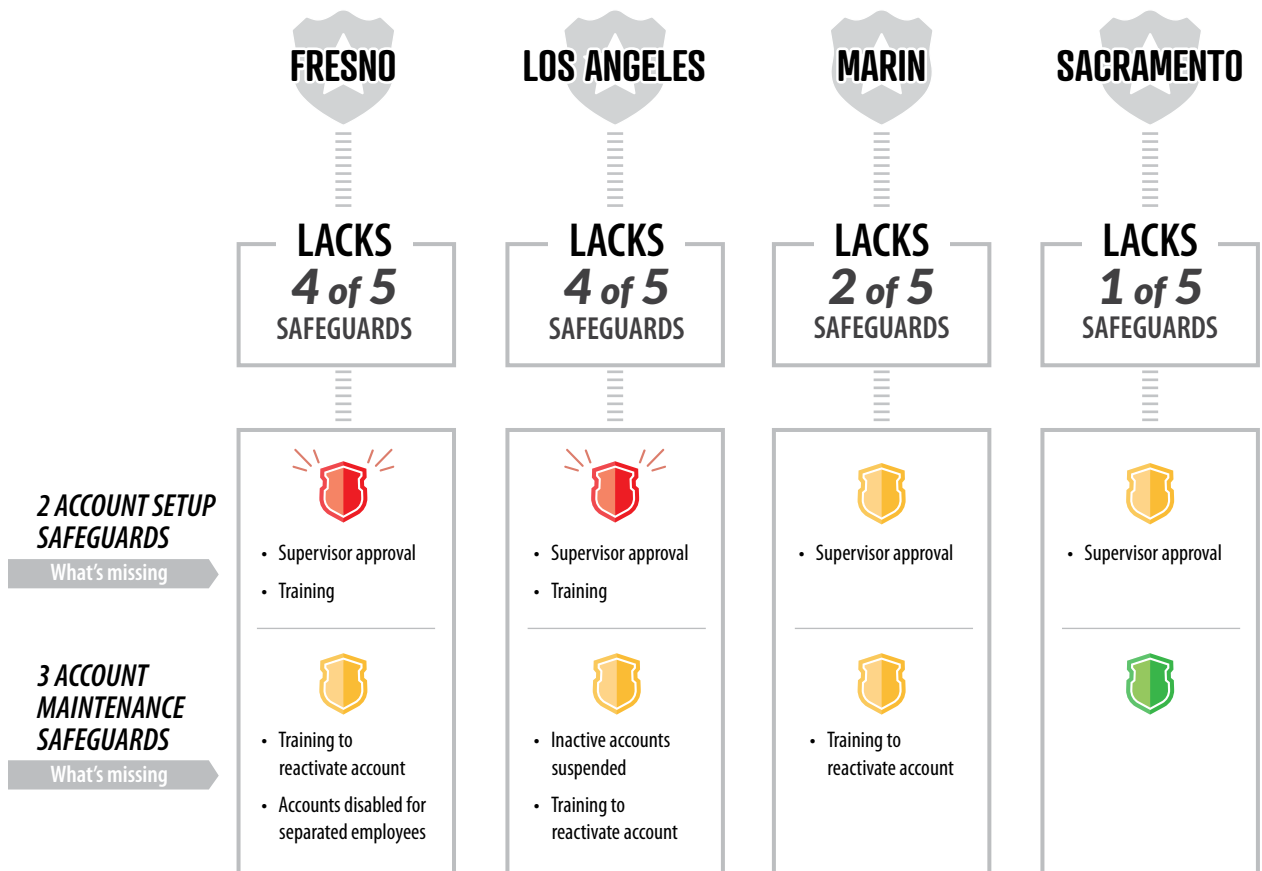
Source: CJIS policy and the *State Administrative Manual*.

The Agencies Need Stronger User-Access Safeguards

The four agencies we reviewed all failed to follow one or more best practices related to user access. State law requires agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, and the text box lists five best practices for user access, from initiating an account to disabling it when an employee separates from the agency. Figure 6 shows the four agencies' status in implementing these best practices. Each ALPR administrator stressed the concept of "need to know, right to know" as a key for data security; however, no agency followed all of the best practices that would help establish the need to know and right to know. For example, no agency had a requirement

that supervisors approve staff requests for creating ALPR user accounts. Such a step would provide assurance that the staff member receiving the account had both a need and a right to access the information in the ALPR system. Los Angeles is particularly lax in this area because the protocol of its IT division is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system nevertheless have access to the system. In contrast, Sacramento follows all but one of the best practices listed in the text box. In doing so, it requires staff to prove their initial and continued need for ALPR data, among other access requirements.

Figure 6
The Agencies Lack Many Best Practice Safeguards for Establishing and Managing User Accounts



Source: Agencies' policies, applicable procedures and protocols, and interviews with the agencies' management.

Agencies could reduce instances of unnecessary access by ensuring that only those staff whose current work assignments require access to ALPR data have that access. The ALPR administrators at Marin and Los Angeles believe that supervisory approval is unnecessary

Limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

because ALPR users are already privy to data they consider more confidential than ALPR data, such as criminal justice information. However, these views do not consider that ALPR systems capture images indiscriminately, irrespective of the criminal history of the individual who is driving the vehicle, and the images allow law enforcement to track individuals. Given that agencies retain these images for several months or years, a user could combine them with personal information from separate data sources to produce a great number of details about someone's life, such as his or her political or religious affiliation. Without proper safeguards, staff could conduct this form of surveillance on any driver. In fact, the chiefs' association acknowledged this possibility and warned that increasing ALPR use and data sharing would enhance the potential for surveillance. Thus, as the chiefs' association concluded, limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

Ensuring that ALPR users are properly trained is another weakness among the agencies we reviewed. Three of the agencies do not ensure that all of their ALPR users are properly trained. The chiefs' association called the training of authorized ALPR users "a critical accountability measure." However, as Figure 6 shows, neither Fresno nor Los Angeles requires all ALPR users to complete ALPR training before initially obtaining system access. Although Los Angeles offers ALPR training, the detective who conducts this training confirmed that it is not required before users can access the ALPR system. Fresno's policy encourages such training; however, its ALPR administrator confirmed that the agency does not provide training to all of its users. Further, Marin's ALPR administrator stated that although Marin provides training when staff first receive access to the ALPR system, it does not require staff to renew their training in order to reactivate their accounts following long periods of not using the system. Without sufficient training, there is little assurance that ALPR users know and understand agency ALPR policies, including recent changes, or are aware of the limits on how they may use ALPR data.

Although the Fresno ALPR administrator agrees that the agency's safeguards surrounding user access are currently inadequate and plans to improve them, the ALPR administrators at Los Angeles, Marin, and Sacramento believe their current practices are acceptable. The administrators at Marin and Los Angeles are reluctant to alter their agencies' existing practices because they believe ALPR data are not as sensitive as other law enforcement data. We disagree with these views because, as we mention previously, ALPR data are sensitive and state laws require reasonable security procedures and practices to protect them. A basic protection for data that must be treated as sensitive is to limit who can access them.

In addition, as we mention earlier, the ALPR images law enforcement agencies collect largely involve vehicles that are not associated with crimes, and if the images were analyzed, the data could reveal behavior patterns and preferences that law enforcement could use to conduct surveillance on individuals. For example, according to a 2012 newspaper article, the New York Police Department collected license plate numbers of vehicles parked near a mosque. The department was purportedly trying to identify terrorist activities. Although the department justified this data collection as part of its strategy to identify potential criminal activities, it targeted mosques and collected license plate numbers at times without any leads or proof of terrorist connections. Given the sensitivity of the information collected in this example, access safeguards would ensure that only those staff who have a need and right to access an ALPR system would possess that privilege.

Law enforcement agencies could further improve safeguards by disabling employees' accounts once they separate or after long periods of nonuse. We reviewed Marin's and Sacramento's processes for disabling accounts of separated employees. Both agencies follow a similar approach, relying on one part of the organization providing information to another. Sacramento produces a personnel transfer and separation list every two weeks, and the IT security group uses it to identify accounts to close. Although the IT security group generally disabled accounts promptly after receiving the list, we found that the contents of the list were not always current. For example, in one instance, a separated employee did not appear on the list until 46 days after his separation date in June 2019. According to a human resources specialist, employees submit their resignation paperwork late at times, which causes human resources to not process this paperwork until after an employee has left the department. Marin's ALPR administrator said that he removes ALPR accounts once he receives a department-wide email notifying him of an employee's resignation or termination. He also stated that he checks ALPR accounts every few months to verify that active accounts match active employees. However, for one employee, the administrator did not disable his ALPR access until two months after he resigned in October 2019. In fact, the administrator did not disable this employee's access until our office pointed out that the account was still active. The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

With regard to Los Angeles and Fresno, Los Angeles' network manager described an automated process for deleting accounts linked to overall network access, which reasonably aligned with best practices. Conversely, Fresno's ALPR administrator said that

The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

he periodically reviews the names of employees with user accounts but started doing so only in September 2019 when he learned of our audit. We did not test deleted accounts at either agency. Deleting accounts prevents separated employees from continuing to access ALPR data and is thus critical to protecting ALPR data and individuals' privacy.

The Agencies Have Failed to Audit ALPR Users' Searches to Ensure That Individuals' Privacy Is Protected

State law requires law enforcement agencies that operate, access, or use ALPR systems to protect their ALPR data—including ALPR images—from unauthorized access, destruction, use, modification, or disclosure. The law specifically requires them to describe and implement a policy detailing how they will monitor their ALPR systems. According to state law, agencies that access or use ALPR systems must also conduct periodic system audits. In its reports on managing ALPR systems, the chiefs' association stated that conducting audits aids in discouraging unnecessary or inappropriate use of the data; in addition, when agency policies include a strong auditing requirement, this reassures the public that their privacy interests are recognized and respected.

A primary form of auditing to prevent misuse is reviewing the searches users conduct in the ALPR systems. Users conduct searches for specific license plates. Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, such as an unknown user account, they should also conduct audits as required by state law. An audit entails a more rigorous approach, including evaluating risk and randomly selecting test items for review. Developing an audit of license plate searches, for example, would involve determining how many searches to review, how to select test items, and how frequently to conduct the audit. Law enforcement agencies have often found evidence of misuse of their databases, showing the need for auditing. For example, a news article reported that CHP investigated 11 cases of database misuse in 2018, including three involving officers improperly looking up information on license plates through CLETS without a need to know the information. The large datasets of ALPR images, dating back at least one year, that the four reviewed agencies maintain can be analyzed to reveal the daily patterns of vehicles that can be linked to individuals and their activities—most of whom have not engaged in criminal activity. A member of law enforcement could misuse ALPR images to stalk an individual or observe vehicles at particular locations and events, such as doctors' offices or clinics and political rallies. Despite these risks, the agencies we reviewed conduct little to no auditing of users' searches.

Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, they should also conduct audits as required by state law.

We asked key officials at the three agencies using the Vigilant system why they had not audited the searches users performed and found that either they were unaware of the auditing requirement in state law or the auditing they did conduct did not include user searches. Fresno's policy states that it should conduct audits on a regular basis, but the ALPR administrator told us he believed audits are the responsibility of the Audits and Inspections Division within the department. However, the sergeant responsible for audits and inspections—who took charge in January 2018—responded that he was not aware of the requirement until our audit. Similarly, the Marin ALPR administrator was unaware of the state law requiring audits of ALPR systems until our audit and thus had not been conducting them. At Sacramento, the policy states that the ALPR administrator will conduct periodic audits of user searches. Even though Sacramento administrators had been monitoring some system functions, they had not audited searches of the older ALPR images. The officer administering the ALPR program until April 2019 said that she did not conduct these audits because her predecessor had not informed her that it was necessary. The ALPR program transferred to a new division in April, and according to the current ALPR administrator, limited staff resources have prevented him from instituting these audits.

Although the agencies have not been conducting audits, we considered the possibility that an agency employee or member of the public may have reported instances of ALPR misuse. We searched each agency's records of internal affairs investigations from January 1, 2016, to the present for cases involving ALPR misuse and did not find any such cases. However, we do not consider this proof that no instances of ALPR misuse occurred. Given that the agencies were not regularly auditing their systems, ALPR misuse may have occurred and gone unnoticed and unreported.

To engage in meaningful auditing of their system users, all four agencies need to address the quality of the information users enter into the system as part of their searches. Before allowing users to conduct searches, Fresno, Los Angeles, and Marin require users to enter case numbers and reasons for the search; however, this is not happening consistently. We reviewed six months of user queries at the three agencies and found that users entered a wide variety of information in the case number field. For example, users at Los Angeles simply entered "investigation" into this field as well as descriptions of vehicles and actual case numbers. In contrast, Sacramento does not require users to enter either case numbers or reasons. Our review showed that in 66 percent of searches, Sacramento's users left both fields blank. When users fail to enter any information or fail to include appropriate detail, identifying misuse through audits becomes nearly impossible.

All four agencies must address the quality of information they will need to audit user searches. In Sacramento, for 66 percent of searches, users left case number and search reason fields blank.

Los Angeles faces additional hurdles in performing meaningful auditing because its ALPR administrators do not have immediate access to data on user searches. Instead, according to the chief data officer, administrators need to request that a software engineer from Los Angeles' ALPR software contractor build and run a query in the system to obtain these data. In 2015 Los Angeles recognized a need to fix this software limitation to enable administrators to audit user searches. The chief data officer for Los Angeles stated that, although an initial upgrade provided an audit dashboard tool for administrators, subsequent software upgrades made this tool unusable, and the company that provides the software is developing a new one. He said that it is Los Angeles' goal to have a new audit dashboard tool by the end of the first quarter of 2020, at which point he will work with the appropriate division within the department to develop an audit plan. Although we agree that an audit tool will facilitate audits, we believe it was entirely possible for Los Angeles to obtain the data on user searches, and thus it could have implemented a process for periodic system audits as state law requires, despite the difficulties.

Fresno, Marin, and Sacramento do not have adequate policies or processes in place for conducting meaningful audits.

The other three agencies also do not have an adequate policy or process in place for conducting meaningful audits. For example, Fresno's ALPR policy states that it should conduct periodic audits, but its policy does not specify how frequently it will audit its ALPR system, who will perform those audits, who will review and approve the audit results, and how long it will retain the audit documents. Specifics such as these provide a clear road map for planning, conducting, documenting, and resolving audits. When followed, the agencies will have records demonstrating their necessary oversight. Marin's latest policy—dated July 2019—also fails to cover these necessary details. Fresno and Marin began reviewing user queries subsequent to the beginning of our audit, but in the absence of an adequate policy or formal plan, their methodologies are lacking. For example, although Fresno began conducting audits that included a random sample of user searches, staff have not developed a formal plan and provided us only with handwritten notes on their methodology. Marin's ALPR administrator has not instituted audits and is simply monitoring license plate searches by looking for instances in which the user did not enter a reason for the search or entered a reason that does not make sense, such as an investigation that does not exist. In addition, at both Fresno and Marin, the individual conducting the audits or monitoring is also a system user, creating a conflict when acting as a system monitor or auditor. Without sound methodologies, the agencies cannot be confident that they have sufficient protocols in place to detect misuse.

Other Areas We Reviewed

To address all the audit objectives approved by the Joint Legislative Audit Committee (Audit Committee), we reviewed two additional subject areas: whether the agencies offered opportunities for the public to comment on their ALPR programs and whether the Sacramento County Department of Human Assistance (Human Assistance) continues to operate an ALPR program.

Three Agencies Provided Information to the Public on Their ALPR Programs

State law requires that public agencies implementing ALPR programs after January 1, 2016, offer an opportunity for the public to comment about those programs. These opportunities increase public awareness that law enforcement agencies are using electronic means to collect information about vehicles in the community and offer a way for the public to provide feedback about the programs. The four agencies we reviewed began using ALPR before 2016 and consequently were not required to offer an opportunity for public comments. Nonetheless, three of the agencies took some steps to communicate with the public about their ALPR programs. Los Angeles and Sacramento published documents describing their ALPR programs, and at a Fresno City Council meeting, the public had an opportunity to comment on the selected ALPR vendor before the council voted on a new contract. The minutes from that meeting reflect that the public made no comments. This transparency helps foster public trust in law enforcement and government as a whole.

Human Assistance No Longer Operates an ALPR Program

Our audit scope included reviewing the ALPR program of Human Assistance, which provides Sacramento County residents with employment assistance and supportive services. Human Assistance contracted with Vigilant for three years to access ALPR images. Human Assistance did not operate its own cameras, and it used the ALPR images to investigate welfare fraud. According to the administrator of its ALPR program, Human Assistance ended its program in 2018 after determining that investigative staff rarely searched the images, so the program could not justify the cost. On November 1, 2018, Human Assistance deleted its ALPR user accounts, leaving the administrator's account active for internal review. On May 31, 2019, Human Assistance's ALPR agreement with Vigilant expired, and the administrator no longer has access to the account. Therefore, we did not perform any additional audit work pertaining to Human Assistance.

Recommendations

Legislature

- To better protect individual's privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:
 - Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.
 - Require 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 systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
 - Establish a maximum data retention period for ALPR images. The Legislature should also establish a maximum data retention period for data or lists, such as hot lists, that are used to link persons of interest with license plate images.
 - Require periodic evaluation of a retention period for ALPR images to ensure that the period is as short as practicable.
 - Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.
 - Specify that those with access to ALPR systems must receive data privacy and data security training. The Legislature should require law enforcement agencies to include training on the appropriateness of including certain data in an ALPR system, such as data from CLETS.

Law Enforcement Agencies

- To ensure that their ALPR policies contain all of the required elements as specified in state law, by August 2020, Fresno, Los Angeles, Marin, and Sacramento should review their policies and draft or revise them as necessary. Also by August 2020 these agencies should post their revised policies on their websites in accordance with state law.

- To protect ALPR data to the appropriate standard, Fresno, Los Angeles, Marin, and Sacramento should do the following:
 - By August 2020, identify the types of data in their ALPR systems and, as they review or draft their ALPR policies, ensure that they clarify the types of information their officers may upload into their ALPR systems, such as, but not limited to, information obtained through CLETS.
 - By August 2020, perform an assessment of their ALPR systems' data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.
- To ensure that the agreements with their cloud vendor offers the strongest possible data protections, by August 2020, Fresno, Marin, and Sacramento should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy.
- To ensure that ALPR images are being shared appropriately, the specific agencies noted should do the following:
 - By April 2020, Fresno, Marin, and Sacramento should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.
 - As Los Angeles develops its ALPR policy, it should be certain to list the entities with which it will share ALPR images and the process for handling image-sharing requests.
 - By August 2020, Marin and Sacramento should each develop a process for handling ALPR image-sharing requests that includes maintaining records separate from the Vigilant system of when and with whom they share images. The process should verify a requesting agency's law enforcement purpose for obtaining the images and consider the requesting agency's need for the images. The process should be documented in the agency's ALPR policy and/or procedures.
 - By August 2020, Fresno should revise its written procedures for ALPR image-sharing, as necessary, to ensure that it follows those procedures.

- To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno, Los Angeles, Marin, and Sacramento should do the following:
 - By August 2020, review the age of the ALPR images their personnel are searching for and ensure that their retention periods for ALPR images are based on department needs. Each agency should reflect in its ALPR policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.
 - Include in their ALPR policies a retention period for data or lists, such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.
- To ensure that ALPR system access is limited to agency staff who have a need and a right to use ALPR data, Fresno, Los Angeles, Marin, and Sacramento should do the following:
 - By April 2020, review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.
 - Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.
 - By August 2020, develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that supervisors must approve accounts for users, providing training to users before granting accounts, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously inactive accounts. Each agency should also ensure that it has procedures in place to deactivate an account immediately for an account holder who separates from the agency or who no longer needs a user account.

- To enable auditing of user access and user queries of ALPR images, Fresno, Los Angeles, Marin, and Sacramento should do the following:
 - By April 2020, assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.
 - Ensure that their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. Each agency should have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.
 - By June 2021, implement their audit plans and complete their first audits.

We conducted this performance audit under the authority vested in the California State Auditor by Government Code 8543 et seq. and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,



ELAINE M. HOWLE, CPA
California State Auditor

February 13, 2020

Blank page inserted for reproduction purposes only.

Appendix A

Summary of ALPR Survey Responses

The Audit Committee requested that we determine ALPR use among law enforcement agencies statewide. Specifically, the Audit Committee asked us to determine whether agencies use ALPR information, what vendors they use, and whether law enforcement agencies have policies and procedures to govern their use and sharing of ALPR information. We surveyed 391 county sheriffs and municipal police departments statewide. We relied upon information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI to obtain assurance that our list of statewide local law enforcement was reasonably comprehensive.

We received 381 responses (97 percent) to the 391 surveys we sent. Ten agencies we surveyed did not respond. The text box lists those agencies. A breakdown of the law enforcement agencies' responses to our statewide survey can be found at <http://auditor.ca.gov/reports/2019-118/supplemental.html>. The discussion here summarizes the survey results.

Agencies That Did Not Respond to Our Survey

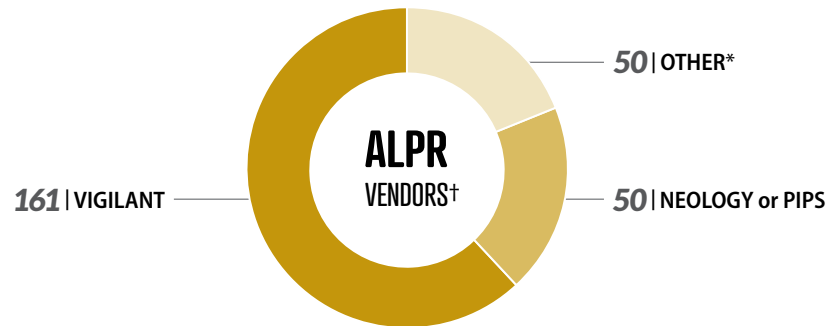
- Anderson Police Department
- Barstow Police Department
- Del Norte County Sheriff's Office
- Lakeport Police Department
- Lodi Police Department
- Mendocino County Sheriff's Office
- Mount Shasta Police Department
- Oceanside Police Department
- San Francisco Sheriff's Department
- Siskiyou County Sheriff's Department

Source: Analysis of survey responses.

Summary of Results From Agencies That Reported Using ALPR Systems

In responding to our survey, law enforcement agencies indicated whether they use ALPR systems and, if so, what vendors' systems they use to collect and access ALPR information. Of the agencies that responded, 60 percent, or 230 agencies, reported that they currently operate or access information from ALPR systems. Of those agencies, 96 percent said they have an ALPR usage and privacy policy. Vigilant is the most common vendor for the agencies that reported using ALPR systems. Figure A.1 summarizes which vendors the 230 law enforcement agencies reported that they use. Finally, 9 percent, or 36 of the agencies we surveyed, stated that they are implementing or planning to implement ALPR systems.

Figure A.1
Vigilant Is the ALPR Vendor the Majority of Law Enforcement Agencies Use



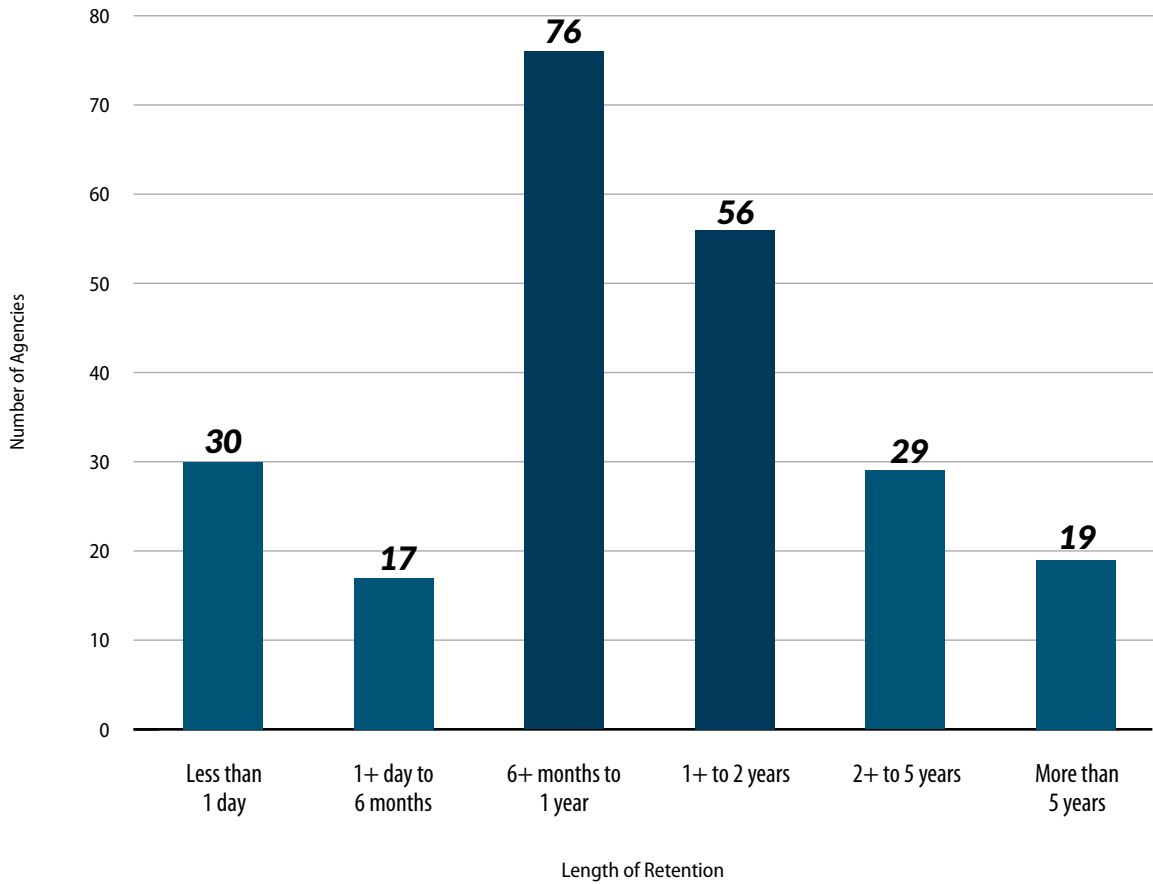
Source: Analysis of survey responses.

* The *Other* category includes vendors such as Genetec, ELSAG, and All Traffic Solutions.

† The total number of ALPR vendors used is greater than the 230 agencies that said they use ALPR systems because some agencies use more than one vendor.

Law enforcement agencies that reported using ALPR systems also answered questions related to their retention and sharing of ALPR information. We asked how long the agencies retain ALPR information not related to ongoing investigations or litigation. As Figure A.2 shows, the retention periods varied, but the majority of law enforcement agencies reported retention periods between six months and two years. Additionally, we asked agencies that operate ALPR systems if they share or sell the information they collect with other law enforcement or public agencies. Seventy-three percent, or 168 agencies that use ALPR systems, reported that they share ALPR images with other law enforcement agencies; only three of those agencies also reported that they share ALPR images with other public agencies that are not law enforcement. None of the agencies we surveyed reported selling images to other law enforcement or public agencies.

Figure A.2
A Majority of Agencies Generally Retain ALPR Information for Between Six Months and Two Years



Source: Analysis of survey responses.

Note: Three responding agencies that use ALPR systems did not indicate a retention period for their information: Bakersfield Police Department, Fountain Valley Police Department, and Pasadena Police Department.

Blank page inserted for reproduction purposes only.

Appendix B

Scope and Methodology

The Audit Committee directed the California State Auditor to conduct an audit of the extent to which local law enforcement agencies are complying with existing law regarding the use of ALPR systems. The analysis the Audit Committee approved contained five objectives. We list the objectives and the methods we used to address them in Table B.

Table B
Audit Objectives and the Methods Used to Address Them

AUDIT OBJECTIVE	METHOD
1 Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant state laws, regulations, and other background materials applicable to the use and operation of ALPR systems by local law enforcement.
2 To the extent possible, determine the following for law enforcement agencies statewide: <ul style="list-style-type: none"> <li data-bbox="337 1020 740 1100">a. Whether they use ALPR information and, if so, what vendors they use to access this information. <li data-bbox="337 1100 740 1180">b. Whether they have policies and procedures in place governing the use and sharing of ALPR information. 	<ul style="list-style-type: none"> <li data-bbox="764 953 1508 982">• Surveyed 391 county sheriff and municipal police departments statewide. <li data-bbox="764 999 1508 1079">• Obtained and verified a list of statewide local law enforcement agencies, using information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI. <li data-bbox="764 1096 1508 1306">• Questioned agencies regarding their use of ALPR systems, including whether they use or are planning to use an ALPR system; if they share or sell the ALPR information; if their ALPR storage is CJIS-compliant; which system they use to store, share, or access ALPR information; if they have a usage and privacy policy and post the policy on their website; how long they retain ALPR information; how many department personnel have access to the ALPR data; and how many total personnel their department has. Full questions and a breakdown of the responses are on our website at http://auditor.ca.gov/reports/2019-118/surveys.html. <li data-bbox="764 1323 1508 1373">• Created an interactive graphic to display responses by county, assembly district, and senate district at http://auditor.ca.gov/reports/2019-118/supplemental.html. <li data-bbox="764 1390 1508 1419">• The survey responses were self-reported, and we did not verify their accuracy.

continued on next page ...

AUDIT OBJECTIVE	METHOD
<p>3 Examine the use of ALPRs by the Sacramento County Sheriff's Office and Department of Human Assistance, the Los Angeles Police Department, the Fresno Police Department, and the Marin County Sheriff's Office by performing the following:</p>	
<p>a. Determine whether they have policies and procedures in place regarding ALPR systems and whether those policies contain the elements state law requires.</p>	<ul style="list-style-type: none"> • Interviewed the agencies' ALPR administrators. • Obtained and reviewed ALPR policies and procedures and determined whether each agency met state law requirements in this area.
<p>b. Determine whether they have followed state law regarding all required public notifications related to ALPR systems and information, including required public hearings.</p>	<ul style="list-style-type: none"> • Interviewed the agencies' public information officers. • Obtained evidence of public notifications and public hearings and determined whether each agency met state requirements in this area.
<p>c. Determine whether they maintain records of access to ALPR information from both within and outside the agency that includes all required documentation and whether they have ensured that ALPR information has only been used for authorized purposes.</p>	<ul style="list-style-type: none"> • Interviewed the agencies' ALPR administrators. • Reviewed access records from the agencies' ALPR systems. • Determined whether the agencies conducted any audits or monitoring by interviewing ALPR administrators, staff of internal audit divisions, and executive staff of any oversight entities. We also reviewed relevant policies and procedures. • Reviewed the agencies' internal affairs files for any cases involving ALPR misuse. • Reviewed Justice's and the FBI's audits of the agencies' IT security and the safeguards those audits identified.
<p>d. Determine whether they have sold, shared, or transferred ALPR information only to other public agencies, except as otherwise permitted by law, and whether they have properly documented these activities.</p>	<ul style="list-style-type: none"> • Interviewed the agencies' ALPR administrators. • Reviewed reports and records about data sharing from the agencies' ALPR systems. • Reviewed existing memorandums of agreement and understanding for data sharing. • Interviewed executive staff at Vigilant regarding ALPR system functionality and their procedures for verifying the law enforcement purpose of client agencies.
<p>e. Determine the nature of any contracts with third-party vendors related to ALPR information.</p>	<ul style="list-style-type: none"> • Interviewed Justice staff responsible for protecting criminal justice information. • Evaluated the agencies' contracts with third-party vendors and determined whether the contracts contained adequate protections for information in the agencies' ALPR systems.
<p>4 Evaluate whether current state law governing ALPR programs can be enhanced to further protect the privacy and civil liberties of California residents.</p>	<ul style="list-style-type: none"> • Interviewed agencies' investigators and ALPR program administrators. • Reviewed the information in the agencies' ALPR systems and identified the necessary protections for that information. • Obtained the agencies' justifications for their ALPR data retention periods. • Analyzed six months of the agencies' ALPR search records— between late January and September 2019, depending on when we visited the agencies—to determine how often the agencies' personnel searched for older data in their ALPR systems. • Reviewed other states' ALPR data retention laws based on a report from the National Conference of State Legislatures and identified best practices for data retention. • Analyzed laws pertaining to privacy, personal information, and criminal justice information and determined whether changes to current ALPR law would further protect the privacy and civil liberties of California residents.
<p>5 Review and assess any other issues that are significant to the audit.</p>	<p>Reviewed informational material produced by law enforcement agencies, nonprofit organizations, and other entities to identify concerns surrounding privacy and ALPR systems.</p>

Source: Analysis of state law, policies, information, and documentation identified in the table column titled Method.

Assessment of Data Reliability

The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information that we use to support our findings, conclusions, and recommendations. In performing this audit, we relied on electronic data files we obtained from Fresno, Los Angeles, Marin, and Sacramento. These files included reports from the agencies' ALPR systems. Because the agencies relied on remote third-party systems to produce the reports, our analysis of these reports was limited to verifying that we had received the information we requested. We did so by reviewing source materials such as user manuals, interviewing vendor staff, and confirming with the agency staff that the number of records in the files we received were correct. We also used electronic lists from the California Police Chiefs Association and the California State Sheriffs' Association to compile a list of statewide police and sheriff departments for our survey. We verified the nature of the data with the associations' staffs, and we also verified record counts by comparing the provided lists with FBI crime-reporting data. We found the data to be sufficiently reliable for our purposes.

Blank page inserted for reproduction purposes only.

February 2020

XAVIER BECERRA
Attorney General

State of California
DEPARTMENT OF JUSTICE



1300 I STREET
SACRAMENTO, CA 95815-4524
Public: (916) 210-5000
Fax (916) 227-3079
Email: Joe.Dominic@doj.ca.gov

January 28, 2020

Elaine Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814


Re: Draft Audit Report - California State Auditor Report 2019-118; Automated License Plate Readers (ALPR)

Dear Ms. Howle:

The Department of Justice (DOJ) appreciates the opportunity to review the above-mentioned draft audit report. DOJ currently has no program in place to provide policy template and guidance to law enforcement agencies for their ALPR programs. Express authority from the Legislature and funding are needed to implement the recommendations.

If you have any questions or concerns regarding this matter, you may contact me at the telephone number listed above.

Sincerely,


Joe Dominic, Chief
California Justice Information Services Division

For **XAVIER BECERRA**
Attorney General

cc: Sean McCluskie, Chief Deputy to the Attorney General
Edward Medrano, Chief, Division of Law Enforcement
Chris Prasad, CPA, Director, Office of Program Oversight and Accountability

Blank page inserted for reproduction purposes only.

February 2020



Mariposa Mall
 P.O. Box 1271
 Fresno, CA 93715-1271

January 27, 2020

ANDREW J. HALL

Chief of Police



Elaine Howle
 California State Auditor
 621 Capitol Mall, Suite 1200
 Sacramento, CA 95814

Dear Ms. Howle:

On behalf of the men and women of the Fresno Police Department, allow me the opportunity to thank you and your team for the time and effort in completing the Automated License Plate Reader (ALPR) audit at the request of the Joint Legislative Audit Committee. The Fresno Police Department always strives to ensure we maintain excellence and utilize best practices in all facets of service to the community especially concerning personal privacy. Building trust in the community is paramount to our agency as we continue our on-going efforts to be a model community policing agency. We will utilize this audit to ensure those goals are achieved.

The following are the Fresno Police Department's response to the audit recommendations included in the report.

1. *"To ensure that agency ALPR policies contain all of the required elements as specified in state law, by August 2020 Fresno should review their ALPR policies and draft or revise them as necessary. Also by August 2020 post their revised policies on their websites in accordance with state law:*

The Fresno Police Department has already begun reviewing and updating our ALPR policy. In fact, it is nearly complete and will be completed well in advance of the August 2020 recommended timeline.

2. *"To protect ALPR data to the appropriate standard, Fresno should do the following:"*
 - a. *By August 2020 identify the types of data in their ALPR systems, and as they review or draft their policies, ensure that they clarify the types of information their officers may upload into their ALPR systems such as, but not limited to information obtained through CLETS."*

As the audit showed, the Fresno Police Department has not entered personal data into the ALPR system; however we will continue to review data and incorporate into policy the parameters for types of data which can be entered.

- b. *By April 2020 perform an assessment of their ALPR systems data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.*

Safety, Service, Trust

Fresno Police Department
ALPR Audit Response
January 23, 2020
Page 2

The Fresno Police Department IT Manager will assess the ALPR system and ensure it is in compliance with CJIS Security Policy best practices.

3. *“To ensure that the agreement with their cloud vendor offers the strongest possible data protections, by August 2020 Fresno should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy.”*

The Fresno Police Department IT Manager will review the Vigilant contract and ensure the contract is updated and in compliance with CJIS Security policy.

4. *To ensure that ALPR images are being shared appropriately:*
 - a. *By April 2020 Fresno should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.*

The Fresno Police Department has suspended most sharing and now only shares images with bordering states.

- b. *By August 2020 Fresno should revise its written procedures for ALPR image sharing, as necessary, to ensure that it follows these procedures.*

The Fresno Police Department will incorporate these changes into the updated policy.

5. To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno should do the following:
 - a. *By August 2020 review the age of the ALPR images their personnel are searching for and ensure their retention periods for ALPR images are based on department needs. {REDACTED} reflect in its ALPR policy the updated retention period in its policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.*

Based on the results of the audit, the Fresno Police Department will amend our current practice of retaining images for one year to six months which is consistent with the time frame the majority of the searches occur.

- b. *Include in their ALPR policies a retention period for data or lists such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.*

The Fresno Police Department will maintain active hot lists for 90 days. If an investigator requires a longer period, approval will be obtained from a commander. This will be incorporated in the revised ALPR policy.

Fresno Police Department
ALPR Audit Response
January 23, 2020
Page 3

6. To enable monitoring of user access and user queries of ALPR images, Fresno should do the following:
 - a. *By April 2020 assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.*

This is already being done and is part of the quarterly audit process.

- b. *Ensure their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. [REDACTED] have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.*

A quarterly audit process has been put in place. The audit process, methodology and responsibilities will be included in the updated ALPR policy.

- c. *By June 2021 implement their audit plans and complete their first audits.*

The audit process is already in place and audits were completed for the last two quarters of 2019.

7. To ensure that ALPR access is limited to agency staff who have a right and a need to use ALPR data, Fresno [REDACTED] should do the following:
 - a. *By April 2020 review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.*

This has been completed. Separated employees are removed upon notification of their separation. The ALPR system automatically deactivates accounts for users who have been inactive for 365 days.

- b. *Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.*

This will be incorporated into the revised ALPR Policy. Access will be granted on a need to know and right to know basis for sworn department members and crime specialists who have investigative responsibility.

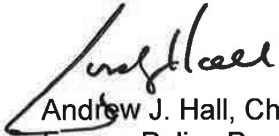
- c. *By August 2020 develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that a supervisor must approve an account for a user, providing training to users before granting an account, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously*

Fresno Police Department
ALPR Audit Response
January 23, 2020
Page 4

inactive accounts. [REDACTED] ensure that it has procedures in place to deactivate accounts immediately for account holders who separate from the agency or who no longer need a user account.

The Fresno Police Department will incorporate supervisor approval for new accounts and minimum training requirements for new users in the revised policy.

Sincerely,



Andrew J. Hall, Chief of Police
Fresno Police Department

AJH: rb

February 2020

LOS ANGELES POLICE DEPARTMENT



MICHEL MOORE
Chief of Police

ERIC GARCETTI
Mayor

P. O. Box 30158
Los Angeles, Calif. 90030
Telephone: (213) 486-0150
TDD: (877) 275-5273
Ref #: 1.1

February 4, 2020

Elaine Howle*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

In response to your draft report titled "Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects," I would like to inform you that the Los Angeles Police Department (LAPD) has the utmost respect for individuals' privacy and currently has policies and procedures in place to safeguard personal information stored on the Automated License Plate Reader (ALPR) Systems. Personnel who utilize ALPR data have been through extensive training on accessing and using the data on a right to know and need to know basis. The LAPD continuously reviews all user accounts and deactivates accounts for separated employees, while allowing ALPR access to all active employees who have attended the training. ① ②

Although our dedication to protecting individuals' privacy is covered in our day to day operations and procedures, the Department is currently working on an ALPR policy to ensure that the protection of those rights is also memorialized in our Department Manual. The aforementioned ALPR policy will be completed by April 2020 and posted on the Department website once it is completed, as required by state law. The policy will address the types of information personnel may upload into the ALPR systems, as well as the retention period for the data or lists (i.e., hot lists used to link persons of interest with license plate images). The LAPD will perform an assessment of the systems' data security features and retention periods for ALPR images to evaluate the need for adjustment, prior to publishing of the ALPR policy. Furthermore, the policy will list the entities the Department shares ALPR images with and the process for handling image-sharing requests.

To ensure the ALPR policy is up to date and our ALPR systems are capturing proper information, the Department will perform periodic audits to assess the information the systems capture when accessed by the Department users. Per the recommendations listed in your audit draft report, the Department will have a plan that describes the periodic audits by February 2021 and will complete the first audit by June 2021.

Should you have any questions concerning this matter, please contact Sergeant Monica Tokoro, at (213) 486-0197.

Very truly yours,


MICHEL R. MOORE
Chief of Police

AN EQUAL EMPLOYMENT OPPORTUNITY EMPLOYER
www.LAPDOnline.org
www.joinLAPD.com

* California State Auditor's comments appear on page 61.

Blank page inserted for reproduction purposes only.

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE LOS ANGELES POLICE DEPARTMENT

To provide clarity and perspective, we are commenting on the response to our audit report from the Los Angeles Police Department. The numbers below correspond with the numbers we have placed in the margin of its response.

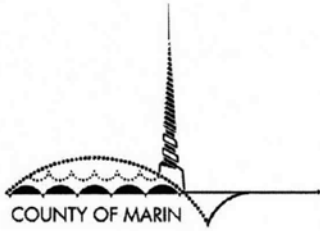
Los Angeles is the only one of four agencies we audited that did not have the ALPR policy state law requires. As we describe on page 15, state law requires law enforcement agencies to have written usage and privacy policies and for the policies to include various elements. As we describe on page 17, the program administrator for Los Angeles initially believed that the agency's many IT policies cover the ALPR program, but we identified deficiencies in the policies he shared with us. When we brought those deficiencies to the administrator's attention, he acknowledged the need for Los Angeles to have an ALPR policy.

①

We stand by our conclusion that Los Angeles does not follow best practices for granting users ALPR system access. As we describe on page 33, of the four agencies we reviewed Los Angeles was the most lax in its approach to authorizing user accounts. The protocol its IT division follows is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system and possibly have not had training, nevertheless have access to the system. Moreover, on page 34 we state that the detective who conducts ALPR training confirmed that Los Angeles has not required training before users can access the ALPR system.

②

Blank page inserted for reproduction purposes only.



OFFICE OF THE
COUNTY COUNSEL

Brian E. Washington
COUNTY COUNSEL

January 28, 2020

Jack F. Govi
ASSISTANT COUNTY COUNSEL

Elaine M. Howle, CPA *
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Renee Giacomini Brewer
CHIEF DEPUTY COUNTY COUNSEL

Dear Ms. Howle:

Patrick M. K. Richardson
Stephen R. Raab
Steven M. Perl
Brian C. Case
Jenna J. Brady
Valorie R. Boughey
Kerry L. Gerchow
Tarisha K. Bal
Deidre K. Smith
Brandon W. Halter
Sarah B. Anker

The Marin County Sheriff's Office appreciates the opportunity to respond to your draft report entitled, Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Marin County Sheriff's Office is pleased to note that although your draft report includes recommendations to the Marin County Sheriff's Office regarding its use of automated license plate reader (ALPR) cameras, your audit team did not find any evidence of abuse or misuse of ALPR data by the Marin County Sheriff's Office.

DEPUTIES

Colleen McGrath
ADMINISTRATIVE SERVICES
OFFICER

Nevertheless, the Marin County Sheriff's Office is and remains committed to the need for further improvement and as stated in your draft report, will consider your report's recommendations. However, based on some of the redactions in the draft report, it is difficult, at times, to determine which findings and conclusions are in reference to the Marin County Sheriff's Office as opposed to the other confidential law enforcement agencies discussed in your draft report.

Marin County Civic Center
3501 Civic Center Drive
Suite 275
San Rafael, CA 94903
415 473 6117 T
415 473 3796 F
415 473 2226 TTY
www.marincounty.org/cl

Accordingly, in responding to the issues discussed in your draft report with additional details and/or context, the Marin County Sheriff's Office will address sections which may not apply to it because it is unable to distinguish which law enforcement agency is being implicated.

The following is the Marin County Sheriff's Office response:

Recommendation No. 1: Improve their ALPR polices.

Response to Recommendation No. 1: While the Marin County Sheriff's Office agrees that its current policy regarding the ALPR system does not specifically describe a "process for periodic system audits," the Marin County Sheriff's Office's policy does state that user/data query audits would be performed. Moreover, although the audit team contends that the ALPR data collected by the

* California State Auditor's comments begin on page 67.

③ PG. 2 OF 4

Marin County Sheriff's Office qualifies as personal information, this is not the case. The draft report readily admits that there is no personally identifiable information contained in a license plate capture. Further, the audit team's erroneous belief is based on a free text box in the ALPR system wherein a user *could* enter a person's name in this text box and attach personal information to the images of license plates captured by the ALPR system. However, the Marin County Sheriff's Office does not utilize this free text box and does not enter any other personal information to be associated with the images taken by its ALPR system. In fact, the draft report concedes this fact as it states in regard to the Marin County Sheriff's Office and open text fields, the audit team "did not find personal information in combination with other sensitive information in the six months of search records [it] studied."

④

Recommendation No. 2: Implement needed ALPR data security.

⑤

Response to Recommendation No. 2: As noted in the draft report, the Marin County Sheriff's Office contracts with a third-party vendor Vigilant Solutions (Vigilant) regarding its ALPR system. While the audit team is critical of Vigilant, all access to Vigilant for the Marin County Sheriff's Office is activity logged and auditable as noted in the draft report, even if the user accesses the system via the internet with a personal device, and those logs are reviewed by the Marin County Sheriff's Office ALPR program administrator; all data on Vigilant is stored on secure servers in the United States as recommended by the audit team; and Vigilant only permits credentialed law enforcement officers with a valid Originating Agency Identifier (ORI) number issued by the Criminal Justice Information System (CJIS) Division of the Federal Bureau of Investigation (FBI). Additionally, as part of its services, Vigilant maintains it is compliant with all relevant requirements set forth in the FBI-CJIS Security Policy as recommended by the audit team.

⑤

Recommendation No. 3: Update vendor contracts with necessary data safeguards.

Response to Recommendation No. 3: As discussed above, while not explicitly stated in the Marin County Sheriff's Office's contract with Vigilant, Vigilant warrants in its services that the data captured by an agency remains the property of the agency; all data is stored on secure servers in the United States; and it conforms with all relevant requirements set forth in the FBI-CJIS Security Policy.

Recommendation No. 4: Ensure that sharing of ALPR images is done appropriately.

Response to Recommendation No. 4: As discussed above, the Marin County Sheriff's Office has confirmed with Vigilant that it has and continues to verify that it only permits credentialed law enforcement officers with a valid ORI number issued by the CJIS Division of the FBI access to the data on its hosted

PG. 3 OF 4

server. While the audit team was critical of the Marin County Sheriff's Office sharing information with agencies such as the Honolulu Police Department, such cooperation with this particular law enforcement agency was done properly and with consideration as to the multiple matters which have in the past involved both agencies. (6)

As for ICE access, any prior approval by the Marin County Sheriff's Office with Vigilant was before any of the relevant state law went into effect. As noted in the draft report, Vigilant confirmed that the recent viewing of ICE accounts in question were not active and that these inactive agencies were not previously visible to the Marin County Sheriff's Office. (6)

Recommendation No. 5: Evaluate and reestablish data retention policies.

Response to Recommendation No. 5: The Marin County Sheriff's Office's two-year retention policy is based on the statute of limitations for most crimes in the State of California. The audit team states that it would like the Marin County's Sheriff's Office to have a more detailed policy regarding retention based on usefulness of images to investigators and even suggest that the retention of the images should be based on whether the images are for minor crimes versus complex crimes. However, it would be impossible for the Marin County Sheriff's Office to know whether the captured images would be used in a minor criminal case or a major felony case at the time the images were taken or at any time afterwards. Indeed, as noted in the draft report, there is no statute of limitations for the crime of murder. (7)

Recommendation No. 6: Develop and implement procedures for granting and managing user accounts.

Response to Recommendation No. 6: The audit team believes that the Marin County Sheriff's Office should require supervisory approval for all users of its ALPR system. As noted above and in the draft report, at this time the Marin County Sheriff's Office does not believe that this particular requirement is appropriate for the following reasons: there is no personal information associated with the images taken by the Marin County Sheriff's Office; as discussed in the draft report, all users of the ALPR system receive training before they are permitted access to the ALPR system; and the Marin County Sheriff's Office regularly audits the use of the ALPR system. (8)

Recommendation No. 7: Develop and implement ALPR system oversight.

Response to Recommendation No. 7: In the draft report, the audit team identifies an incident in which it claims it brought to the Marin County Sheriff's Office's attention an active account for a resigned employee. However, this is not accurate. The system administrator was notified about deactivating the account on the same day the audit team informed him about this account. However, the (9)

PG. 4 OF 4

ALPR administrator had deactivated the account *prior* to the audit team discussing this particular account with him. Moreover, the ALPR administrator does not solely rely on a department-wide email notification regarding resigned or terminated employees as discussed in the draft report. In addition to the audits he regularly performs, the ALPR administrator also performs periodic spot checks to verify that active accounts match active employees.

Should you have any questions regarding this response, including any comments and clarifications made herein, please do not hesitate to contact us directly.

Sincerely,



Kerry L. Gerchow
Deputy County Counsel

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE MARIN COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Marin County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

Marin's response correctly notes that our review of its internal affairs investigations records did not identify evidence of abuse or misuse of ALPR data. However, as we state on page 37, we do not consider this absence as proof that no instances of ALPR misuse occurred. There is the possibility that misuse occurred and went unnoticed and unreported, particularly since Marin does not conduct audits of its ALPR system.

①

During our exit conference, we specifically informed Marin that we would send it only those portions of the draft report that were relevant to it. The text that we redacted pertains to the other entities that were part of the audit and that we are required by law to keep confidential. Further, during its review of the draft report, Marin did not communicate with us to seek clarification regarding the report content we provided, despite our providing multiple opportunities for it to do so.

②

Marin is incorrect in stating that we contend that the license plate images Marin collects qualify as personal information. On page 11, we note that a law enforcement agency can enter additional information, such as personal information, into its ALPR system. However, we do not assert that the ALPR image alone contains personal information.

③

Marin has mischaracterized our finding. In its response, Marin states that we based our conclusion on a free-text box wherein a user could enter an individual's name and attach it to a license plate image. However, as we describe on pages 18 and 19, we based our conclusion on information that users enter into open text fields as part of license plate searches, specifically the fields for case numbers and purpose for the searches. On page 37, we note that Marin requires users to enter both case numbers and reasons for the search before allowing such searches. Although we did not find evidence users had entered personal information in combination with other sensitive information in the six months of search records we studied, the fact that these text fields exist means that users could enter such information during ALPR searches, as we point out on pages 18 and 19. Moreover, Marin's ALPR policy does not prohibit users from entering personal information in combination with other sensitive information in its ALPR system.

④

- ⑤ We disagree with the focus of Marin's response, which implies that the vendor's security controls are a suitable substitute for specific contract safeguards. As we show in Figure 3 on page 22, Marin's contract does not contain any of the safeguards CJIS policy recommends for contracts with cloud vendors. We note on page 21 that CJIS policy states that ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.
- ⑥ We disagree with Marin's belief that it has managed its image sharing appropriately. Although Marin described in its response the type of information that it could maintain to document its image-sharing decisions, it did not provide such evidence documenting why it made past sharing decisions, and its ALPR policy does not include a process for approving image-sharing requests, as we state on page 26. Moreover, Marin acknowledged in its response the issue we describe on page 26 regarding ICE and the fact that the status of Marin's sharing relationship with ICE was not always visible to Marin. This issue underscores the need for Marin to maintain records regarding sharing decisions.
- ⑦ Marin appears to miss the point of our recommendation. As we state on page 29, we concluded that Marin did not establish its retention period based on when it uses the ALPR images it captures. On page 31, we mention minor and complex crimes as examples of ALPR data being used narrowly, such as for the single purpose of locating stolen vehicles, or broadly, such as for investigation of crimes in addition to stolen vehicles. Our recommendation—based on our analysis of Marin's search activity as referenced on page 30—provides a method for Marin to better align how long it retains ALPR data with whether it actually uses the data as they age.
- ⑧ The reasons Marin cites in its response for not adopting our recommendation are not valid. Requiring a supervisor to approve a user for an ALPR account is a meaningful step in establishing that user's need to access ALPR data and right to know what the data portray in an effort to avoid the ALPR data being misused. In point 4 above, we describe that the existence of text fields in the ALPR system allows for personal information to be linked to license plate images. Further, we note that Marin has no policy prohibiting its users from entering personal information in its ALPR system. In addition, despite Marin's claim of training all users, we state on page 34 that Marin does not require staff to renew their training when reactivating their user accounts following long periods of not using the ALPR system. Finally, we found that contrary to Marin's assertion, it had not regularly audited its system. As we discuss

on page 37, Marin's ALPR administrator was unaware of the state law requiring audits of ALPR systems, so he had not been conducting them. Despite recent efforts to institute some form of monitoring, as we describe on page 38, the limitations in its approach led us to conclude that Marin does not have sufficient protocols in place to detect the misuse of user accounts.

Marin's assertion is incorrect. As we describe on page 35, we reviewed Marin's processes for disabling the accounts of separated employees. Although Marin's ALPR administrator informed us of his approach for deactivating an account when he receives an all-staff email that an employee is separating from the department, we found such an email dated August 6, 2019, after which one separated employee continued to hold an active account as of October 22, 2019. After we informed the administrator of this employee's continued access, the administrator acknowledged that the account was still active, and we directly observed him deactivating the account.

⑨

Blank page inserted for reproduction purposes only.

February 2020

Human Assistance

Ann Edwards, Director

**Branches**Customer Service Operations
Finance and Administration
Community and Program Support

County Veterans Services Office

County of Sacramento

January 27, 2020

Elaine M. Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

SUBJECT: License Plate Readers Audit Response

Dear Ms. Howle:

We are writing in response to the draft findings of your report, titled Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Department of Human Assistance (DHA) appreciates the work performed by the California State Auditor. No recommendations were issued in the report, and DHA agrees with the results of the audit.

If you have any questions regarding this matter, please contact Lane Ruddick, Program Integrity Chief, by telephone at (916) 875-1275, or by email at ruddickl@saccounty.net.

Sincerely,

A handwritten signature in cursive script that reads "Ann Edwards".

Ann Edwards
Director

Blank page inserted for reproduction purposes only.



SACRAMENTO COUNTY SHERIFF'S OFFICE

Scott R. Jones
Sheriff

January 28, 2020

Elaine M. Howle, CPA*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

I am in receipt of the draft report entitled *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects*, which includes recommendations for the Sacramento County Sheriff's Office to revise and improve some of our Automated License Plate Reader program (ALPR) processes.

While I agree with some of your findings, I disagree with some of the characterizations made. As the Sheriff of Sacramento County, I take seriously the protection of our citizens, including their personal privacy. Within our role as guardians of the data we collect, my staff works diligently to develop and consistently apply security protocols that maintain the integrity of our systems. ①

The Summary (Results in Brief) section of the report was clearly written separately or prior to the completion of the main body of the report, because it fails to present your teams' actual conclusions. Let me address each point. ①

Recommendation #1 – Review and revise policies

Before the Audit began, the Sacramento County Sheriff's Office began reviewing and revising policies governing a wide range of service deliverables. Although the Sacramento County Sheriff's Office existing policy contains the majority of the requirements outlined in California Civil Code section 1798.90.51, it does not list the restriction on selling ALPR data. As expressed during the interviews, my staff did say that the restriction on selling data is not listed in the policy because the Sacramento Sheriff's Office does not sell any data. The lack of specifically addressing this fact in the ALPR policy is an oversight.

Elaine M. Howle, CPA
January 28, 2020
Page 2

Recommendation #2 – Identify types of data and perform a security assessment

As you learned during the audit, the Sacramento County Sheriff's Office began reorganizing ALPR related security over two years ago. The initial step of this process was securing funding to hire a fulltime Information Technology Analyst in hopes of increasing program administration because this employee's primary job will be the continuous development of ALPR related security protocols that either meet or exceed these recommendations.

Recommendation #3 – Ensure the vendor offers the strongest possible data protections

The Sacramento County Sheriff's Office completed extensive research in the use of cloud storage systems and CJIS security. I am aware your team received the latest contract between the Sacramento County Sheriff's Office and Vigilant Solutions and the Vigilant CJIS Security Policy Guide. Both the contract and comprehensive policy provide a thorough explanation regarding compliance including agreeing to participate in any Technical Security Compliance Audit performed by the FBI-CJIS Division.

②

Recommendation #4 – Develop a process for handling ALPR image-sharing requests

Although the existing policy does provide language on how sharing data can occur, the Sacramento County Sheriff's Office began developing a ticketing system for handling various technology requests over four years ago. As such, the natural progression was to utilize the same request, approval, and record retention system used by the entire organization.

③

Recommendation #5 – Review the retention periods of ALPR images and data

The Sacramento County Sheriff's Office is continually reviewing data retention practices. Although, a simple review of searches provides a small subset of activity, the success of an ALPR program could only come from tracking and identifying which cases provided leads or convictions of data. During the audit, my understanding is your team was told this very fact. As the agency prepares to transition to a new report writing system, I request our crime analysts to conduct a multi-year study that will provide a realistic view of how long ALPR images provide usefulness in the criminal justice system.

④

Recommendation #6 – Enable monitoring of user access and user queries of ALPR images

Throughout the audit your team requested a substantial number of reports and logs showing when accounts were activated, deactivated, or changes occurred. The ability to provide these reports demonstrated the robust nature of the logging system. Although your team learned the

Elaine M. Howle, CPA
January 28, 2020
Page 3

Sacramento County Sheriff's Office has no reported incidents of ALPR misuse, I have directed my program administrator to make certain fields mandatory to ensure proper documentation of usage. With the addition of a dedicated IT Analyst, the expansion of audits already occurring will surely continue.

Recommendation #7 – Ensure that ALPR access is limited to agency staff who have a right and a need to know

Not only is this recommendation listed in the Sacramento County Sheriff's Office policy, it is the way the organization operates with all data systems. As this directly relates to ALPR, only 561 employees, out of a department of 2,170, have access to the system. While I understand your position that a supervisor should approve each account, there were over 5,880 personnel moves during 2019. The Sacramento County Sheriff's Office uses Role Based Access Controls. Rather than rely solely on a supervisor to approve a request, the application of Role Based Access Control is how the Security Operations unit of the Sacramento Sheriff's Office processes access to this and all other law enforcement data systems. Role Based Access Controls are addressed by the National Institute of Standards and Technology as a best practice.

⑤

In Conclusion

In the end, we are not opposed to implementing many of your recommendations and in fact, are already in the process of doing so. Throughout the process, which was long and took many staff hours, we made every effort to cooperate with the auditor's requests for information and tried to anticipate the types of problems they would find while trying to understand the actual uses and practices within the ALPR program.

During interviews and based on some of the requests, we felt concern that there was a bias toward a particular outcome, intended or otherwise. Because this report contains many redacted sections, there is still some concern about what has not been shown to us. Nonetheless, we await your full findings about Sacramento and the other agencies covered in this report.

⑥

⑦

Very truly yours,



SCOTT R. JONES, SHERIFF

Blank page inserted for reproduction purposes only.

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE SACRAMENTO COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Sacramento County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

We stand by the language we use to describe Sacramento's ALPR program. Our report provides appropriate context and sufficient evidence to support our findings. Further, the Results in Brief section of the report serves as a summary of the report as a whole and as such it represents the overall conclusions for this report. The details of our findings and conclusions are included in the Audit Results section of the report.

①

We disagree with Sacramento's contention that the department's current contract is thorough. On pages 22 and 23, we acknowledge that Sacramento updated its contract with Vigilant in September 2019. In reviewing that latest version, we determined that it is missing some of the best practices outlined in CJIS policy, as we show in Figure 3 on page 22. On page 21, we note that CJIS policy states that a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

②

Sacramento's response implies that a process for approving image-sharing requests and maintaining records outside of the Vigilant system was already in place. However, although Sacramento states that it began developing a ticketing system for handling technology requests more than four years ago, as we discuss on page 26, Sacramento could not provide any evidence of records outside of the Vigilant user interface demonstrating when or why it agreed to share with particular entities. As we further point out on page 26, Sacramento's ALPR policy currently does not include a process for approving sharing requests.

③

Sacramento's proposed study of ALPR images may benefit its ALPR program. Our analysis of the search records from the agencies we reviewed—summarized on page 30 and in Table 2—presents one method of identifying the age of the data personnel are using. We point out on page 31 that the agencies' existing ALPR systems provide the ability to conduct such an analysis. Nevertheless, our recommendation does not preclude the type of analysis Sacramento describes in its response.

④

- ⑤ We stand by our recommendation that Sacramento should have a policy that clearly states the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on a need to know and a right to know. As we state on page 32, each ALPR administrator, including Sacramento's, stressed the concept of "need to know, right to know." Assigning an individual an ALPR account based strictly on his or her classification or role—the practice Sacramento follows—does not ensure that an individual has a need to know because of their specific assigned work.
- ⑥ Sacramento's concern about bias is unfounded. To meet generally accepted government auditing standards, which my office is obligated to comply with, we have and follow policies and procedures for all audits to ensure that we identify and rectify any threats to our independence, including bias. Moreover, we follow quality control procedures on every audit that ensure that we have sufficient and appropriate evidence to support our findings and conclusions.
- ⑦ Sacramento received draft text that was relevant to our findings about it. State law requires us to keep confidential information about an unpublished audit. Consequently, we cannot share with one agency information about another. Sacramento received a draft audit report with redacted information regarding other agencies as necessary to maintain confidentiality. During our exit conference, we stressed that staff should contact us with questions they might have about the draft report during the formal review period; Sacramento did not contact us. We also contacted Sacramento's ALPR administrator during the formal review period to inquire about questions staff may have, and he did not return our call.