Smile! You're On Camera--Legal Developments and Best Practices for Disclosure and Retention of Public Camera Footage

Donald A. Larkin
Eli J. Flushman
Burke, Williams & Sorensen LLP

Introduction:

The use of video cameras has become an important tool for public safety. Most law enforcement agencies use some combination of dash-cam, body-worn cameras, and drone video. Camera footage is valuable both for the prosecution of crimes and for defending officers against claims of misconduct. The increased use of video creates opportunities for greater efficiencies for public safety and transparency in policing, but also raises significant privacy issues. The legislature and the courts have provided imprecise guidance in how to balance these competing interests. This paper will discuss best practices for the use and retention of police video, and will outline current law regarding video disclosure.

In addition to video footage, many agencies are using license plate readers to identify and locate stolen and suspect vehicles. The use of license plate readers raises unique privacy and law enforcement questions. While we do not take a position on the use of license plate readers, we will discuss some of the significant issues, and make recommendations on best practices for agencies that choose to use them.

Body-Worn Camera Policy and Retention:

Policies for the use, storage and retention of camera footage are important both to ensure consistency and transparency, but also because having a policy regarding the use of camera footage may be helpful in limiting the scope of footage that an agency needs to review in response to a CPRA request.

Agencies are required to have a policy for the use of body-worn cameras. Penal Code section 832.18 sets out the requirements for a body-worn camera policy. Under 832.18, the policy must:

- Identify who is responsible for downloading footage.
- Identify when data should be downloaded. The timing should, "ensure the data is entered into the system in a timely manner, the cameras are properly maintained and ready for the next use, and for purposes of tagging and categorizing the data."
- Include measures to prevent alteration or deletion of the camera data.
- Require that footage is categorized and tagged according to the type of event at the time of download.

- Identify means and location of storage (e.g. in-house server or third-party cloud database).[1]

Penal Code section 832.18 also requires agencies to specify how long recorded data is stored.[2] The minimum retention periods under the statute are:

- 60 days for non-evidentiary data.
- 2 years if the video:
    - "[I]s of an incident involving the use of force by a peace officer or an officer-involved shooting."[3]
    - "[I]s of an incident that [results in] the detention or arrest of an individual."[4]
    - Is relevant to a citizen complaint against an officer or the agency.[5]

In addition, if the video is relevant to a criminal prosecution, it should be retained for additional time, consistent with other evidence that may be relevant to the prosecution.[6] Access logs and deletion records should be kept permanently.[7]

There is legislation pending that would require policies to be updated to address the recording of individuals undergoing medical or psychological evaluations or treatments. If passed and approved by the governor, the provisions would go into effect July 1, 2027.[8]

Policies and Retention Requirements for Dash-Cam and Drones:

There is no statutory requirement to have a policy for the storage of dash-camera or drone footage.[9] However, the same policy considerations that apply to body-worn cameras apply to

---

[1] If an agency decides to use a third-party vendor, it must consider the experience and reputation of the vendor, the use of contracts to protect the agency's data, inclusion of a built-in audit trail, having a reliable back-up, a system with includes technical assistance capabilities. The agency should consult with legal counsel "to ensure the method of data storage meets legal requirements for chain-of-custody concerns." Penal Code § 832.18(b)(7).

[2] Penal Code § 832.18(b)(5).

[3] Penal Code § 832.18(b)(5)(B)(i)

[4] Penal Code § 832.18(b)(5)(B)(ii)

[5] Penal Code § 832.18(b)(5)(B)(iii)

[6] Penal Code § 832.18(b)(5)(C)

[7] Penal Code § 832.18(b)(5)(E)

[8] California Senate Bill No. 691, California 2025-2026 Regular Session.

[9] Under California Assembly Bill No. 481 (2021) (Gov. Code § 7070 *et. seq*.), law enforcement agencies are required to have policies for the use of military equipment, including drones. The

other video recordings used by law enforcement. Penal Code section 832.18 sets a minimum standard. Agencies should consider expanding the required body-cam policy to include other types of video recording.

But note that there is no express authority to limit retention of video other than body-worn camera video to 60 days. Dash-cam footage may be considered "routine video monitoring" under Government Code section 34090.6, which defines video monitoring as including "mobile in-car video systems."[10] Under section 34090.6, recordings of routine video monitoring must be maintained for a period of one year. There is no specific retention requirement for drone video. Drone video footage may be subject to the default two-year retention requirement under Government Code section 34090(d).

There is very little legislative or judicial guidance regarding retention of dash-cam or drone footage that is not relevant for any public purpose. A conservative approach is to simply retain all dash-cam and other video footage for one or two years. However, this may not be practical for some smaller agencies. Some agencies have taken the position that only video that is retained for a public purpose must be retained for the statutory period.

Other Policy Considerations—Artificial Intelligence and Camera Footage

New technology allows artificial intelligence to assist with report-writing by creating summaries and transcripts from audio and video recordings. Under Penal Code section 13663, if artificial intelligence is used to summarize camera footage and prepare a report, the report must 1) disclose that artificial intelligence was used, and 2) include a signed statement from an officer that they reviewed the report and verified the facts. There are other procedural requirements in section 13663 for the use of artificial intelligence in police reports that should be incorporated into an agency policy.

Disclosure of Video Recordings Under the California Public Records Act

In general, records of investigations by police agencies are exempt from disclosure under the CPRA.[11] However, there are certain exceptions to this general rule. One exception, provided under California Senate Bill 1421 (2019), is for audio or video recordings that "relate to a critical incident."[12] A recording "relates to a critical incident if it depicts . . . (1) An incident involving the discharge of a firearm at a person by a peace officer or custodial officer," or "(2) An incident in which the use of force by a peace officer or custodial officer against a person resulted in death or in great bodily injury."

---

policies are required to address how equipment is used and the purpose of its use. Agencies may want to consider including information about the storage and retention of camera footage in those policies. (see: Gov. Code § 7070 *et seq.*)

[10] Section 34090.6 applies to cities, but the same requirements are applied elsewhere to counties and special districts.

[11] Gov. Code § 7923.600.

[12] Gov. Code § 7923.625.

The term "great bodily injury" is not defined for purposes of disclosure under the CPRA. The only other use of the term in the code is as a Penal Code sentencing enhancement for felonies that do not have bodily harm as an element.[13] Under the Penal Code, "'great bodily injury' means a significant or substantial physical injury."[14] In *City of Fresno v. Superior Court* ((2026) __Cal. App 5th ___), the 5th District Court of Appeal held that the Penal Code definition applied to disclosure under the CPRA. However, the court did not discuss how this definition applies to specific injuries. While case law interpreting the sentencing enhancement may be helpful, whether the enhancement applies is a jury question. This leads to inconsistent definitions of the term.

California law also requires police agencies to report annually to the Department of Justice any use of force incidents that caused "serious bodily injury." "Serious bodily injury" is defined in the Government Code to mean "a bodily injury that involves a substantial risk of death, unconsciousness, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member or organ."[15] The disclosure to the Department of Justice may be a helpful tool in determining whether a specific incident should be disclosed.

Video That "Depicts" a Critical Incident

In *Sacramento Television Stations Inc. v. Superior Ct.*, ((2025) 111 Cal. App. 5th 984), the Third District Court of Appeal addressed the question of what constitutes a video that "depicts" a critical incident. The case involved an officer-involved shooting by officers from the Roseville Police Department.[16]

In *Sacramento Television Stations,* Roseville officers responded to a request for assistance from California Highway Patrol officers, who had come under fire while attempting to serve a warrant on a suspect in a local park. When Roseville officers arrived, they immediately opened fire on the suspect. The officer-involved shooting by Roseville lasted just seconds. Almost immediately after Roseville officers began shooting, the suspect fled into another part of the park. The Roseville officers stopped shooting, and instead sent drone up to search for the suspect. When the officers located the suspect with the drone, he had taken two hostages. The suspect shot both hostages, killing one. Roseville officers were able to negotiate the suspect's surrender without any more shooting.

In response to a request from a local CBS affiliate, Roseville police released four 39 second videos of the officer-involved shooting.[17] These were all of the videos that Roseville determined "depicted" the shooting. CBS later learned that there was a drone video that had not been

[13] See Penal Code § 12022.7.

[14] Penal Code §12022.7(f)(1)

[15] Gov. Code § 12525.

[16] The facts outlined here are from the trial court pleadings and briefing.

[17] The Highway Patrol officers did not have body-worn camera.

released, and requested a copy of that video. Roseville denied the request for the drone video for various reasons, including that the video did not depict the officer-involved shooting. CBS filed a writ, which the trial court denied. The trial court did not view the drone video in camera, and did not make a determination on whether the video depicted the officer-involved shooting, instead finding that release of the video would interfere with the criminal prosecution of the suspect.

The Court of Appeal overturned the trial court's basis for denying the writ, and instead focused on arguments over whether the drone video should be released as depicting the officer-involved shooting.

CBS argued for the broadest possible disclosure, claiming that Government Code section 7923.625 requires disclosure of footage "from the time that [Roseville PD] arrived on scene at the critical incident to the time the scene was secured."[18] The First Amendment Coalition's amicus argument was slightly narrower, claiming that the statute "requires disclosure of recordings that depict 'the totality of circumstances before and after a police shooting.'" Including "sufficient 'post-shooting' footage to confirm that law enforcement officers 'promptly rendered first aid, secured the scene, and refrained from contaminating or planting evidence.'"[19]

Roseville's position was that an "incident involving the discharge of a firearm" includes "the context leading up to the discharge, the discharge itself, and the officer's disengagement following the discharge—here no more than thirty-nine (39) seconds for each discharge."[20] CalCities filed an amicus brief in support of Roseville, arguing that the "occurrence encompassed 'a series of incidents,' of which the officer-involved shooting was just one. Under this view, [the suspect's] arrest was a distinct incident, as was the effort to render medical aid to the victims. As for the meaning of the words 'incident' and 'involving' in subdivision (e)(1), the amicus brief contends the word 'involving' is 'merely a modifier that identifies the type of incidents that are subject to disclosure,' while the word 'incident' —which one dictionary defines as a 'discr[ete] occurrence or happening'—is 'the operative term' in the phrase."[21]

The Court of Appeal found that "the construction of subdivision (e) proposed by amici for Sac TV to be too broad, and the construction proposed by the City and its amici, while perhaps acceptable in the abstract, to be too narrow as applied here."[22]

Instead, the Court held that CBS is entitled to receive "(a) *uninterrupted* copies of *all* Roseville PD recordings of the . . . occurrence that were captured during the three-minute window of time when, the City alleges, the entire incident involving firearm discharge by Roseville PD took place, along with (b) ***additional recordings that provide sufficient context to permit an understanding of why the first shot was fired and what happened in the immediate aftermath***

---

[18] *Sacramento Television Stations Inc.* 111 Cal.App.5th at 1002.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

of the final shot."[23]

The Scope of the Investigative Exemption

In addition to critical incidents, agencies may be required to disclose camera footage on the basis that it falls outside of the investigative exemption. *Castanares v. Superior Court* ((2023) 98 Cal.App.5th 295) was the first appellate decision to address the scope of the investigative exemption as applied to video footage. The case involved a request from a member of the public for footage from a pilot drone program in Chula Vista. At the time, Chula Vista was participating in a pilot program using "drones as first responders for certain 911 calls. Per this program, a police officer determines when sending a drone to examine a situation is an appropriate response to a public call for assistance. If the officer decides that the use of a drone is suitable, a remote pilot flies the drone to the area in question, streaming video to the officers to better inform them how to respond to the situation."[24] Chula Vista denied the request, citing the investigative exemption under Government Code section 7923.600. The requester filed a writ, which the trial court denied, finding that the footage was subject to the exemption.

The Fourth District Court of Appeal held that the trial court "erred in determining, as a matter of law, all video footage from the drone program is exempt under section 7923.600, subdivision (a) as records of investigations."[25] Instead, the Court of Appeal identified three categories of footage that should be evaluated independently.

The first category is footage that is "part of an investigatory file." That footage is categorically exempt from disclosure.[26]

The second category are "instances where officers used a drone to investigate whether a violation of law was occurring or had occurred but did not create a corresponding investigatory file." The Court identified specific examples, including "dispatching a drone to investigate a possible assault, a claim of someone causing a disturbance, or a suspected break-in; yet, the resultant video footage did not become part of an investigatory file."[27] These types of incidents are also subject to the investigatory exemption.

The third category include drone footage that does not fall within the first two categories. "Such footage would consist of using a drone to make a factual inquiry to determine what kind of assistance is required, not to investigate a suspected violation of law. For example, a 911 call about a mountain lion roaming a neighborhood, a water leak, or a stranded motorist on the freeway could warrant the use of a drone but do not suggest a crime might have been committed

---

[23] *Id.* at p. 1005.

[24] *Castanares at p.* 300.

[25] *Id.*

[26] *Id. at p. 310.*

[27] *Id.*

or is in the process of being committed."[28] Under the Court of Appeal's analysis, this type of footage does not fall within the investigative exemption to the CPRA.

The Court of Appeal decision does not address other possibilities, where the type of call is unknown at the time the drone is deployed. For example, a drone may be deployed to a call of a person lying on the sidewalk, or a person acting erratically in public. The purpose of sending the drone would be to determine whether or not to send law enforcement, or whether it is a purely medical call. It is unclear from the opinion which category that type of call would fall into.

The *Castanares* court also addressed privacy and the burden of producing hours of drone video. Chula Vista argued that due to the time necessary to review and redact hours and hours of video footage, "the public interest in nondisclosure clearly outweighs the public interest in disclosure" under the CPRA balancing test.[29] The Fourth District acknowledged privacy interests in the drone videos, and the presumed need for redaction. The "need to redact the drone video footage is compelled by privacy concerns. As the trial court correctly noted, our state Constitution expressly grants all Californians the right of privacy. (Cal. Const., art. I, § 1.) And here, we agree that the drone video footage implicates serious privacy concerns."[30] However, the Court held that Chula Vista "did not carry its burden in showing the catchall [balancing test] provision applies here."[31]

While *Castanares* is one of several appellate opinions that have reaffirmed that there is a level of burden on public agencies that could theoretically tip the balance in favor of nondisclosure, no appellate case has yet defined the tipping point.

The *Gilroy* Case and Retention Requirements

One way to reduce the burden of video review is to follow the agency's retention schedule, and promptly destroy records as appropriate. In *City of Gilroy v. Superior Court* ((2026) 19 Cal.5th 38), the Supreme Court addressed whether the CPRA requires agencies to retain exempt records from the date the exemption is invoked until the requestor is able to obtain judicial review of the agency decision. The case involved a series of CPRA requests from the Law Foundation of Silicon Valley for records related to Gilroy's encampment cleanup efforts. In 2019, the Law Foundation expressly requested body-worn camera footage related to the encampment cleanups. Gilroy denied the request under the investigative privilege.[32] At the same time, they informed the Law Foundation that footage from before early 2018 had been destroyed under Gilroy's records retention schedule.

---

[28] *Id.*

[29] Gov. Code § 7922.000.

[30] *Id.* at p. 314.

[31] *Id.* at p. 316.

[32] The City later voluntarily released some of the body-worn camera footage that was not related to enforcement efforts, without conceding their position that it was exempt.

The Law Foundation argued that Gilroy was on notice at the time of their request that they were seeking the records, so the City should have placed a litigation hold on the recordings at the time of request, even without a threat of litigation over the City's determination that they were exempt. The Law Foundation asserted that the hold should have remained for the full three-year statute of limitations.[33]

The Supreme Court reaffirmed that the CPRA is not a retention statute, holding "[w]e are unpersuaded that by providing for judicial oversight in the CPRA, the Legislature intended to require the retention of records for three years, commencing with the assertion of a statutory exemption. In essence, the Law Foundation's argument is that the CPRA imposes a records retention requirement because the CPRA allows for litigation. But if litigation is what justifies preservation, then it seems unlikely that the Legislature intended for broad preservation of potentially responsive public documents given that, as the parties here agree, public records requests rarely result in litigation."[34]

However, the Court also addressed the question of whether the scope of declaratory relief available under the CPRA extends to an agency's past actions. The Law Foundation argued that Gilroy conducted an inadequate search for records, asserted the investigatory exemption for body-worn camera footage without reviewing all of the footage before making a determination, and for responding to the request late.

The Supreme Court held "that the CPRA authorizes declaratory relief that a public agency has violated its provisions even in some circumstances when it is uncontested that there are no existing nonexempt records to disclose." Declaratory relief was permissible in the *Gilroy* case "because [the declarations] resolve an ongoing dispute about the parties' respective statutory rights and obligations and thus serve to guide their future conduct."[35]

Automated License Plate Readers

Automated License Plate Readers (ALPRs) are defined by statute as a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.[36] In essence they are camera systems that automatically capture, analyze, and store vehicle license plate data using optical character recognition (OCR) to convert plate images into text, which are then automatically checked against databases for various information, such as stolen vehicles or missing persons lists (i.e., "hot lists").[37] The

[33] *City of Gilroy* at p. 63.

[34] *Id.* at p. 65.

[35] *Id.* at p. 63.

[36] Civ. Code § 1798.90.5, subd. (d)

[37] California State Auditors Report, 2019-118, "Automated License Plate Readers, To better Protect Individuals Privacy, Law Enforcement Must Increase its Safeguards for the Data it Collects (hereafter, "State Auditors Report")(February 2020), p. 7)

ALPR cameras are typically mounted either on a patrol vehicle which are able to scan license plates while in motion, or mounted on fixed locations, like light polls. This tool has been in existence since the 1970's, but widespread adoption began in the mid 2000's.[38]

Use of ALPRs can result in the creation of millions of images of license plates over a short period of time.[39] Although these images are collected while vehicles are in public where there is no reasonable expectation of privacy of a license plate, the use and retention of those images raises privacy concerns.[40]

In California the use ALPR technology is permitted, but its implementation, use, sharing, and disseminating of information derived from such technology is regulated primarily by Civil Code section 1798.90.5 *et seq*. The regulations are intended to balance the technology's investigative benefits against privacy concerns and misuse.[41] The statute sets forth the most significant requirements for the use of ALPR technology in California. In addition, the California Department of Justice issued an information bulletin to state and local law enforcement agencies in October 2023 to provide further guidance regarding how ALPR information is to be stored, collected, shared, and used.[42]

Below is an overview of the statutory requirements for operating, using, accessing, and sharing information from an ALPR system:

- Privacy and Usage Policy.

The statute requires an agency to implement a publicly available, written usage and privacy policy on the agency web site that contains certain minimum requirements for an "ALPR operator"[43] and similar requirements that apply to an "end-user."[44] While most agencies will use ALPR technology as both operators and end-users, the differences between the policy requirements denote different obligations and considerations that must be addressed in the policy.

The requirements that apply to both operator and an end-user policies are that it must include:

---

[38] *Id.*

[39] *American Civil Liberties Union Foundation v. Superior Court* (2017) 3 Cal.5th 1032, 1037

[40] *Id. at* 3 Cal.5th 1032, 1044

[41] State Auditors Report, *supra*, at p. 2

[42] California Department of Justice, Information bulletin 2023-DLE-06, "California Automated License Plate Reader Data Guidance" (hereafter, "DOJ Guidance").

[43] Civ. Code 1798.90.51. ALPR Operator defined as "a person that operates an ALPR system . . . ." (Civ. Code § 1798.90.5, subd., (c).)

[44] Civ. Code § 1798.90.53. ALPR end user defined as "a person that accesses or uses an ALPR system . . . ." (1798.90.5, subd., (a).)

- The **purposes** of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.
- The title of the official custodian, or owner, of the ALPR system **responsible** for implementing this section.
- A description of the reasonable measures that will be used to **ensure the accuracy** of ALPR information and correct data errors.
- The length of time ALPR information will be **retained**, and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information.[45]

The remaining minimum requirements while closely aligned, impose slightly different substantive considerations whether operating an ALPR system or for accessing the data as an end-user. Below is a comparison of the similar but different remaining minimum policy requirements:

ALPR operator	**ALPR end-user**
The authorized purposes ***for using the ALPR system and collecting ALPR information*.**	The authorized purposes ***for accessing and using ALPR information.***
A description of the job title or other designation of the employees and independent contractors who are authorized to ***use or access the ALPR system, or to collect ALPR information***. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.	A description of the job title or other designation of the employees and independent contractors who are authorized ***to access and use ALPR information***. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.
A description of how the ALPR system will be monitored to ensure the security of the information ***and compliance with applicable privacy laws***.	A description of how the ALPR system will be monitored to ensure the security of the information ***accessed or used, and compliance with all applicable privacy laws and a process for periodic system audits.***[46]

An agency should be sure to carefully craft clear policies that define the purposes and procedures to meet these minimum requirements. The more detailed the policy, the more effective it will be and the better chance the agency can avoid misuse and avoid surprises. Further, a policy should be periodically revisited to ensure the policy meets the real world application of the ALPR system. As the use of ALPR systems evolve, the purposes and values for its use may also evolve, and that should be reflected in the policy. In addition, vendors frequently update their systems and provide new ways of navigating or accessing the ALPR information that may not reflect how the policy was originally written. For example, many ALPR systems allow for sharing access with another

[45] Civ. Code § 1798.90.51, subd. (b); Gov. Code § 1798.90.53, subd. (b).

[46] *Id.*

agency to occur through a simply toggle of a button, but the original policy may require a written request and determination be made. As such, an agency should ensure that their real world use both complies and is reflected in their policy.

- Data Security.

ALPR operators and end users are required to maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.[47]

In addition to completing training, the types of safeguards noted above may include, supervisor approval for account access, individual log in credentials, two-step authentication, require access only through specific workstations, restrict access to staff who perform certain functions, or require periodic re-training. Imposing clear guidelines or limitations on a valid reason for accessing and conducting a search and how to document the reason clearly will aid in meeting the data security requirements. In addition, a strong auditing process that both ferrets out misuse and creates a framework for implementing changes in the policy will further support meeting this data security obligation.

Another point of data security is the contract with the vendor for the ALPR system. The contract should include provisions to ensure the sufficient safeguards to protect ALPR data. Contract provisions may include clearly identifying that the agency owns the data it uploads into the system, that data will not be stored outside of the United States, and that employees of the vendor will undergo training and background checks. Taking care to ensure the contract also protects the data is a part of providing sufficient data security.

- Access Logging and Auditing.

Systems must log all access to ALPR data, including the (1) date and time the information is accessed, (2) the license plate number (and other data elements), (3) the user name of the person who accesses the information and the organization with whom the person is affiliated, and (4) the purpose of the query.[48]

While access logging functions are typically automated, ensuring that automated process gathers all the required information, as well as any other details, can assist the agency in completing a more effective audit.[49]

Auditing the ALPR system is the most effective tool in ensuring overall compliance with the regulations. However, neither the statute or any cases provide information on what qualifies as a "periodic system audit." Each agency therefore must consider the expectations of their community

[47] Civ. Code § 1798.90.51, subd. (a); 1798.90.53, subd. (a)

[48] Civ. Code § 1798.90.52, subd. (a)

[49] Civ. Code § 1798.90.53, subd. (b)(2)(C)

and council and craft audit procedures that will help identify and correct misuse. For some agencies that may mean an annual or quarterly audit, and for other agencies that may be monthly, or more.

The audit procedures should provide sufficient detail to help ensure an effective audit. Such procedures should identify who will complete the audit, how often an audit is conducted, what type of report or summary will be prepared, who will review and approve the audit. The policy may also want to include some general guidelines on how to conduct the audit, including guidance on random spot checks, or reviewing who is accessing the ALPR information both internally and externally. An agency should be sure the audit includes a sufficient review of the reasons for accessing the data match applicable policy, that security procedures are both being followed and are effective, that records are properly being destroyed, and that training is being effectively conducted. A report summarizing the audit is a good tool to ensure accountability. Such a report may include details regarding any identified misuse or policy violations and corrective actions taken, as well as potential suggestions on updating the policy, and may provide guidance on future audit reviews.

- Public Comment.

Public agencies that operate an ALPR system are required to provide an opportunity for public comment *before* implementing an ALPR system.[50] It should be noted that this requirement for public comment must occur at a regularly scheduled public meeting.

- Sharing.

The ALPR statute restricts a public agency from selling, sharing, or transferring ALPR information, except to another "public agency, and only as otherwise permitted by law."[51] the Term "ALPR Information" means information or data collected through the use of an ALPR system.[52] This would include the license plate data collected. The term "public agency" is defined as agencies within the state of California.[53] Or to put it another way, a public agency under the statute *does not* include the federal government or an agency or law enforcement department from another state. Any effective audit must include a step to ensure that the data is *only* shared with a public agency as defined in the statute.

- Retention of ALPR records.

The ALPR statutes do not specify retention period for ALPR data. As such an agency should follow its retention schedule. The agency may want to consider a specific retention period that reflects the utility of retaining such data and that is specific to certain types of records (e.g., audit reports

[50] Civ. Code § 1798.90.55, subd. (a)

[51] Civ. Code § 1798.90.55, subd. (b)

[52] Civ. Code § 1798.90.5, sub. (b)

[53] Civ. Code § 1798.90.5, subd. (f): "Public agency" means the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including, but not limited to, a law enforcement agency.

v. bulk data), and balance that against privacy concerns. Having a process to purge the data at the time it is no longer useful will help to protect individual privacy. An agency can review the search parameters being used to help inform itself of the useful period of the data.

- Violations and enforcement.

The ALPR statute authorizes individuals who have been harmed by a violation of the ALPR statute to bring a civil action against a person who knowingly caused the harm.[54] A court can award a combination of damages, which may include, (1) actual damages, not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500), (2) punitive damages upon proof of willful or reckless disregard of the law, (3) reasonable attorney fees and litigation costs, and (4) other preliminary or equitable relief.[55]

There is one case construing this cause of action, *Bartholomew v. Parking Concepts, Inc*. (2026) 118 Cal.App.5th 438. In that case, a private parking garage operator was alleged to be automatically collecting license plate information in violation of the statute by failing to implement and make publicly available a policy governing the collection and use of this data.[56] The trial court sustained the operators demurrer without leave to amend and the owner appealed. The appellate court construed whether the lack of the publicly available policy constituted the "harm" envisioned. The court noted that the statute does not require a plaintiff to suffer measurable monetary damages in order to establish harm, as there is a provision for a set amount of liquidated damages.[57] However the court declined to extend the meaning of "harm" to equate to *any* violation of the ALPR law.[58] The court reasoned that the legislatures inclusion of two examples of harm causing violation indicated that more than just a violation is required, "as there would be no need to provide examples if *any* violation was sufficient.[59]

Nevertheless, the court considered whether the lack of the publicly available policy constituted a cause of action to sustain a demurrer. The court determined that the failure to create a publicly available policy in compliance with the statute *does* constitute "harm" within the meaning of the ALPR law. The court found that the lack of the policy deprives an individual of the "right to know" that their data is being tracked and inform them of whether they want to avoid the location.

As such, agencies using ALPR systems must establish a policy and make it publicly available to allow individuals the right to know that their information is being tracked.

Additional potential repercussions for violations of the ALPR statutes include enforcement efforts from the California Department of Justice. In October of 2025 the California Attorney General

---

[54] Civ. Code 1798.90.54, subd., (a)

[55] Civ. Code § 1798.90.54, subd. (b)

[56] *Bartholomew v. Parking Concepts, Inc*. (2026) 118 Cal.App.5th 438, 442-443.

[57] *Bartholomew v. Parking Concepts, Inc*. (2026) 118 Cal.App.5th 438, 447

[58] *Ibid.*

[59] *Ibid.*

filed a lawsuit against the City of El Cajon over its refusal to comply with state law prohibiting the sharing of license plate data with federal and out-of-state law enforcement agencies.[60] The state's petition seeks a writ of mandate, injunctive and declaratory relief directing the city to cease sharing and barring the sharing of ALPR data with out-of-state agencies. The case is currently pending in Superior Court in San Diego County.

The bottom line is that there are real enforcement consequences for violations of the statute. In particular in today's climate sharing with federal and out-of-state agencies has become a hot topic due to the threat it may be used to conduct extreme immigration enforcement, or may track persons seeking to conduct abortions. If an agency allows misuse of its ALPR system, regardless of any legal liability, the department and personnel may face significant public scrutiny. This may include news coverage, or facing a city council and angry constituents who demand answers regarding any alleged misuse.

ALPRs and the Public Records Act.

Given the immense amount of images that ALPRs create, agencies should expect that information related to ALPRs will be requested through a Public Records Act request or through a subpoena in litigation. The remaining portion of this article will discuss the law related to requests for such data and related public records.

Bulk ALPR Data

While exemptions in the public records act specific to law enforcement records protect "records of investigation"[61] case law has restricted that specific exemption in relation to bulk ALPR data. In *American Civil Liberties Union Foundation v. Superior Court,*[62]the California Supreme Court considered a request on the Los Angeles Police Department and the Los Angeles Sheriff's Department, for all ALPR data collected during a one-week period. The law enforcement agencies withheld the records under the records of investigation exemption.[63] In conducting its analysis the court noted the stark differences between the types of records of investigation considered in a previous case, *Haynie v. Superior Court*,[64] where the records sought concerned an individual deputy stopping an individual driver based on a single close in time tip from a neighbor, juxtaposed again the collection of bulk data of ALPR information.[65] The court recognized that the concerns in *Haynie* included that a record of investigation reveals certain choices that should be kept confidential, including in informant's choice to come forward, or an

[60] *The People of the State of California v. City of El Cajon* (Super. Ct. San Diego County, pending, filed Oct. 3, 2025, Case No. 25CU053437C)

[61] Gov. Code 7923.600

[62] *American Civil Liberties Union Foundation v. Superior Court* (2017) 3 Cal.5th 1032

[63] *Id.* at 3 Cal.5th 1032, 1038.

[64] *Haynie v. Superior Court* (2001) 26 Cal.4th 1061

[65] *American Civil Liberties Union Foundation v. Superior Court* (2017) 3 Cal.5th 1032, 1041

investigator's choice to focus on particular individuals or use certain investigation methods.[66] Whereas ALPR scan are conducted with an expectation that the vast majority of the data collected will prove irrelevant for law enforcement purposes.[67] The court thus held that the process of ALPR scanning does not produce records of investigation because the *scans* are not conducted as part of a targeted inquiry into any particular crime or crimes.[68] Thus, ALPR scans and the bulk information are not exempt as records of investigation pursuant to Government Code section 7923.600.

However, the unaltered bulk ALPR data was determined to be exempt under the public interest balancing test, as the court upheld the trial court's determination that that the balance of interests "weighed clearly against disclosure of raw ALPR scan data."[69] The court reasoned that disclosing unaltered plate scan data to the public threatens individual privacy and could potentially reveal where a person lives, works, or frequently visit.[70]

The court, also considered the trial courts finding that even anonymized ALPR data was exempt under the public interest balancing test. The court could not agree with the court's reasoning, suggesting that the trial court was too speculative, and therefore, there did not appear to be a clear overbalance on the side of confidentiality.[71] Ultimately, the court declined to determine whether the "catchall" exemption would apply to anonymized data, suggesting greater consideration be provided to the feasibility of anonymization and the public interests implicated thereby.

As such, if an agency can demonstrate that on the facts of a particular case the public interest in nondisclosure *clearly* outweighs the public interest in disclosure, such data may nevertheless be withheld as exempt.

Another exemption may also provide additional protection of disclosure of ALPR bulk data. Section 7927.705 of the Government Code provides that the disclosure of records which are exempted or prohibited pursuant to federal or state law is not required. As noted by the DOJ guidelines, the ALPR statute prohibits an end-user or operator from selling, sharing, or transferring ALPR information, except to another public agency, and only as otherwise permitted by law, and implores agencies to consider all applicable relevant exemptions when responding to a request.[72] As such, sharing or transferring ALPR information, which is defined as information or data collected through the use of an ALPR system, in response to a public records act request is prohibited by Civil Code section 1798.90.55, subdivision (b).

---

[66] *Id.*

[67] *Id.* at 3 Cal.5th 1032, 1042

[68] *Id.*

[69] *American Civil Liberties Union Foundation v. Superior Court* (2017) 3 Cal.5th 1032, 1044

[70] *Ibid.*

[71] *Id.* 3 Cal.5th 1032, 1045-46

[72] Civ. Code § 1798.90.55, subd. (b)

Audit Records.

Another common request agencies may receive are related to records of audits of the ALPR system. As a starting matter, the Public Records Act imposes no duty to create any records. The act requires that "upon a request for a copy of records that reasonably describes an identifiable record or records, [the agency] shall make the records promptly available."[73] An identifiable record must therefore already exist. It should also be noted that a "public record" is defined to include writing relating to the conduct of the public's business "prepared, owned, used, or retained by any state or local agency.[74] Therefore, a public record must already exist to be retained by an agency. And given the requirement to complete periodic audits, where such audits exist, they would appear disclosable, subject to some potential exemptions requiring redactions as discussed below.

In addition, in the author's experience, requests have been made that essentially seek an audit on demand, requesting the agency produce audit results for a specific period of time (e.g. January 1, 2025 – December 31, 2025), and demanding the agency run an audit function within the ALPR vendor's software for the requested time period. Unless the Agency has run this audit already, an agency may be able to conclude that no such record exists. However, the agency should be mindful of its duty to assist members of the public related to their request.[75]

While there may be no duty to create a record and run an audit on demand, periodic audits are required. Analysis must be conducted on whether the audit, or portions thereof, are exempt. The following are considerations that may exempt portions of audits:

- Privacy related information included within the audit records (e.g. license plate numbers). An agency would have to articulate that disclosure is unwarranted under the public interest balancing test.[76]
- Records of investigatory information may be included in audit records.[77] Agencies may need to review audit details and redact investigation details captured in a report, such as suspect names or suspect license plates. These details may be included in the "reasons" section within the system. However, an effective policy that details how to craft the reasons may assist the agency in avoiding having to make such redactions.
- To the extent ALPR information is contained in the audit results it may be able to be redacted given the prohibition on sharing or transferring ALPR information to only certain authorized persons.[78] The Agency may have to provide certain information such

[73] Gov. Code § 7922.530

[74] Gov. Code § 7920.530, subd. (b)

[75] Gov. Code § 7922.600

[76] Gov. Code § 7922.000

[77] Gov. Code § 7923.600

[78] Civ. Code 1798.90.55, subd. (b); Gov. Code § 7927.705

as the agencies making the queries, but may be able to redact other data, such as license plates and other data.

- Any other information where the public interest in non-disclosure clearly outweighs the public interest in disclosure.[79]

Having routine audits and reports that detail findings and actions taken may prove to provide an effective balance of providing summary information about the ALPR system audit negating challenges to redactions to certain data points.

Locations of ALPR cameras.

The location of ALPR cameras is another item the author sees frequently requested. Whether to disclose the locations is treated differently among jurisdictions. Some agencies simply provide the locations. While other agencies take the position that the location of the cameras are exempt under the public interest balancing test. While there is public interest in knowing the locations to ensure law enforcement surveillance systems operate effectively and promote public safety, the disclosure of such information can undermine the effectiveness of the technology, and negatively impacting the utility of this law enforcement tool. Disclosing the location may enable individuals engaging in unlawful activity to deliberately avoid detection by altering routes, timing, and behaviors, severely undermining the effectiveness of the system, and also undermining public safety. Further, ALPRs can be moved from one location to another, so providing the location may be stale in a matter of time.

ALPRs and Subpoenas

ALPR data is information that can be useful in civil litigation and is sought from time to time via civil subpoena. However, producing the records in response to a subpoena would involve sharing or transferring ALPR information, which is not allowed unless to another public agency, and only as otherwise permitted by law.[80] The DOJ guidelines implore agencies to consider all applicable privileges in such situations.[81] To the extent such "ALPR information" is requested through a subpoena an agency may want to consider whether the person requesting is authorized to receive such data, and if not, objecting with reference to the prohibition pursuant to Civil Code section 1798.90.55, subdivision (b). A litigant *may* be able to obtain a court order that could conceivably equate to sufficient authority permitting some limited release. However, In such a case, care must be taken that sufficient redactions have been made to protect privacy unrelated to the litigation. In addition, depending on an agencies retention schedule, before objecting, the agency should confirm whether the record continues to exist, as if the data has been destroyed according to policy it may make the request moot.

[79] Gov. Code § 7922.000

[80] Civ. Code § 1798.90.55, subd. (b)

[81] DOJ Guidelines, p. 3