**CHICO POLICE DEPARTMENT**

# Chico PD License Plate Reader Program Supplemental Information

A Companion Reference: ALPR Technology, Data, and Auditing Concepts

# Table of Contents

1. **Broad Overview of ALPR Technology**
    a. Synopsis:

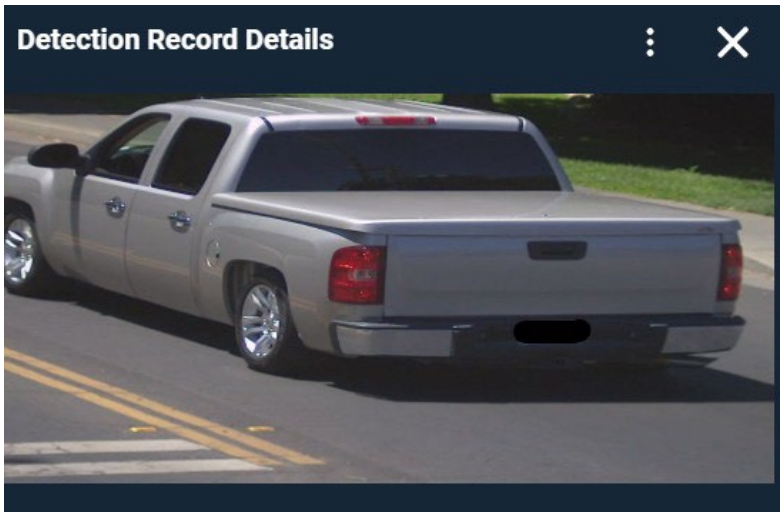
Industry and academic sources predominately assert that license plate camera technology was implemented for law enforcement purposes in the late 1970's in the United Kingdom, although automation came many years later. Widespread use in the United States did not come about until the 2000's. Technical limitations and costs made implementation prohibitive to most agencies regardless of efficacy at that time. Advances in technology combined with significant price decreases have made technology more accessible and ALPR technology is now currently widespread. Among other applications, ALPR cameras are utilized for parking enforcement, toll collection, private security, and commercially (by tow trucks, taxi cabs, and private entities).

It is important to carve out specific distinctions between the different types of ALPR programs based on their applications. In addition, it is imperative to understand the scope and capabilities of their interfaces with additional emphasis on software vs. Artificial Intelligence (A.I.). For the purposes of "what" is being collected, the actual physical camera is less important than its application and supporting software.

ALPR cameras take still framed photographs of vehicles, specifically targeted at acquiring the license plate. The stored photographs are referred to as "Detections." The snapshot of a vehicle (detection) is then uploaded and stored in a "database." Detections created by ALPR systems are processed and stored according to their respective applications. Although factually accurate that a red-light enforcement camera essentially detects a vehicle, as does a tollbooth camera, the subsequent processing and storage of the data is distinctly different. Distinctions between these different systems will be explained below in upcoming sections of this report. For the purposes of this report, the focus is Motorola ALPR technology and the LEARN platform by which the data is accessed. The LEARN platform's name has recently been rebranded to Vehicle Manager 8.0 by Motorola, but the names are used interchangeably. References to other ALPR vendors or applications of ALPR technology are for illustrative purposes and to create distinctions.

b. Detection Data:

Detection = still framed photograph




Data = a description of the photograph


A "detection" is essentially a still framed photograph. "Data" is information about the photograph. In a technical sense, the data is simply the digital makeup of the photograph combined with certain descriptions of the photograph. In a practical sense, the "data" is what vehicle related information can be learned from examining the photograph. **Detection data does not contain any Personal Identifying Information (PII).** See section 2 for more information on PII. Operators of an ALPR system must access separate secure systems such as the Department of Motor Vehicles to receive any information regarding the registered owner of a license plate. Knowing the registered owner of the vehicle is a

potential investigative lead, but that alone does not determine who was driving at the time of the detection.

LPR's are designed to photograph vehicles and make calculated assumptions of some of the vehicle's features, of which the license plate is the primary focus. The first assumption made by the system is if the object in view of the camera is a vehicle, if yes, then take a photograph. That photograph is then automatically examined for a license plate. Character recognition software 'reads' the license plate using Optical Character Recognition (OCR) and links the license plate to the photograph. If an occupant is visible in the photograph, nothing about the occupants is evaluated or labeled and stored. **Motorola ALPR technology does not use any form of facial recognition software.** The Motorola software attempts to determine the possible color, possible make, and possible type of vehicle depicted in that single still photograph. This detection data (photo combined with basic characteristics) is stored in Chico's database.

For routine detections (photograph), the following data is typically ascertained

1. License plate and state (if present)
    a. No plate, partial plate, obstructed
2. Possible vehicle make (Ford, Chevy, Dodge)
3. Possible vehicle color
4. Possible vehicle type (car, truck, other)
5) Date/time/location of the photograph (metadata)

The length of time ALPR detection data must be retained is not specified by law. Civil Code §§ 1798.90.51(b)[1]/1798.90.53(b)[2] require that ALPR users create policy indicating their retention practice. CPD policy 450.5 A.1. establishes CPD's retention is for one (1) year. This retention timeframe is based on Government Code §§ 34090.6[3] which allows for the purging of electronic images after one year (1). All CPD detections are stored on a rolling 365-day basis (photos and descriptions perpetually deleted 366 days after the detection was recorded).

---

[1] Cal. Civ. Code § 1798.90.51(b), *California Legislative Information*, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.90.51
[2] Cal. Civ. Code § 1798.90.53(b), *California Legislative Information*, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.90.53
[3] Cal. Gov't Code § 34090.6, *California Legislative Information*, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=34090.6

c. Archival Transaction logs:

Many of the functions of Vehicle Manager 8.0 are tracked and logged by the system. This archival data is reduced to its barest form and is utilized to record things like search parameters, user's actions, settings, user profile changes, camera settings etc. Transaction log data is not the same as detection data and contains no meta data associated with the vehicle. Transaction log data can be retrieved via the auditing functions incorporated into Vehicle Manager 8.0. Many of these auditing functions are decidedly not user friendly and are distinctly designed for technical support interactions. Transaction data is retained for 10 years. For example, a transaction log can indicate that a user conducted a search on a certain date of a certain plate, but the detection data is not present. In order to see the detection the user saw, the auditor would need to return to the search functions of Vehicle Manager 8.0 and conduct the same search the user performed. Yes, this will create another transaction of the auditor's new search, which was an attempt to recreate the search being investigated. Since detection data deletes after one year, any attempt to recreate a search that occurred over a year prior will result in no detection being located. See section 3 for additional information regarding auditing.

d. Technology System Distinctions:

I. Red Light Cameras:

Red Light Cameras are not ALPR devices as related to their function and they do not feed detections into a searchable database, additionally they are not a part of the Motorola ecosystem. The City of Chico operates a red-light enforcement program through a company called Verra Mobility[4]. These systems exist to automate the observation of a vehicle failing to stop at a traffic control device (red-light), a violation of 21453 CVC. The same process would be accomplished by an officer parked at the location. These systems do not act autonomously to issue traffic citations. Potential violations are flagged and sent to a human operator to review the picture and/or video and make a determination if a violation has occurred or not. The potential violation is then sent to a second human operator for additional verification. Every potential violation is reviewed by a human who must take additional steps before issuing a citation. Essentially, the camera captures evidence of the violation, a human interprets the evidence, a second human interprets the evidence, a human causes the issuance of a citation, then a human appears in court to present the evidence. Although some of these systems may utilize Optical Character Recognition (OCR) to 'read' a license plate, the photos or videos do not feed into a database as a detection, and they are not searchable like ALPR data. Depending upon the proprietary products produced by the individual companies, some of these systems do

[4] Verra Mobility, *Red-Light Safety Solutions*, https://www.verramobility.com/government/red-light-safety/

interface directly with systems such as the DMV or other CLETS/NLETS systems that contain PII.

II. Tollbooths:

These systems can be a combination of technologies like Radio-Frequency Identification (RFID) readers and ALPR. Although these systems can use ALPR technology, they are designed for collecting fees and to monitor other traffic related functions. These systems do collect and store data about vehicles, but retention of that data is usually predicated on when fees are received. Vehicles registered with the system (like FasTrak[5]) can have fees processed quickly and the corresponding data can be purged after payment is received. Vehicle data can sometimes be kept indefinitely for the purposes of debt collection. ALPR cameras used for tolling can participate in an ecosystem with other toll locations. If the toll location is utilizing Motorola equipment, they can opt to allow access to law enforcement at the discretion of the operators of the toll system. Detections would be available to a search by law enforcement only for the period of time the detection is retained by the toll operator. Given that most detections are deleted once payment is received, detection viewing is very limited but still a viable option.

III. Parking Services:

ALPR technology can be used for parking management/enforcement. The application of these systems is different than that of law enforcement but again, if the parking system is Motorola, the vehicle detections by a parking ALPR can be accessed by law enforcement. No information from a law enforcement system is available to a parking system user. The City of Chico utilizes Motorola ALPR for parking enforcement[6] and detections from parking ALPR are accessible to CPD's authorized administrators and users. The parking enforcement ALPR system is managed by the City's Engineering Department and not the Police Department. The parking system users primarily engage in "digital chalking" of vehicle locations, which is cross referenced to the data collected at a parking kiosk or a smart phone application. The parking system can detect unregistered vehicles and send alerts about vehicles that have not paid previous parking citations[7]. The system interface is completely different to that of a law enforcement ALPR system and parking system users cannot search through a database of previous detections nor do they receive law

[5] Bay Area Toll Auth. / FasTrak, *FasTrak — Home*, https://www.bayareafastrak.org/en/home/index.shtml
[6] Motorola Solutions, *LPR for Parking Enforcement Brochure*, https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/lpr-for-parking-enforcement-brochure.pdf (last visited Sept. 6, 2026).
[7] Cal. Veh. Code § 22651(i)(1) (West 2025) (authorizing impoundment of a vehicle known to have been issued "five or more notices of parking violations" that remain unresolved, or five or more notices for failure to pay or appear on traffic violations).

enforcement related ALPR alerts directly. Should a parking ALPR detect a vehicle wanted by law enforcement, the alert is sent to the Police Department and not the parking enforcement user. ALPR detections generated by parking services cameras are stored in their database for 14 days. CPD's ALPR system has shared access to the parking ALPR database through the Motorola ecosystem. Parking detections are not fed into CPD's database, they are available for up to 14 days when a search is conducted. If a CPD user conducts a search for a vehicle for a timeframe greater than 15 days, there will be no parking services detections to be viewed.

IV. Private Security/Access Control ALPR:

These systems are truly ALPR systems in the traditional sense, but they are privately owned and operated. Motorola (and Flock) offer privately owned systems for monitoring vehicles by private entities such as retail outlets, HOA's, casinos, sports arenas, parking lots, and airports. These systems do not automatically feed into a law enforcement database but do have the option to allow access to detections if the system is of like kind. Private systems do not have access to detection data from law enforcement only systems. An example of this technology is marketed by Motorola through its Avigilon subsidiary[8]. The Avigilon platform hosts a variety of camera solutions and can support the same LQ6[9] model ALPR cameras currently marketed to law enforcement. Similar to the parking application of ALPR technology, the user interface and database is distinctly different from law enforcement.

V. Surveillance Cameras:

**These are not ALPR cameras**. A surveillance camera, publicly or privately owned, is not an ALPR camera and does not feed vehicle detections into a searchable database. The Motorola ALPR system does not receive detection data from surveillance cameras. Motorola (and Flock) do manufacture and sell surveillance cameras. Motorola surveillance cameras operate via a separate platform named Avigilon. Surveillance cameras allow for live feed viewing and or to record surveillance footage. Retention of video footage can vary and the capacity to search the data is also dependent on the system's capability. Privately owned surveillance footage can be shared with law enforcement at the discretion of the operators or owners. The City of Chico owns and operates numerous surveillance cameras through the Avigilon platform, some of which are in public spaces. CPD can access and

[8] Avigilon (a Motorola Solutions company), *Automatic License Plate Recognition Systems | ALPR Software*, https://www.avigilon.com/license-plate-recognition-solutions

[9] Motorola Solutions, *L6Q Quick-Deploy LPR Camera System Data Sheet* (2025), https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/l6q-quick-deploy-lpr-system/l6q-quick-deploy-lpr-camera-datasheet.pdf.

utilize this footage as needed but it is not ALPR detection data. Footage needed for investigations or evidence is downloaded from the system and stored indefinitely in our Evidence department. All routine video footage recorded by the City has a legally required retention of one (1) year[10]. Retention for one (1) year is a minimum standard, and settings can vary based on system capacity to be stored longer. According to Chico's IT department, City owned surveillance camera storage servers are built with the capacity to store up to two years of data for each camera currently operating. This technical capacity allows for potential adding of cameras without the need to upgrade storage capacity. According to IT, there is no defined process for deleting video footage at a certain time, they have only ensured the footage isn't deleted too soon in order to comply with Government Code §§ 34090.6.

## VI. ALPR for Law Enforcement:

These systems are designated for law enforcement purposes to enhance public safety and create efficiencies. Generally speaking, the physical infrastructure (cameras/equipment/database) of a law enforcement ALPR system and a non-law enforcement system are virtually the same, in the instance of Motorola, Vehicle Manager 8.0 is the platform for law enforcement ALPR management while Avigilon is the ALPR manager for private entities. The differences between law enforcement and private ALPR systems appear when discussing the capabilities of the software supporting the systems, the databases, and the sharing relationships between other ALPR systems.

Motorola systems have applications outside of law enforcement and they can overlap in what can be broadly categorized as a one-way relationship. Motorola has created an ecosystem in which data can exist and be transferred between other ALPR systems, if permitted by the user. Individual agencies or private entities can create their own network of ALPR cameras and ingest vehicle detections which are owned and stored (via database) by the originating law enforcement agency or private entity. With permission, a non-law enforcement entity can allow access to a privately owned database of stored detections, but a private entity cannot access a law enforcement database of detections. The Vehicle Manager 8.0 platform is the ecosystem by which the sharing of information is facilitated. A common misconception is that unique agency detections "feed" into a partnering agency's database and vice versa. Access to a database is distinctly different than a continuous uploading of each other's detections. CPD's database does not contain detections from a partnering agency; permissions allow a query of data and then facilitates the transfer only if there is a responsive record.

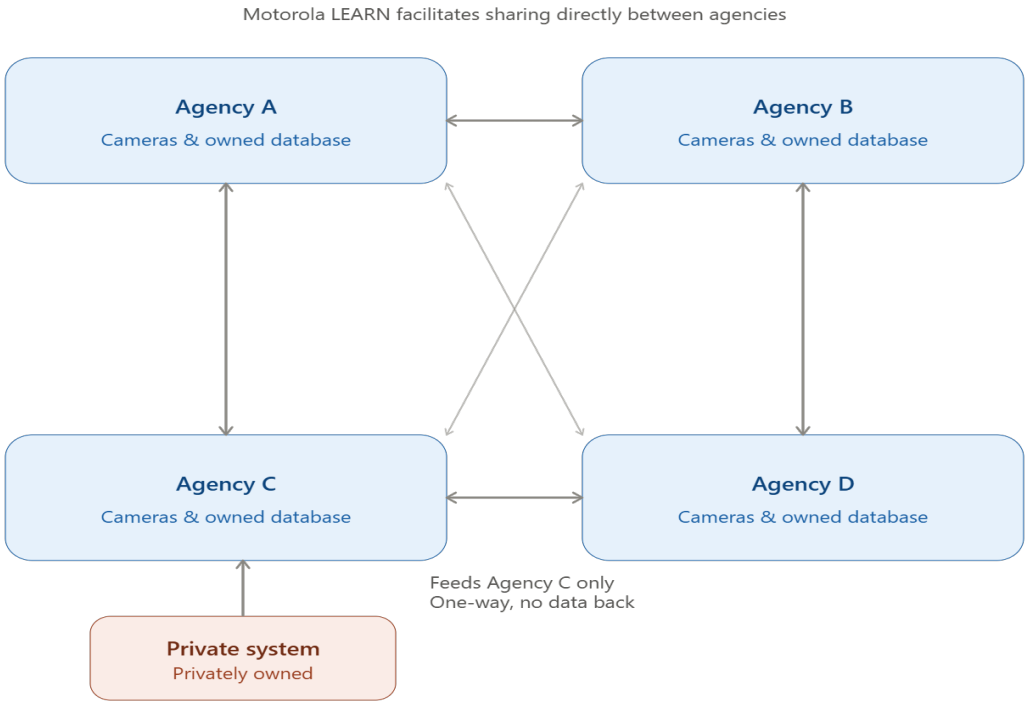
[10] California Government Code § 34090.6

It is not uncommon for a law enforcement agency to operate a Flock, or other, ALPR system for their network, but also pay for access to a Motorola account and vice versa. Although different system manufactures do not overlap, the detection data obtained from any system can still aid in investigations regardless of the system that collected it. For example, the City of Chico operates a Motorola system while the Butte County Sheriff's Office (BCSO) operates a Flock system. CPD and BCSO collaborate daily and routinely share resources and information. It is extremely common for criminal elements to travel across city, county, and state jurisdictions. It would be ideal for sharing to occur between the two platforms but that isn't the current situation. **The Motorola ecosystem does not interface with Flock and CPD does not have access to the Flock platform.**

e. ALPR Sharing MOU (Ecosystem):

Motorola agencies can elect to operate their system as a standalone network or can engage in a 'sharing' relationship with another Motorola agency. These relationships are formed through memorandums of understanding (MOU)[11] between the participating agencies. Agencies can elect any combination of sharing their data and/or receiving data from another participant. CPD expressly owns the detection data and independently stores it separately from all other entities and agencies. Every photograph a CPD camera captures goes into a CPD file that CPD owns. All other Motorola system operators have their own cameras capturing photographs that they exclusively own. For illustrative purposes, CPD places all our photos into a bucket and only CPD can look into CPD's bucket. All other Motorola entities place their photos into their buckets for only their use. If CPD wants to look into another bucket, or if someone wants to look into CPD's bucket, each party must agree to the terms (in an MOU) by which someone gets to look. The MOUs between agencies serve as terms of use agreements for looking at each other's detections.

[11] Vigilant Solutions, *Memorandum of Understanding Between Agencies: License Plate Recognition (LPR) Equipped Law Enforcement Agencies for Sharing LPR Detection Data and Hotlists* (system-generated template document, LEARN platform) (on file with author).




For the purposes of understanding the concept of "sharing data" it is important to distinguish between an inquiry for data and the actual receiving of data. A statewide inquiry by a user of the Vehicle Manager 8.0 platform will register as a search of Chico's records regardless of Chico's database containing a detection that is relevant to the inquiry. This can often be misleading as an inquiry into Chico's detections does not automatically indicate Chico's detections were the focus of the inquiry or that a Chico detection was shared. The data logs will record all requests for responsive records regardless if Chico's system has any responsive records.

f. <u>Flock:</u>

Flock took a similar approach to data storage and ownership with an important distinction called data anonymization. The process of anonymizing essentially strips data sets of their context. This is a common practice with data, not just digital data. For example, a hospital might collect very detailed patient records but anonymize the data to show only the total number of patients treated, types of treatments, or breakdown demographics of a patient pool with no link back to the individual identities of those patients. An example of anonymizing data in law enforcement can be found in SB 953, The Racial Identity and

Profiling Act (RIPA)[12]. This statutory requirement created a process by which all police detentions are tracked and sent to a central database for further study. Prior to the data being transferred, all information that could correlate the detained person's identity (PII) to the detention circumstances is anonymized, leaving only very specific circumstance information to be transferred.

Flock subscribers have a similar ecosystem to that of Motorola and individually own and store their data, however; Flock went a step further by "anonymizing" the collected data and pushing it beyond the Flock user ecosystem and into a central repository for the company's use. At face value, Flock and Motorola operate similarly until anonymized data is pushed beyond the Flock ecosystem to a private data pool. For the purposes of this report and Flock's business practices staff have not investigated exactly how detected data is anonymized and what that means regarding privacy. This dynamic is technically complicated and legally nuanced but seems to be at the heart of the Flock controversy, specifically why Flock wants the data and what can be done with anonymized data.

g. Motorola:

Motorola Solutions is a global leader in public safety and enterprise security, providing mission-critical communications, video surveillance, and secure command center technologies. Both encrypted and unencrypted Motorola radio systems have been the backbone of countless public and private organizations. The City of Chico is currently in the process of finalizing a state-of-the-art Motorola P25 digital radio network. The long-standing successful relationship with Motorola is one of the primary reasons for selecting Motorola as the source and host of CPD's ALPR program. Motorola does not capture any vehicle data for their own use, nor will they ever use the data for their own purposes or for enhancing A.I. machine learning models. All data obtained by Chico's ALPR system is hosted by Motorola's cloud-based Microsoft Azure servers which are CJIS compliant[13] and the industry standard for government databases. The data obtained through the Motorola system is specifically owned by the City of Chico, unlike Flock wherein Flock owns the data they collect from their subscribers.

---

[12] Cal. Gov. Code § 12525.5(d) (West 2025) (prohibiting law enforcement agencies from reporting the name, address, social security number, or other unique personal identifying information of a stopped person to the Department of Justice, and prohibiting the Department from releasing to the public any unique identifying information of the reporting officer).

[13] Motorola Solutions, Inc., *Vigilant LEARN CJIS Security Compliance Guide* (Chicago: Motorola Solutions, 2022), https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/vigilant_learn_cjis_security_compliance_guide.pdf.

h. Computer programs (automation) and A.I.:

The term A.I. has broad implications and is widely misunderstood. There are technical delineations between conventional 'hard code' programs that follow a set of predefined instructions (rules) and A.I. models (machine learning). Spellcheck is a traditional program that rapidly displays what a user types incorrectly against a list of words spelled correctly. As this capability became more sophisticated, predictive text in addition to just checking spelling was added. The program began providing suggestions for the words the user was most likely typing and offered to finish the word. Predictive text could be perceived as A.I. by "predicting" what the user is typing versus responding to what was already typed and comparing it to a known list. In reality, predictive text is still comparing what was typed against a list of what could be typed. In other words, the results (predictions) are bound by known fields on both sides, what is being typed versus all possibilities of what could be typed. If "X" is input, then "Y" are the possible results. Spellcheck and predictive text are really effective programs but are not A.I.. True machine learning is only limited by the size of the database it can reference to produce a result, but it is not bound by fixed input output rules. At some point, the tech industry started branding really good programs as A.I. mostly for marketing purposes. A.I. became the wave of the future and just about everything started being labeled as being A.I. enhanced. Conventional email accounts now ubiquitously have an A.I. assistant. Google and Yahoo search engines now provide an A.I. result to a conventional search.

An important distinction when discussing A.I. is the difference between A.I. models built for a specific purpose and generative A.I. models. A purpose-built A.I. application can only accomplish tasks it is designed to complete, such as generating video, enhancing digital photographs. A purpose-built A.I. model used to enhance photographs cannot be asked to produce an essay. Generative A.I. on the other hand is not restricted to only specific tasks (although still limited). Depending on the system, it can write an essay, complete internet searches, and generate graphics all from one interface.

Motorola ALPR products do have purpose-built A.I. enhanced capabilities. These A.I. enhanced functions are contained within the system and are used to enhance detections and sort data. The A.I. enhanced functions in the Motorola ALPR system do not source from the internet and do not use customer data to enhance its machine learning database. Specific to Motorola, A.I. enhancement is apparent in two ways, the first is in the identification of vehicle information in a detection, the second is through the use of the "Assist" feature in Vehicle Manager 8.0. ****NOTE: The Assist feature has never been activated for CPD's ALPR system. No CPD users have permission settings to utilize Assist and cannot self-enable the feature. ****

**Detections:** A purpose built A.I. model process the detection and attempts to determine a make, model, and color of a detected vehicle. There is nothing generative about this process. The A.I. model uses its understanding of vehicle makes, models, and colors to label what is present in the photo. The Motorola system does not use CPD's data to enhance the abilities of its A.I. model.

**Assist**: Via the Vehicle Manager 8.0 platform, there is a search tool called Assist. Asist is a purpose built A.I. enhancement similar to what is used in the detection process. This feature allows the user to enter free text search criteria as a method of searching detections. For example, a user could type something to the effect of "large white truck with picture of a clown on the side." Although "white" and "truck" might be a part of the detection's original description, "large" and "picture of a clown on the side" are not. A.I. will attempt to define what "large" means as well as what could be a "clown." Additionally, A.I. would need to determine what qualified as the "side" of the vehicle. None of these search terms are contained in the detection data, but they are potentially discernable from analyzing the photographs. The A.I. model will return results to the best of its ability to follow the prompts, but it will not generate any original content, and it cannot take any independent action.

If a potential suspect vehicle is identified using this feature, it is a static return and does not create a hotplate or alert officers to stop this vehicle. A user could potentially learn a previously unknown license plate for this suspect vehicle and use that information as a lead in their investigation. It is extremely common for victims and witnesses to remember specific details about a suspect vehicle but never see (or remember) the license plate. **Despite the obvious utility of this capability, CPD elected not to utilize advanced A.I. features given the unsettled legalities and public sentiment surrounding A.I. and Facial Recognition technology.**

i. <u>Facial Recognition:</u>

**Motorola ALPR products and software do not contain any facial recognition technology**. Facial recognition technology is truly A.I. in the fact that it doesn't follow rule-based outcomes. The program must first devise some (proprietary) method of assigning unique values to a variety of human facial features before it can search other faces for those features. Typically, a face is presented to the system as the reference (photograph or video of a person's face). That baseline photo or video of the subject is turned into some type of unique digital "faceprint." The system would then need to look at other photos or videos to see if the same digital face "faceprint" is found. Although facial recognition is A.I., and is ubiquitously present in smart phones, laptops, and passport portals, it is

typically narrowed to that singular function. Facial recognition software doesn't typically get repurposed to compose essays or write poems. Additionally, results of facial recognition searches still return to a human operator to determine accuracy and significance.

j. Hotplates and Hotlists:

The Motorola ALPR system is not connected to any other databases, including DMV, and does not contain or access any PII. Through a process called "Hot listing" licenses plates detected by the system can be compared against specific data such as a list of stolen plates, missing persons, criminal suspects, etc. These plates are commonly referred to as "Hot Plates" because they have been sent to a hot list. The hot lists do not contain any PII but rather are the mechanism by which the ALPR system is isolated from the larger databases that do contain PII. By hot listing plates, agencies can collaborate in an attempt to locate these vehicles. Hot lists and hot plates are not new and were not developed because of ALPR technology. Hot lists operate in the same way regardless of a human running the plate at their computer or over the radio via dispatch. Once the plate is searched through state or national systems, it is automatically compared to the hot lists. Vehicle license plates that match those on a hot list are what is termed a "Hit." A hit is simply a match to a known list of wanted license plates.

The Motorola ALPR system utilizes the hot list concept in two ways. The first is the traditional crosschecking of a detected plate against the hot list of wanted vehicles in state and national databases. This traditional hot list reference is automated and does not require a person to request the check via a different system. The second is a local hot list that exists only inside the Motorola ecosystem. A Motorola user can enter a hot plate into a local hot list. The local hot lists are not linked to state or national systems, but the local hot plates can be shared with other agencies within the Motorola ecosystem. This is referred to as "hot list sharing." The local hot plate feature is typically utilized when the want on a vehicle does not rise to the level of a statewide or nationwide entry or for specific investigative reasons there is no need to have an agency (or officer) unfamiliar with the vehicle take action based on the hot plate alert.

A local hot plate, can list the reason the vehicle is wanted and typically what to do if the vehicle is found. However, unlike a hit from a state or national hot plate, a local hot plate hit is not independent justification for taking action. A local hot plate hit will provide instructions to the officers on how to proceed if they are legally able to do so. A hit from a state or national hot plate (such a stolen plate) is valid probable cause to stop the wanted vehicle. For example, if the ALPR system detects a stolen vehicle and the hit is sent to an

officer, the officer's first obligation is to run the license plate through a state or national system as independent confirmation of the hit. Even though the ALPR hit originated from a state or national hotlist, the hit still needs to be confirmed[14].

k. Detection Browsing and Detection Viewing:

Detection – Photos and corresponding metadata; function of the system.

Detection Browsing- The act of searching detections; conduct of a user.

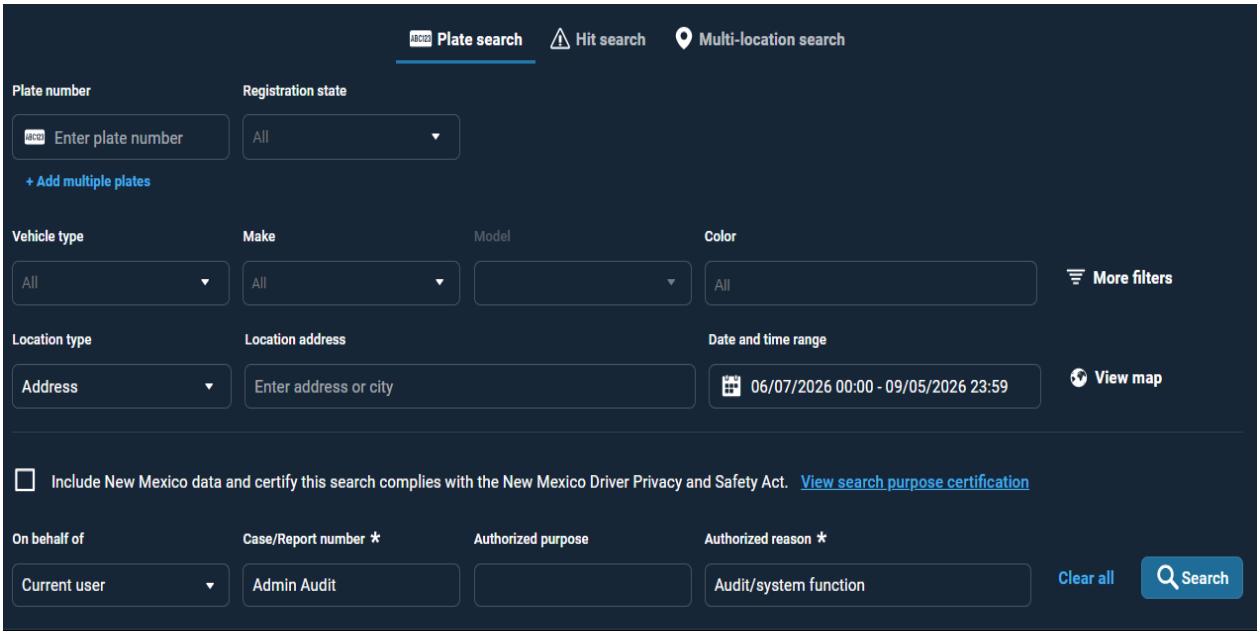
Detection Viewing- The act of viewing a detection return; conduct of a user.

A detection is a vehicle's photograph potentially labeled by license plate, possible make, possible color, etc. Every time a vehicle passes by an ALPR, a detection is registered and stored in Chico's database. The Chico ALPR system generates approximately 7 million detections per month across all the cameras. Detections are not searches of plates by users of the system. One is a function of the system while the other is the action of the user. Any statistic number that is represented as a "detection" only depicts a number of photos in the system. For example, an ALPR system could record one million detections, but zero searches could be conducted by system users. Simply looking at the total number of detections in the system does not tell the whole story. The number of detections can illustrate the vastness of data, but it indicates very little about how the information is viewed or utilized.

The act of searching for a vehicle is called "Detection Browsing." Detection browsing is a search of vehicles that have already been detected by the system (a search of detections that have already occurred). Essentially, by entering the license plate, the user is filtering the existing detections for the plate they need to see.

[14] Chico Police Department, *Policy Manual*, Policy 450 — Automated License Plate Readers (ALPRs), § 450.4(f) (Lexipol, LLC, rev. June 2, 2026).

Search Interface




If a search for the desired license plate returns 1 detection or 1000 detections, those are not views. Only one search may be conducted by the user, but multiple possible detection returns may be received. The number of returns is a function of the system, not conduct of the user. Any number represented as a detection return only depicts how many photos potentially match the search criteria. The return is simply indicating that 1, 100, or 1000 detections of that queried license plate exist within the available one-year cache of detections. For example, if multiple lanes of a single intersection are covered, a single vehicle might get detected twice at that intersection after passing through one time. The number of detections grows from there based on how many cameras are creating detections and how often vehicles pass the cameras. One vehicle can generate a lot of detections while others might not ever pass an ALPR location.

If a user opens one out of 1000 detections, then they have "viewed" only one of those 1000 detections. The number of detections returned is usually higher based on the fewer filters selected by the user. For example, if the user searches for a full one-year period, all cameras, all times, for all vehicles, they are probably going to receive tens of thousands of detection returns. Conversely, if the user searches for a specific license plate, on a single day, during a specific timeframe, they will receive a lot fewer returns.

Understanding detections vs. detection browsing vs. detection viewing is important for understanding the audit process and the various logs tracked by the system. Large numbers of detections can appear compelling but have very little to do with user's

conduct. A large number of detection returns after a single search can also appear significant but can still be misleading if none or just a few of the detection returns are viewed by the user. For example, if a federal agent in Oklahoma uses wide-open filter settings and searches only a partial plate "123" there is an extremely high likelihood the data log will indicate thousands of records from the City of Chico, as well hundreds of thousands across the nation. If the agent in Oklahoma sees there are a large number of potential returns but never opens any of them, then zero views occurred. A search has occurred, but the results were never viewed. The agent could then narrow the search terms to only vehicles within Oklahoma, City of Tulsa, date range of 6/15/26 to 6/16/26, which would result far fewer results, none of which were from the City of Chico. For the first example, a potential audit trail would show a single search by the Federal agent with a number indicated tens of thousands of returns from Chico. If the agent never viewed any of the returns, then the audit trail would stop there. In the second example, there would be no audit trail for CPD to see because the agent's second search excluded the City of Chico's system. Only the audit logs from the user's federal agency would have any further information about the second search.

**2. Personal Identifying Information (PII) and Databases:**

PII is generally defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII are a driver's license, social security number, passport, arrest records, and fingerprints.

There are numerous databases utilized by the government in general and by law enforcement. Each local agency typically has a Computer Aided Dispatch systems (CAD) and a Records Management Systems (RMS). These systems are generally owned, operated, populated, and maintained at the individual agency level. These systems retain the 'history' of an agencies calls for service, address history, arrest history, person contact history, and written reports. In general, these systems are isolated to the agency that operates them. These local systems independently host large amounts of Personal Identifying Information (PII).

Separate from local CAD/RMS, several other databases are operated and maintained by the State of California, such as the Department of Motor Vehicles (DMV), Wanted Persons System (WPS), Missing and Unidentified Persons System (MUPS), Domestic Violence Restraining Order System (DVROS), Automated Firearms System (AFS), and the Stolen Vehicle System (SVS). The California Law Enforcement Telecommunications System (CLETS) allows for the rapid exchange of information between agencies.

Other states operate in a similar fashion as California with a variety of their own databases. The federal government also maintains databases and at times acts as a central repository of certain types of information. Examples of federal systems are the Criminal Justice Information System (CJIS), Interstate Identification Index (III), and National Data Exchange (NDex), National Crime Information Center (NCIC), and Federal Aviation Administration (FAA). As with the local and state databases, these federal systems often maintain a large amount of PII. The National Law Enforcement Communication system (NLETS) allows for the rapid exchange of information between states and between the states and the federal government.

Using one or both of the exchange systems CLETS or NLETS, law enforcement can transfer certain qualifying information to agencies within the state, or agencies around the country. A relevant example of usage of these systems would be stolen vehicle data. A local agency can enter a stolen vehicle's information into the Stolen Vehicle System (SVS), which then feeds into CLETS, which then feeds into NLETS. This exchange of information allows other agencies to collaborate in an attempt to locate and recover the stolen vehicle.

### 3. Auditing:

Auditing is the act of verifying or independently examining a system, process or function. For the purposes of ALPR programs, auditing can take many forms. Assessing or reviewing the system's settings (access/retention/hotlists), MOU's (sharing), user conduct (searching), and system's function (detections) are all examples of audits. California Civil Code 1798.90.51 (b)(2)(C), commonly known as SB-34, broadly outlines that an agency must monitor the security of information and compliance with privacy laws. The statutory auditing requirements don't specify audit frequency, methodology, who performs it, how to document it, or who reviews the results. This leaves the process up to the individual agencies operating an ALPR system. Auditing is a process occurring after the fact as opposed to active monitoring in real time or some type of tiered supervisory approval prior to a search being conducted. Statutorily required auditing should not be confused with statutorily required security protocols, user permissions, access rights, or data security. Auditing will always be a passive tool for discovering issues leading to corrective measures.

a. <u>CPD's Audit Methodology</u>:

The CPD ALPR audit process involves several distinct operations: detection browsing, external data requests, allied agency MOUs, retention settings, system function, and authorized users. Each element of the audit process focuses on either an aspect of the program, function of the system, or conduct of its users. CPD has created an audit

template and implements a monthly frequency of audits for the use of ALPR technology to ensure abuse of the system is not taking place. Below is a description of the detailed audit process in place at CPD.

b. Detection Browsing & Viewing:

An audit of detection browsing and viewing is focused on conduct of CPD's users. This is the most robust and heavily scrutinized auditing function. The Vehicle Manager 8.0 system stores archival transaction logs for each search conducted by a user. The archival transaction log does list plates involved in the user's query, but it does not reproduce the detection data, just a record of the query criteria. These transaction logs are not inherently user friendly and do not intuitively provide a picture of conduct to a common viewer. Results are provided on in Excell spreadsheet format with one line per record, but multiple columns comprised of: Query Type, Username, User Type, Case#/LE Report#, Requestor, Query Pars, Date Time, IP Address, ORI, Reason, and Record Count.

For the purposes of understanding the audit, Case#/LE Report#, Query Pars, Reason, and Record Count are the most relevant columns.

**Case#/LE Report#:** is the column in which a user must enter a valid case number, call log number, warrant number, or outside agency number. This column is heavily scrutinized during the audit. When a search is performed, this field is required or a search is not possible however, the field is free text. Case numbers come in many different formats and therefore a forced field is not possible. This allows for anything to be typed into the field, and a search can move forward. In general, if a user enters a badge number or starts a case number "26-" and then never finishes, they can complete the search. During the audit this field is manually examined line by line for anything unconventional. CPD case numbers are readily recognizable as are warrant numbers. Entries that are blank (hit the spacebar) or nonsensical numbers are flagged for clarification from the user to ensure accurate documentation.

**Quary Pars:** is the column that records all the search parameters (filters) selected by the user. This column contains the most data per search of any other column. Several default parameters are inherent (such as 90 days and 50 records) but the user can define the search as needed. This column contains the plate or partial plate that was searched by the user. This column indicates if a specific state registration, a date and time range, vehicle model, or a specific camera was designated. This is also the column that indicates if any of the search results were viewed by the user. When viewing an audit report, seeing search parameters in this column shows what was searched. The next line on the report will not contain search parameters, it will read something to the effect of "View Detection."

The audit report does not generate a separate report for searches conducted and detections viewed. It is very common to see a single search followed by numerous "View Detections" of the same plate. This is typical behavior of a user and not an indication of misuse. The user searched a plate for a reason and then should view the detection. A search line that does not have "View Detection" adjacent to it is usually indicative that zero records were available to view.

During this portion of the audit process, anomalies are scrutinized and clarification is sought from the user, but additionally, spot checking of acceptable searches is also conducted. Despite seeing nothing noteworthy in the transaction logs, staff routinely select approximately 10 searches and cross check CPD's records management system to determine if the vehicle searched is associated with the case number provided by the user.

Automated Verification: While preparing this report, staff had several conversations with IT staff and some efficiency ideas manifested. Currently, an in-house program is being developed by Chico IT that can automatically compare all transaction logs of searches against CPD's records management system in order to streamline the audit process. The use of a CPD case number is not the only type of acceptable case number, but an automation of this type would drastically increase the efficiency of the spot-checking process. There is no requirement to complete a spot-checking process, but it undoubtedly enhances the oversight of ALPR usage and CPD prioritizes adding this method as an additional audit and oversight of the program and users.

**Reason:** This column logs the reason the user is conducting the search. As with Case#/LE Report#, this column is heavily scrutinized as it is another major indicator of user conduct. Prior to conducting a search, the "Reason" is required before a search can proceed. This is another free text field and does not follow a forced format. Vehicle Manager 8.0 does allow for forced format fields (pick lists) to be populated, but CPD did not select to use this feature. Picklists inherently push all reasons into an acceptable category and can mask conduct. Free text fields allow users to be more (or less) specific, provide unconventional reasons and are a better indicator of the users' conduct. Too little information such as "investigation" is easily spotted and clarification can be sought. Additionally, blank fields (spacebar) are easily spotted, and clarification (including training, up to and including discipline for consistent reoccurrences) can be coordinated with the user.

**Records Count**: This column is where the transaction logs record if any detections are present in the system that match the query performed by the user. If a plate is searched and that plate has never been detected, then the number in this column is zero. When auditing the activity of a Chico user, it is normal to see this number in the hundreds

because most searches by users in Chico involve vehicles present in Chico. When viewing an audit report of an outside agency, it is extremely common to see a zero because the agency conducted a state or nationwide search. When related to conduct of users, wide open searches of this kind are not a search of Chico's database, they are a request to know if Chico has any records matching the search query. A zero is an indication that a Chico ALPR has never detected the vehicle being searched.

c. External Data Requests:

This segment of the audit focuses on request for ALPR data that occur outside of the Vehicle Manager 8.0 platform. Agencies with shared access (via MOU) can query Chico records via the system. Agencies that do not operate a Motorola system can contact a CPD user and inquire if Chico's system has detected a vehicle. This process is a request for records by another agency. The ALPR policy (450) outlines the records release process and requires written documentation of the request and approval by a lieutenant or above.

During an audit of this segment, any search indicating it was done for an outside agency is matched with the corresponding written request and lieutenant approval (usual via email). Clarification is sought from the user on any search that doesn't appear to have the proper documentation and approval.

d. Allied Agency MOUs:

This segment is done on a continual basis and during the monthly audit process. MOUs are exchanged digitally via Vehicle Manager 8.0. Upon receiving a request for access, the system administrator is notified both by email and withing Vehicle Manager 8.0. This prompt is the first level of review, and it can be easily determined if the requestor is within CPD's acceptable share group. Prior to 7/8/26, this share group was California, Oregon, Nevada, Arizona and federal agencies. If the agency fell outside of this sharing group, then the request was not accepted. If the agency fell within the sharing group, then it was accepted. During the monthly audit, a second check of MOUs is conducted. Inside Vehicle Manager 8.0, all MOUs can be sorted by state. This check only takes moments and is one of the easier tasks to perform. Any MOU not within the share group can be easily spotted.

Post 7/8/26, all MOUs fall solely within California. Vehicle Manager 8.0 has a feature to automatically exclude all share requests outside of California. This feature is now enabled and CPD no longer receives requests for out-of-state or federal agencies. A monthly review of MOU's is still conducted as further confirmation.

e. Retention Settings:

This segment is done monthly and again only takes moments to verify that all record retention settings are set to the appropriate timeframes. These settings do not automatically change, but verification is still good practice.

f. Authorized Users:

This segment is conducted continuously and monthly. User profiles are automatically set to inactive if the user has not logged into Vehicle Manager 8.0 for 90 days. Additionally, CPD notifies all system administrators citywide when an employee separates employment. Perpetually, when these separation notices are received, the user is removed from Vehicle Manager 8.0 shortly thereafter. In the event a separation notice is missed, the monthly check of authorized user reveals the need to remove the user. If both the separation notice and the monthly checks miss the need to remove a user, then the automatic 90 inactive user is a tertiary safeguard.