

FAQs

What is ALPR, and how does it work?

- ALPR technology uses a combination of cameras and computer software to scan the license plates of passing vehicles. These computer-readable images of license plates enable police to compare plate numbers against those of wanted vehicles and vehicles associated with wanted individuals and missing persons. ALPR cameras focus is on rear license plates only and are not designed to capture images of vehicle occupants or utilize facial recognition technology.

What are the uses and benefits of ALPR technology?

The use of ALPR technology offers several benefits, including crime deterrence, real-time alerts to police when stolen or wanted vehicles enter an area, and enhanced investigative capabilities in the event of a crime having already occurred.

Deterrence: Even if officers are unable to locate and stop the vehicle in question, suspects may see the police response and be deterred from further criminal activity. Indeed, the mere presence of the ALPR cameras, visibly mounted on public infrastructure and potentially accompanied by signage, may act as a deterrent. Police personnel have reported to staff that some criminals will intentionally target jurisdictions without ALPR technology to increase their chances of successfully avoiding detection while committing crimes.

Real-Time Alerts: When a real-time ALPR alert occurs, notifying police of the presence of a wanted or stolen vehicle, officers can respond to the area to search for the vehicle. If officers locate the vehicle, prior to making an enforcement stop, they visually confirm the plate number and manually check it against law enforcement databases to confirm the accuracy of the ALPR information and the legal justification for the stop.

Solve Crimes Already Committed: In addition to providing opportunities to prevent crime and apprehend wanted persons via real-time alerts, ALPR data is used by investigators to solve crimes that have already occurred. Typically, by the time a crime is reported to the police, the suspects have already fled the area, and it is the police's job to identify and locate them at a later time. While victims and witnesses can often provide responding officers with a description of the vehicle used by a suspect, those descriptions are frequently incomplete (e.g., a partial license plate number, vehicle type, and color only) or consist of a license plate number that corresponds to a stolen vehicle or a stolen plate. Investigators can turn that imperfect or incomplete information into actionable leads by querying the ALPR database.

What information is captured by ALPR technology?

- The system captures the following information:
 - Date, time, and location
 - License plate (including the state, the plate number or partial plate number, or the absence of a license plate)
 - Vehicle characteristics (the make, model, type, and color)
 - A photo of the vehicle showing the license plate

What information is NOT captured by ALPR technology

- Facial recognition
- People
- Gender
- Race

Acceptable Use

- Data is used for law enforcement purposes only. Data is owned by Sacramento State PD and is never sold to third parties or shared with campus entities for use in employment disciplinary action.

Prohibited Uses

- Immigration enforcement, traffic enforcement, harassment or intimidation, usage based solely on a protected class (i.e., race, sex, religion), or personal use.

What sort of privacy safeguards exist?

The Police Department is mindful of privacy concerns that some community members may have regarding ALPR technology and the data that it collects. The Police Department took those concerns into account when proposing how the use of ALPR technology could be implemented at Sacramento State.

The use of ALPR technology is specifically regulated by California Civil Code §1798.90.5, et seq.

The Department's policies and training satisfy the requirements of all of these statutes.

The Police Department has ensured that ALPR cameras are positioned to focus on the rear license plates and are not positioned to capture images of vehicle occupants or utilize facial recognition technology.

Data captured by ALPR technology is automatically purged after 1 year, unless a specific record has been identified as relevant to a specific criminal investigation. (Government Code §34090.6)

Data obtained from ALPR technology is only accessible to appropriately trained staff with a legitimate law enforcement need. All queries are logged and subject to audit. This is consistent with decades-long legal standards of access to other law enforcement computer databases, like driver's license information, vehicle registration information, and criminal history records. Unlawful use of law enforcement computer databases is against state law and subjects personnel to civil and criminal liability as well as discipline up to and including termination.

ALPR data is transmitted and stored in an encrypted format, consistent with industry-standard Criminal Justice Information System (CJIS) security protocols.

Does ALPR technology provide constant surveillance of members of the public?

No. ALPR technology only provides authorized law enforcement personnel with information about a vehicle located on a public roadway for a single moment in time at a single location. This information is used solely by law enforcement to provide potential leads that support criminal investigations.

Is every ALPR image reviewed?

No, images are only reviewed by law enforcement personnel when required and based upon a law enforcement investigation.

Is ALPR data shared for the purpose of immigration enforcement?

No. No authorized law enforcement user or agency may access California ALPR databases for the sole purpose of immigration enforcement. In gathering, sharing, and storing information, California law enforcement agencies comply with all applicable laws, rules, and regulations, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 et seq.). Each California law enforcement agency, consistent with California Government Code Sections 7282, 7282.5, and 7284.8 (b), works to ensure that databases are governed in a manner that limits the availability of information therein to the fullest extent practicable and consistent with federal and state law, to anyone or any entity for the purpose of immigration enforcement.