

41-6a-2001 Title.

This part is known as the "Automatic License Plate Reader System Act."

Enacted by Chapter 447, 2013 General Session

Effective 1/1/2025

41-6a-2002 Definitions.

As used in this chapter:

- (1) "Active criminal investigation" means an officer has documented reasonable suspicion that a crime is being or has been committed, and believes the suspected criminal activity may be connected to a vehicle, a registered owner of a vehicle, or an occupant of a vehicle.
- (2) "Automatic license plate reader system" means a system of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert an image of a license plate into computer-readable data.
- (3) "Captured plate data" means the global positioning system coordinates, date and time, photograph, license plate number, and any other data captured by or derived from an automatic license plate reader system.
- (4)
 - (a) "Governmental entity" means:
 - (i) executive department agencies of the state;
 - (ii) the offices of the governor, the lieutenant governor, the state auditor, the attorney general, and the state treasurer;
 - (iii) the Board of Pardons and Parole;
 - (iv) the Board of Examiners;
 - (v) the National Guard;
 - (vi) the Career Service Review Office;
 - (vii) the State Board of Education;
 - (viii) the Utah Board of Higher Education;
 - (ix) the State Archives;
 - (x) the Office of the Legislative Auditor General;
 - (xi) the Office of the Legislative Fiscal Analyst;
 - (xii) the Office of Legislative Research and General Counsel;
 - (xiii) the Legislature;
 - (xiv) legislative committees, except any political party, group, caucus, or rules or sifting committee of the Legislature;
 - (xv) courts, the Judicial Council, the Administrative Office of the Courts, and similar administrative units in the judicial branch;
 - (xvi) any state-funded institution of higher education or public education;
 - (xvii) any political subdivision of the state; or
 - (xviii) a law enforcement agency.
 - (b) "Governmental entity" includes:
 - (i) every office, agency, board, bureau, committee, department, advisory board, or commission of an entity listed in Subsections (4)(a)(i) through (xviii) that is funded or established by the government to carry out the public's business; or
 - (ii) a person acting as an agent of a governmental entity or acting on behalf of a governmental entity.
- (5) "Nongovernmental entity" means a person that is not a governmental entity.
- (6) "Secured area" means an area, enclosed by clear boundaries, to which access is limited and not open to the public and entry is only obtainable through specific access-control points.

Amended by Chapter 251, 2024 General Session

Effective 10/14/2025

41-6a-2003 Automatic license plate reader systems -- Restrictions.

- (1) Except as provided in Subsection (2), a governmental entity may not use an automatic license plate reader system.
- (2) Subject to Subsection (3), an automatic license plate reader system may be used:
 - (a) by a law enforcement agency to access captured license plate data:
 - (i) as part of an active criminal investigation;
 - (ii) to apprehend an individual with an outstanding warrant;
 - (iii) to locate a missing or endangered person; or
 - (iv) to locate a stolen vehicle;
 - (b) by a law enforcement agency to access the Utah Criminal Justice Information System to:
 - (i) verify valid vehicle registration information;
 - (ii) confirm vehicle identification;
 - (iii) verify insurance information; or
 - (iv) identify a stolen vehicle;
 - (c) by a governmental parking enforcement entity for the purpose of enforcing state and local parking laws;
 - (d) by a parking enforcement entity for regulating the use of a parking facility;
 - (e) for the purpose of controlling access to a secured area;
 - (f) for the purpose of collecting an electronic toll;
 - (g) for the purpose of enforcing motor carrier laws;
 - (h) by a public transit district for the purpose of assessing parking needs and conducting a travel pattern analysis;
 - (i) by an institution of higher education as described in Section 53H-1-102:
 - (i) for a purpose described in Subsections (2)(a) through (e); or
 - (ii) if the data collected is anonymized, for research and educational purposes;
 - (j) by the Utah Inland Port Authority, created in Section 11-58-201, or by a contractor of the Utah Inland Port Authority with the approval of the board of the Utah Inland Port Authority, if:
 - (i) the automatic license plate reader system is used only within a project area, as defined in Section 11-58-102, of the Utah Inland Port Authority;
 - (ii) the purpose of using the automatic license plate reader system is to improve supply chain efficiency or the efficiency of the movement of goods by analyzing and researching data related to commercial vehicle traffic; and
 - (iii) specific license plate information is anonymized; or
 - (k) by an international airport owned by a governmental entity for the purpose of promoting efficient regulation and implementation of traffic control and direction, parking, security, and other similar operational objectives on the airport campus.
- (3) A law enforcement agency may not use an automatic license plate reader system unless:
 - (a) the law enforcement agency has a written policy regarding the use, management, and auditing of the automatic license plate reader system;
 - (b) for any stationary device installed with the purpose of capturing license plate data of vehicles traveling on a state highway, the law enforcement agency obtains a special use permit as described in Section 72-1-212 from the Department of Transportation before installing the device; and
 - (c) the policy under Subsection (3)(a) and any special use permits granted in accordance with Subsection (3)(b) are:
 - (i) posted and publicly available on the appropriate city, county, or state website; or

Effective 5/3/2023

41-6a-2004 Captured plate data -- Preservation and disclosure.

- (1) Captured plate data obtained for the purposes described in Section 41-6a-2003:
 - (a) in accordance with Section 63G-2-305, is a protected record under Title 63G, Chapter 2, Government Records Access and Management Act, if the captured plate data is maintained by a governmental entity;
 - (b) may not be used or shared for any purpose other than the purposes described in Section 41-6a-2003;
 - (c) except as provided in Subsection (3), may not be preserved for more than nine months by a governmental entity except pursuant to:
 - (i) a preservation request under Section 41-6a-2005;
 - (ii) a disclosure order under Subsection 41-6a-2005(2); or
 - (iii) a warrant issued under the Utah Rules of Criminal Procedure or an equivalent federal warrant; and
 - (d) may only be disclosed:
 - (i) in accordance with the disclosure requirements for a protected record under Section 63G-2-202;
 - (ii) pursuant to a disclosure order under Subsection 41-6a-2005(2); or
 - (iii) pursuant to a warrant issued under the Utah Rules of Criminal Procedure or an equivalent federal warrant.
- (2)
 - (a) A governmental entity that is authorized to use an automatic license plate reader system under this part may not sell captured plate data for any purpose.
 - (b) A governmental entity that is authorized to use an automatic license plate reader system under this part may not share or use captured plate data for a purpose not authorized under Subsection 41-6a-2003(2).
 - (c) Notwithstanding the provisions of this section, a governmental entity may preserve and disclose aggregate captured plate data for planning and statistical purposes if the information identifying a specific license plate is not preserved or disclosed.
- (3) Plate data collected in accordance with Section 72-6-118 may be preserved so long as necessary to collect the payment of a toll or penalty imposed in accordance with Section 72-6-118 and the nine-month preservation limitation described in Subsection (1)(c) shall not apply.
- (4)
 - (a) Except as provided in Subsections (1)(c)(i) through (1)(c)(iii), a governmental entity shall destroy as soon as reasonably possible, in an unrecoverable manner, plate data obtained pursuant to this chapter that is not specifically necessary to achieve the authorized objectives under Subsection 41-6a-2003(2).
 - (b) Subsection (4)(a) applies to data a governmental entity obtains:
 - (i) from a nongovernmental entity pursuant to a warrant; or
 - (ii) from an automatic license plate reader system owned or operated by a governmental entity.

Amended by Chapter 524, 2023 General Session

Effective 5/3/2023

41-6a-2005 Preservation request.

- (1) A person or governmental entity using an automatic license plate reader system shall take all steps necessary to preserve captured plate data in its possession for 14 days after the date the data is captured pending the issuance of a court order requiring the disclosure of the captured plate data if a governmental entity or defendant in a criminal case requesting the captured plate data submits a written statement to the person or governmental entity using an automatic license plate reader system:
 - (a) requesting the person or governmental entity to preserve the captured plate data;
 - (b) identifying:
 - (i) the camera or cameras for which captured plate data shall be preserved;
 - (ii) the license plate for which captured plate data shall be preserved; or
 - (iii) the dates and time frames for which captured plate data shall be preserved; and
 - (c) notifying the person or governmental entity maintaining the captured plate data that the governmental entity or defendant in a criminal case is applying for a court order for disclosure of the captured plate data.
- (2)
 - (a) A governmental entity or defendant in a criminal case may apply for a court order for the disclosure of captured plate data possessed by a governmental entity.
 - (b) A court that is a court of competent jurisdiction shall issue a court order requiring the disclosure of captured plate data if the governmental entity or defendant in a criminal case offers specific and articulable facts showing that there are reasonable grounds to believe that the captured plate data is relevant and material to an ongoing criminal or missing person investigation.
- (3) Captured plate data that is the subject of an application for a disclosure order under Subsection (2) may be destroyed at the later of:
 - (a) the date that an application for an order under Subsection (2) is denied and any appeal exhausted;
 - (b) the end of 14 days, if the person or governmental entity does not otherwise preserve the captured plate data; or
 - (c) the end of the period described in Subsection 41-6a-2004(1)(c).
- (4) Notwithstanding Subsection (2), a governmental entity may enter into a memorandum of understanding with another governmental entity to share access to an automatic license plate reader system or captured plate data otherwise authorized by this part.
- (5) A governmental entity may obtain, receive, or use captured plate data from a nongovernmental entity only:
 - (a)
 - (i) pursuant to a warrant issued using the procedures described in the Utah Rules of Criminal Procedure or an equivalent federal warrant; or
 - (ii) using the procedure described in Subsection (2); and
 - (b) for the purposes authorized in Subsection 41-6a-2003(2).
- (6)
 - (a) A law enforcement agency shall preserve a record of:
 - (i) the number of times a search of captured license plate data is conducted by the agency or the agency's employees or agents; and
 - (ii) the crime type and incident number associated with each search of captured license plate data.

Effective 5/3/2023

41-6a-2006 Penalties.

A person who knowingly or intentionally uses, obtains, or discloses captured license plate data in violation of this part is guilty of a class B misdemeanor.

Amended by Chapter 524, 2023 General Session

Automated License Plate Readers (ALPRs)

461.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of the automated license plate reader (ALPR) technology (Utah Code 41-6a-2003).

461.2 ADMINISTRATION

The ALPR technology, also known as license plate recognition (LPR), allows for the automated detection of license plates. It is used by the North Salt Lake Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the Administration Deputy Chief. The Administration Deputy Chief will assign personnel under the Administration Deputy Chief's command to administer the day-to-day operation of the ALPR equipment and data.

461.2.1 SPECIAL USE PERMITS

The Administration Deputy Chief or the authorized designee shall obtain required special use permits before installation of stationary ALPR equipment when applicable (Utah Code 41-6a-2003; Utah Code 72-1-212).

461.3 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use or allow others to use the equipment or database records for any unauthorized purpose.

- (a) An ALPR shall only be used for official and legitimate law enforcement business (Utah Code 41-6a-2003).
- (b) Particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings, and other major incidents that qualify for use of an ALPR. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- (c) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (d) If practicable, the officer should verify an ALPR response through the appropriate law enforcement database before taking enforcement action that is based solely upon an ALPR alert.
- (e) No ALPR operator may access confidential department, state, or federal data unless otherwise authorized to do so.

North Salt Lake Police Department

North Salt Lake PD Policy Manual

Automated License Plate Readers (ALPRs)

461.3.1 LIMITATIONS ON USE

ALPR data shall only be used for the following official law enforcement business (Utah Code 41-6a-2003):

- (a) As part of an active criminal investigation as defined by Utah Code 41-6a-2002
- (b) To apprehend an individual with an outstanding warrant
- (c) To locate a missing or endangered person
- (d) To locate a stolen vehicle

An ALPR system may be used to access the Utah Criminal Justice Information System to verify vehicle registration or insurance information, confirm vehicle identification, or identify a stolen vehicle (Utah Code 41-6a-2003).

461.4 DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the North Salt Lake Police Department and because such data may contain confidential information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law (Utah Code 41-6a-2004).

The Administration Deputy Chief is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

The Administration Deputy Chief or the authorized designee shall take steps to have all ALPR data that is not reasonably related to official law enforcement business purged in an unrecoverable manner as soon as practicable. In no event shall this data be maintained longer than nine months unless it is subject to a warrant, preservation request, or disclosure order (Utah Code 41-6a-2004). Data that will not be purged should be downloaded from the server onto portable media and booked into evidence.

461.4.1 NON-GOVERNMENTAL AGENCY ALPR

ALPR data captured by a non-governmental agency device may only be obtained pursuant to a warrant or a court order (Utah Code 41-6a-2005).

461.5 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The North Salt Lake Police Department will observe the following safeguards regarding access to and use of stored data:

- (a) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
- (b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data

North Salt Lake Police Department

North Salt Lake PD Policy Manual

Automated License Plate Readers (ALPRs)

- relate to a specific criminal investigation or department-related civil or administrative action.
- (c) The number of ALPR data searches conducted by members as well as the crime type and incident numbers associated with each search shall be recorded and preserved for at least five years (Utah Code 41-6a-2005).
 - (d) ALPR system audits should be conducted on a regular basis.

461.6 POLICY

The policy of the North Salt Lake Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

461.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
 - 1. The name of the agency.
 - 2. The name of the person requesting.
 - 3. The intended purpose of obtaining the information.
- (b) The request is reviewed by the Administration Deputy Chief or the authorized designee and approved before the request is fulfilled.
- (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

461.8 PUBLIC ACCESS

This policy and any special use permits obtained for stationary ALPRs shall be published on the City website or on the Utah Public Notice Website if the Department does not have access to a City website (Utah Code 41-6a-2003; Utah Code 72-1-212).

MEMORANDUM OF UNDERSTANDING BETWEEN AGENCIES

License Plate Recognition (LPR) Equipped

Law Enforcement Agencies

FOR SHARING LPR DETECTION DATA AND HOTLISTS

I. OVERVIEW

A. Introduction:

The purpose of this "Memorandum of Understanding" (MOU) is to outline conditions under which the Agency Parties (North Salt Lake City Police Department (UT) and Davis County Sheriffs Office (UT)) will share and use "LPR detection data" (scanned plates) and/or "hotlist" information as defined on the last page of this MOU. The Motorola Solutions' hosted system provides for simple point-and-click data sharing between credentialed Agency Managers with data sharing privileges enabled by their respective agencies.

This MOU provides a basic understanding for the sharing of data between agencies; any additional requirements (liabilities, governing law, etc) should be documented separately in a written agreement between agencies.

B. Background:

License Plate Recognition (LPR) is a computer-based system that utilizes emerging technology to capture a color image, as well as an infrared image, of the license plate of a vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file," also known as a "hotlist," and can contain information on stolen or wanted vehicles as well as vehicles associated with Amber Alerts, warrant subjects, and agency defined-information.

LPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. LPR systems have all the necessary equipment to scan plates, notify the user of a vehicle hit, and upload the LPR detection data into an LPR repository for retention and research.

The Agencies entering into this MOU, realizing the mutual benefits to be gained by sharing information, seek to share LPR detection data and/or hotlist information as defined on the last page of this MOU.

II. AUTHORIZED RELEASE OF INFORMATION

A. Sharing of Information:

Each Agency Party authorizes access to its LPR detection data and/or hotlist information as defined on the last page of this MOU residing in its Motorola Solutions account to other Agency Parties as permitted by applicable state law. An Agency Party that does not want certain information made available to any other Agency Party is responsible for ensuring that the information is not made available for data sharing. There is no obligation to share LPR detection data and/or hotlist information with any Agency Parties based solely on this MOU.

B. Limitation on Information Sharing:

LPR detection data and/or hotlist information shall only be shared with or released to authorized employees of the Agency Parties who have an approved login and password ("Authorized Users"), and a need and/or right to know.

III. INFORMATION OWNERSHIP

A. Ownership:

Each Agency Party retains control of all information in its account. Each Agency Party is responsible for creating, updating, and deleting records in its own account according to its own retention policies. Each Agency Party shall use reasonable efforts to ensure the completeness and accuracy of its data.

B. Release of Information:

Agency Parties and authorized users shall release or make available information accessed from an LPR account only to persons or entities authorized to receive LPR information.

C. Unauthorized Requests:

If an Agency Party receives a request for information in an LPR account by anyone who is not authorized to receive information from the LPR account, that Agency Party shall refer the request to the law enforcement agency that originated the requested information ("Source Agency").

D. Public Record Requests, Subpoenas and Court Orders:

Any Agency Party receiving a public records request, subpoena, or court order ("Legal Request") for information in an LPR account not authored by or originated by that Agency Party shall immediately provide a copy of the Legal Request to the Source Agency, prior to providing a response to the Legal Request.

IV. USER ACCESS

A. Login Application Process:

Each Agency Party's Agency Manager is responsible for management of user accounts at that Agency Party. Each Agency Party agrees that all authorized users shall be limited to current employees who are legally authorized to review criminal history data for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency Manager. The Agency Manager shall have discretion to deny or revoke individual access for their respective agency.

B. Login Assignments:

Each Authorized User will be issued a user login and a password by the Agency Manager. Authorized Users may be assigned to groups that have different levels of access rights based on the level of restriction of the information.

C. Termination of Logins:

Each Agency Manager is responsible for timely removal of any login accounts as Authorized Users leave the Agency, no longer qualify for access into the system, or are denied access by the Agency Manager for any other reason.

D. Intended Use:

Each Authorized User agrees that scanned plate, hotlist information, and networking resources are to be used solely for law enforcement purposes only and consistent with the law. Authorized Users shall not use or share the information for any unethical, illegal, criminal, or commercial purpose. Pursuant to California Government Code Section 3, Chapter 17.25 (commencing with section 7284) federal, state, or local law enforcement agencies shall not use any non-criminal history information contained within the database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. sections 1373 and 1644.

E. Limitations on Use of Logins:

An Authorized User shall not access information in an LPR repository by using a name or password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

F. Audit Trail:

Each transaction is to be logged, to include a Case Number, and an audit trail created. Each Agency Manager shall conduct an internal audit on a periodic basis to ensure user queries are made for legitimate law enforcement purposes only. This information shall be recorded and retained to allow the agency manager to complete the internal audit. Each agency manager shall maintain the audit trail pursuant to the retention policies of that Agency Party. Requests for transaction logs shall be made in writing to the Agency Manager, who shall provide the logs to the requesting party within a reasonable amount of time.

V. CONFIDENTIALITY OF INFORMATION

A. Information Confidentiality:

Information in an LPR account is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information in an LPR account. Otherwise, the information shall be kept confidential for purposes of not compromising active investigations or undercover operations, jeopardizing officer or public safety.

B. Internal Requests for Information:

An Authorized User who receives a request from a non-authorized requestor for information in an LPR account shall not release that information, but may refer the requestor to the Source Agency.

C. Removal or Editing of Records:

Agency Parties shall determine their own schedule for record deletion and other edits to their own data. This will be determined by policy and/or legal requirements.

VI. MOU TERMS

A. Term:

This MOU will commence upon its creation, which occurs on the date that the data share takes place within the Motorola Solutions hosted platform. It may be terminated at any time when an Agency Manager revokes data sharing access from another agency.

VII. EXECUTION OF MOU

This MOU is executed by the Parties below, for the below-described data. Each Party acknowledges that it has received a copy of this MOU, and will comply with its terms and conditions. Each Party certifies that he/she is authorized by its Party to execute this data sharing relationship.

Data Shared Between Parties: North Salt Lake City Police Department (UT) DETECTION DATA

Sharing Agency: North Salt Lake City Police Department (UT)
Agency Manager Authoring Share: Mitch Gwilliam
Agency Manager Email: mitchg@nslcity.org
Title:

Receiving Agency: Davis County Sheriffs Office (UT)
Agency Manager Receiving Share: Joshua Boucher
Agency Manager Email: jboucher@co.davis.ut.us
Title:

Date of MOU: 05-19-2026



Resources

[Learn more about Motorola Solutions LPR technology](#)

[Read our LPR Privacy Policy](#)

[Visit the Motorola Solutions Trust Center](#)



MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2026 Motorola Solutions, Inc. All rights reserved. 07-2026 [ES01]



Date: 25 Aug 2026

1. Operational Framework: License Plate Recognition (LPR)

Motorola Solutions' technology is designed strictly as an investigative tool. Motorola Solutions' L6Q and L5F License Plate Recognition (LPR) systems are purpose-built for vehicular identification. An LPR record captures a single photograph of a license plate in public view at an isolated point in time. The L6Q and L5F systems function within the mature VehicleManager platform serving as a dedicated resource independent of general monitoring frameworks. By design, our LPR systems are mission-locked to vehicle-centric data. The L6Q/L5F LPR is specifically restricted to the analysis of license plates, vehicle make, model, color and unique vehicle accessories or attributes.

2. Mandatory Technical Exclusions: Non-Vehicular Scanning Prohibitions

The algorithms powering the L6Q, L5F, and the VehicleManager platform are engineered to disregard non-vehicular data. The system is technically incapable of performing, analyzing, or supporting:

- **Facial Recognition:** The system contains no biometric processing for human subjects.
- **Pedestrian Monitoring:** No logic exists for tracking or analyzing individual humans.
- **Bicycle/Non-Motorized:** The scanning logic ignores non-vehicular entities.

Technical Control Verification . Because the algorithm is developed in-house, these parameters are not merely "features" that can be toggled; they are foundational hard-coded constraints.

Final Summary The L6Q and L5F systems represent a high-integrity recognition environment where privacy is enforced through both physical hardware limitations and hard-coded software prohibitions. By combining specialized optical engineering with a secure, customer-owned data model, these systems provide a powerful investigative resource that is technically incapable of identifying non-vehicular attributes.

Sincerely,

A handwritten signature in black ink that reads 'Daniel Wilburn'. The signature is fluid and cursive, with a long horizontal line extending from the end of the name.

Daniel Wilburn
Director of Product Management



Guide

Motorola Solutions License Plate Recognition

Advancing public safety.
Protecting local privacy.

Designed for public safety, Motorola Solutions' Vehicle Intelligence product suite facilitates privacy, security and more comprehensive compliance with every search. Our technology is purpose built to solve crimes like locating missing children and recovering stolen vehicles. It is never intended for mass surveillance or tracking of law-abiding citizens.

Every interaction generates a clear audit footprint, delivering transparency and reinforcing the public trust we have spent nearly a century building as a partner to first responders.

Partnering with Motorola Solutions provides:

Absolute sovereignty

Agencies retain 100% ownership and control of their LPR data. Motorola Solutions never pools, networks or independently shares it.

Zero-trust sharing

Off by default. Sharing interfaces require explicit, manual, agency administrator-approved invitations. There are no pre-programmed data networks.

Agency-configured retention

Fully customized and controlled by the agency to preserve critical investigative evidence.

Hardware integrity

Devices are fully NDAA and TAA-compliant, featuring dual-layer encryption via FIPS 140-3 Level 1 certified modules.

Comprehensive auditing

Every search, export and access attempt is logged with user identity, timestamp and the required operational reason.

Data sovereignty & controlled sharing

Motorola Solutions gives customers complete control over their data by ensuring that accounts default to zero pre-programmed data-sharing or data-receiving relationships. This means that your department retains total autonomy from day one, with no forced networking or automated data pipelines. Within this sovereign architecture, agency administrators hold the exclusive authority to configure data access in accordance with their own policies and applicable laws; they can agree to flexible one-way or bi-directional sharing parameters, and are never required to share their own locally captured data just to receive data from external agencies.

Secure architecture & customer-defined retention

CJIS-compliant housing

All captured license plate data resides in an environment designed from the ground up to be CJIS-compliant, safeguarding the evidentiary chain of custody.

Agency-driven retention

Customers retain complete data ownership, allowing them to set retention periods according to local laws and policies.

Automatic deletion of shared data

To maintain strict data integrity, shared LPR data is only viewable during the owning agency's designated retention period before being automatically deleted.

Transparent auditing

Full search transparency

Every single action within the platform is fully auditable to ensure organizational accountability and maintain public trust.

Activity logs

The system logs the specific user identity, precise timestamps and mandatory operational justifications for every search conducted.

Advanced investigative analytics

Broad investigative analysis: VehicleManager software delivers a broad, high-level analysis of vehicles of interest to significantly boost investigative capabilities.

Deep analytical features: VehicleManager moves beyond basic plate reads by offering advanced, unique capabilities including speed analysis and parameterized geo-fencing.

Enhanced operational outcomes: Utilizing these deep behavioral analytics directly improves agency efficiency, optimizes resource allocation, and leads to more successful case resolutions.



The ecosystem advantage

Unique integrations with our license plate recognition technology

Unified technology stack: Features a broad, interconnected ecosystem that seamlessly links critical communications, command center software and video security solutions.

Accelerated case closures: Captures a more comprehensive picture of events for evidentiary purposes, directly aiding investigators in closing cases faster.

Our commitment

Compliance & public trust

Compliance by design: Intentionally engineers LPR products to enable customers to maintain full compliance with all laws, regulations, and localized agency policies.

Ethical data management: Promotes key data privacy principles and ethical management, extending these strict compliance requirements to all third-party providers.

Industry-first AI transparency: Offers transparency into algorithmic workflows via AI Nutrition Labels.

A century of trust: Champions public trust as a core pillar of responsible technology use, serving as a reliable and ethical vendor to law enforcement for nearly one hundred years.

Proven public safety outcomes

Principles translated into high-impact case resolution

Abduction emergencies: Rapidly deployed to track suspect flight paths, allowing officers to safely recover kidnapped children and detain abductors in real-time.

Interstate drug interdiction: Identifies and intercepts key transport vehicles associated with cartel distribution networks, leading to major seizures of illegal narcotics.

Violent crime resolution: Empowers investigators to analyze vehicle movements surrounding campus shootings and armed assaults, isolating getaway cars even when witnesses cannot provide descriptions.

Cold case identifications: Preserved historical data allows traffic investigators to link fleeing vehicles to fatal hit-and-run scenes months after the initial incident, bringing closure to victims' families.

The Motorola Solutions difference

STRATEGIC DESIGN AREA	MOTOROLA SOLUTIONS MODEL
Data ownership & autonomy	Complete agency sovereignty. Motorola Solutions cannot manipulate, pool or independently control data parameters.
Data sharing	Zero pre-programmed relationships. Fully federated, isolated agency databases prevent broad network lookup exposure.
Data retention	Fully controlled by agency policy. Protects the long-term integrity of complex investigations with restrictions embedded in the system.
Public trust & compliance	Nearly 100 years of public safety partnership. Products explicitly designed to adapt to local privacy laws and maintain public trust.

Common questions regarding LPR

How does Motorola Solutions answer community concerns regarding mass surveillance?

Motorola Solutions technology is designed strictly as a targeted investigative tool, not a system for pervasive tracking. An LPR record captures a single photograph of a license plate in public view at an isolated point in time. We encourage our customers to transparently communicate to their communities why and how this technology is deployed

Can federal agencies or outside entities access Motorola Solutions' database?

No. There are no built-in data pathways, back doors, or automatic routing mechanisms exposed to federal agencies. If a federal entity requests data, agencies can accept or deny the share request based on their LPR policy. Your administrators retain absolute veto power and determine the response based entirely on local ordinances and state laws.

What mechanism allows supervisors to audit system usage?

Every search query triggers mandatory logging within our audit framework. Administrators can configure automated reporting to track exactly which user executed a search, the timestamp of the event, the precise records accessed, and the mandatory operational justification text entered by the user.

How does Motorola Solutions prepare, teach and inform customers on LPR usage and compliance?

Motorola Solutions offers broad and customizable training as part of your VehicleManager subscription, including on-site sessions and extensive online, on-demand content about responsible LPR use and compliance. Customers can request additional training at no extra cost.

