Apex Logistics International Inc.

AUTOMATED LICENSE PLATE READER (ALPR)
USAGE AND PRIVACY POLICY

Effective Date	
Last Revised	
Approved By	
Official Custodian	Shawn Arai
Governing Law	Cal. Civ. Code §§ 1798.90.5–1798.90.55 (SB 34)

This policy is made available to the public in writing and is posted conspicuously on the Company's website, as required by California Civil Code § 1798.90.51(b).

Section 1: PURPOSE AND SCOPE

This Automated License Plate Reader ("ALPR") Usage and Privacy Policy establishes the rules, procedures, and safeguards governing the collection, use, maintenance, sharing, and dissemination of data obtained through automated license plate recognition technology. This policy is adopted in compliance with California Civil Code §§ 1798.90.5–1798.90.55, as enacted by Senate Bill 34 (SB 34), and all other applicable federal, state, and local privacy laws.

This policy applies to all ALPR systems owned, leased, operated, or accessed by Apex Logistics International Inc. ("Company" or "Organization"), and to all employees, contractors, agents, and service providers who may operate, access, or use ALPR data in any capacity.

The purpose of this policy is to ensure that the use of ALPR technology is consistent with respect for individuals' privacy and civil liberties while enabling the Company to fulfill its legitimate operational and security objectives.

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a), 1798.90.53(a)

Section 2: DEFINITIONS

2.1 ALPR System

An "ALPR system" means a searchable, computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

2.2 ALPR Information

"ALPR information" or "ALPR data" means information or data collected through the use of an ALPR system, including but not limited to:

- License plate numbers and registration data
- Photographs, video images, or other visual recordings of vehicles and license plates
- Date, time, and geolocation coordinates of each vehicle detection
- Any data derived from or linked to license plate images, including vehicle make, model, and color when captured

2.3 ALPR Operator

An "ALPR operator" means a person that operates an ALPR system, as defined by Cal. Civ. Code § 1798.90.5(a). The Company serves as an ALPR operator to the extent it owns, leases, or directly operates ALPR systems.

2.4 ALPR End-User

An "ALPR end-user" means a person that accesses or uses an ALPR system, or accesses or uses ALPR information, whether or not that person operates the system, as defined by Cal. Civ. Code § 1798.90.5(b).

2.5 Hot List

A "hot list" means a list of specific license plates associated with stolen vehicles, wanted persons, AMBER Alerts, missing or endangered persons, or vehicles reasonably suspected of being involved in the commission of a crime.

2.6 Personal Information

ALPR data may constitute “personal information” as defined under the California Consumer Privacy Act (CCPA) and other applicable California privacy statutes.

Legal Authority: Cal. Civ. Code § 1798.90.5

Section 3: AUTHORIZED PURPOSES FOR COLLECTION AND USE

The Company collects and uses ALPR data solely for the following legitimate and authorized business purposes:

- Facility access control and perimeter security
- Theft prevention, asset protection, and loss mitigation
- Investigation of violations of Company policies, rules, or applicable laws
- Supporting law enforcement investigations when responding to lawful requests
- Compliance with legal, regulatory, or contractual obligations

ALPR data shall not be collected or used for any purpose unrelated to the authorized purposes enumerated above. Any new or expanded use of ALPR data must be approved in writing by the Official Custodian and reflected in an amendment to this policy.

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a)(1), 1798.90.53(a)(1)

Section 4: PROHIBITED USES

The Company strictly prohibits the following uses of ALPR data:

- Tracking, profiling, or targeting individuals based on race, ethnicity, religion, national origin, gender, sexual orientation, disability, or any other protected characteristic
- Harassment, intimidation, stalking, or any form of unlawful discrimination
- Personal use by any employee, contractor, or agent for purposes unrelated to authorized business operations
- Accessing ALPR data without a legitimate, documented business purpose
- Selling ALPR information to any third party under any circumstances
- Sharing or transferring ALPR data in violation of Cal. Civ. Code § 1798.90.55
- Automated decision-making that produces legal or similarly significant effects on individuals without appropriate safeguards, human review, and due process

Any employee, contractor, or agent who engages in prohibited use of ALPR data shall be subject to disciplinary action up to and including termination, and may face civil and criminal liability as provided by law.

Legal Authority: Cal. Civ. Code § 1798.90.54

Section 5: AUTHORIZED PERSONNEL AND ACCESS CONTROLS

5.1 Designated Authorized Users

Access to the ALPR system and ALPR information is restricted to the following authorized personnel categories:

- ALPR System Administrator(s): Responsible for system configuration, maintenance, and access management
- Security Operations Personnel: Authorized to access ALPR data for real-time monitoring and incident response
- Designated Investigators: Authorized to query ALPR data in connection with active investigations
- Privacy/Compliance Officer: Authorized to audit ALPR access and usage for compliance purposes
- Management Officials: As designated by the Official Custodian, with documented business need

All authorized users must be identified by job title or designation and individually approved by the Official Custodian prior to being granted system access.

5.2 Role-Based Access Controls

Access to ALPR data is governed by role-based access controls (RBAC). Each authorized user is granted the minimum level of access necessary to perform their assigned duties. Access privileges are reviewed no less than quarterly and promptly revoked upon change of assignment, separation from employment, or termination of contractor engagement.

5.3 Authentication and Account Management

All ALPR system accounts require supervisory approval before activation. Multi-factor authentication (MFA) or equivalent robust authentication protocols are required for all users. Shared or generic accounts are prohibited. Each user must have a unique login credential that enables individual-level accountability.

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a)(4), 1798.90.52(a)

Section 6: DATA RETENTION AND DESTRUCTION

6.1 Retention Period

ALPR data is retained only for the minimum period reasonably necessary to fulfill the authorized purposes described in Section 3 and to comply with legal, regulatory, or contractual obligations.

The standard retention periods are as follows:

Data Category	Maximum Retention Period
Non-hit ALPR data (no hot list match)	30 days
Hot list match data	As required for investigation/litigation
Data subject to legal hold	Duration of hold plus 30 days
Audit and access logs	Minimum 3 years

Note for Public Agencies: Pursuant to Cal. Civ. Code § 1798.90.55(b), a public agency operating as an ALPR operator or end-user shall not access ALPR information that does not match information on a hot list for more than sixty (60) days after the date of collection.

6.2 Secure Destruction

Upon expiration of the applicable retention period, ALPR data shall be securely deleted or permanently anonymized using industry-standard methods. Destruction shall be documented and certified by the ALPR System Administrator.

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a)(6), 1798.90.53(a)(6), 1798.90.55(b)

Section 7: DATA SECURITY SAFEGUARDS

The Company maintains reasonable administrative, technical, operational, and physical safeguards to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure, as required by Cal. Civ. Code §§ 1798.90.51(a)(3) and 1798.90.53(a)(3). These safeguards include, but are not limited to:

7.1 Technical Safeguards

- Encryption of ALPR data at rest and in transit
- Multi-factor authentication for all system access
- Login/password-protected systems capable of documenting all access by username, date, and time
- Network segmentation and intrusion detection/prevention systems
- Regular vulnerability assessments and penetration testing

7.2 Administrative Safeguards

- Written information security policies and procedures
- Background checks for all personnel with ALPR system access
- Mandatory privacy and security training (see Section 6)
- Regular compliance audits and policy reviews

7.3 Physical Safeguards

- Physical access controls for ALPR infrastructure and data centers
- Secured and tamper-evident ALPR camera installations
- Environmental protections for ALPR servers and storage systems

7.4 Incident Response

The Company maintains a documented incident response plan for security breaches involving ALPR data. In the event of a breach, the Company will comply with all applicable breach notification requirements under California law, including Cal. Civ. Code § 1798.82 (California Data Breach Notification Law).

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a)(3), 1798.90.52(a), 1798.90.53(a)(3)

Section 8: ACCESS LOGGING AND AUDIT TRAIL

Pursuant to Cal. Civ. Code § 1798.90.52, the Company maintains a comprehensive audit trail of all access to ALPR information. Every query or access event is logged with the following information:

- Date and time of access
- Username and organizational affiliation of the person accessing the data

- License plate number(s) or other data elements used to query the system
- Stated purpose or justification for the query
- Case file number or investigation reference, where applicable

Access logs are protected from tampering, unauthorized modification, and deletion. Logs are retained for a minimum of three (3) years and are subject to periodic review by the Privacy/Compliance Officer to detect unauthorized access, misuse, or anomalous activity.

All ALPR data downloaded to mobile workstations or portable storage must remain accessible only through login/password-protected systems capable of documenting all access by username, date, and time.

Legal Authority: Cal. Civ. Code § 1798.90.52

Section 9: SYSTEM MONITORING AND COMPLIANCE

The Company implements ongoing monitoring of the ALPR system to ensure the security of ALPR information and compliance with applicable privacy laws, as required by Cal. Civ. Code § 1798.90.51(a)(5). Monitoring activities include:

- Automated alerts for unusual access patterns, bulk queries, or off-hours access
- Periodic review of access logs by the Privacy/Compliance Officer
- Quarterly audits of user access privileges and account status
- Annual comprehensive compliance reviews, including assessment of data retention practices, training completion, and policy adherence
- Remediation tracking and documentation of corrective actions

The Official Custodian is responsible for ensuring that monitoring activities are conducted regularly and that findings are reported to appropriate management.

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a)(5), 1798.90.53(a)(5)

Section 10: DATA ACCURACY AND ERROR CORRECTION

The Company implements reasonable measures to ensure the accuracy of ALPR information and to promptly correct data errors, as required by Cal. Civ. Code § 1798.90.51(a)(7). These measures include:

- Regular calibration and maintenance of ALPR cameras and optical character recognition (OCR) software to minimize read errors
- Verification procedures before any enforcement or investigative action is taken based solely on ALPR data
- A documented process for individuals to report suspected data errors or inaccuracies
- Prompt investigation and correction of reported errors, with notification to any parties with whom erroneous data was shared

No adverse action shall be taken against any individual based solely on an unverified ALPR data match without independent corroboration.

Legal Authority: Cal. Civ. Code § 1798.90.51(a)(7)

Section 11: SHARING, TRANSFER, AND DISCLOSURE OF ALPR DATA

11.1 Prohibition on Sale

The Company does not sell ALPR information under any circumstances.

11.2 Authorized Disclosures

ALPR data may be shared or disclosed only under the following limited circumstances:

- With service providers and vendors who support the ALPR system and are bound by written contractual obligations to protect the data, use it solely for authorized purposes, and comply with this policy and applicable law
- When compelled by valid legal process, including subpoenas, court orders, or search warrants issued by a court of competent jurisdiction
- With law enforcement agencies in response to lawful requests, consistent with Cal. Civ. Code § 1798.90.55 and applicable law

11.3 Restrictions for Public Agencies

If the Company operates as a public agency: ALPR information shall not be sold, shared, or transferred except to another public agency, and only as otherwise permitted by law. ALPR information shall not be shared with private entities, out-of-state agencies, or federal agencies except as expressly authorized by California law.

11.4 Recipient Obligations

All recipients of ALPR data are required to maintain privacy and security protections at least as stringent as those described in this policy and as required by California law.

Legal Authority: Cal. Civ. Code §§ 1798.90.51(a)(2), 1798.90.53(a)(2), 1798.90.55(a)

Section 12: INDIVIDUAL RIGHTS AND REQUESTS

The Company respects the privacy rights of individuals whose data may be captured by ALPR systems. Where required by law, individuals may exercise the following rights:

- Right to Know: Request information about whether their personal information has been collected and how it has been used
- Right to Access: Obtain a copy of ALPR data associated with their vehicle, subject to legal limitations
- Right to Deletion: Request deletion of ALPR data, subject to applicable exemptions for ongoing investigations, legal holds, or compliance obligations
- Right to Correct: Request correction of inaccurate ALPR data

Requests may be submitted to the Official Custodian at:

Email: shawn.arai@apexglobe.com

The Company will verify the identity of the requestor before processing any request. Requests will be responded to within the timeframes required by applicable law (typically 45 calendar days under the CCPA).

Section 13: PUBLIC NOTICE AND TRANSPARENCY

This policy is made available to the public in writing and is posted conspicuously on the Company's Internet website, in compliance with Cal. Civ. Code § 1798.90.51(b).

If the Company is a public agency that operates or intends to operate an ALPR system, it shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body before implementing the ALPR program, as required by Cal. Civ. Code § 1798.90.51(b)(2).

Legal Authority: Cal. Civ. Code § 1798.90.51(b)

Section 14: ENFORCEMENT, VIOLATIONS, AND REMEDIES

14.1 Internal Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, referral for criminal prosecution, and/or civil liability.

14.2 Civil Remedies Under California Law

Pursuant to Cal. Civ. Code § 1798.90.54, an individual who has been harmed by a violation of the ALPR statutes, including unauthorized access or use of ALPR information or a breach of security of an ALPR system, may bring a civil action against the responsible party. Available remedies include:

- Actual damages, but not less than liquidated damages of two thousand five hundred dollars ($2,500)
- Punitive damages upon proof of willful or reckless disregard of the law
- Reasonable attorney's fees and litigation costs
- Preliminary and equitable relief as the court determines appropriate

Legal Authority: Cal. Civ. Code § 1798.90.54

Section 15: VENDOR AND THIRD-PARTY MANAGEMENT

All ALPR vendors, manufacturers, suppliers, and third-party service providers must be bound by written agreements that require:

- Compliance with this policy and all applicable California ALPR laws
- Implementation of security safeguards at least as protective as those described in Section 8
- Limitations on data use to authorized purposes only
- Prohibition on providing default access to any national ALPR database without express written authorization from the Company
- Prompt notification to the Company of any security breach or unauthorized access involving ALPR data
- Return or secure destruction of all ALPR data upon termination of the agreement

The Company conducts due diligence on all ALPR vendors before engagement and periodically reviews vendor compliance with contractual and legal requirements.

Section 16: OFFICIAL CUSTODIAN

The following individual is designated as the Official Custodian and owner of the ALPR system, responsible for oversight, compliance, and administration of this policy:

Name: Shawn Arai

Title: Security Risk & Client Assurance Manager

Email: shawn.arai@apexglobe.com

Phone:(310) 735-8295

The Official Custodian is responsible for reviewing this policy at least annually, ensuring compliance with all applicable laws, coordinating training, overseeing audits, and serving as the primary point of contact for questions, complaints, and data subject requests related to the ALPR system.

Legal Authority: Cal. Civ. Code § 1798.90.51(a)(3)

Section 17: POLICY REVIEW AND AMENDMENTS

This policy shall be reviewed no less than annually by the Official Custodian and updated as necessary to reflect changes in applicable law, technology, organizational practices, or operational requirements. Material amendments will be reflected by updating the “Last Revised” date and, where required, providing appropriate public notice.

All prior versions of this policy shall be archived and retained for a minimum of five (5) years for audit and compliance purposes.

Section 18: GOVERNING LAW AND REGULATORY CROSS-REFERENCES

This policy is governed by and shall be interpreted in accordance with the laws of the State of California. The following statutes and regulations are incorporated by reference:

- California Civil Code §§ 1798.90.5–1798.90.55 (SB 34 — ALPR Privacy)

- California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100–1798.199.100
- California Data Breach Notification Law, Cal. Civ. Code § 1798.82
- California Public Records Act (CPRA), Cal. Gov. Code §§ 7920.000 et seq., as applicable
- All applicable federal, state, and local privacy and data protection laws

APPROVED BY:	**DATE:**
Signature	*Date*
Printed Name and Title	