ATTACHMENT B

Los Angeles Speed Safety System

Use Policy

LADOT January 2026

Background

Speeding endangers everyone on the road, not just the driver. Speeding is a leading cause of crashes that result in serious injuries and fatalities, contributing to nearly one-third of all traffic deaths nationwide in 2023.[1] The risk of severe injury or death increases sharply with higher speeds: a crash at 50 miles per hour carries a 59% chance of serious injury, compared with just 15% at 40 miles per hour.[2] In Los Angeles, there were an average of 1,916 crashes per year between 2020 and 2024, and speeding was a factor in one-third of them.[3] Enforcing speed limits is critical to reducing collisions that cause injuries and deaths.

The City of Los Angeles (the City) employs a variety of strategies to reduce speeding, including traffic engineering, public education, and enforcement. As part of these efforts, the City uses Speed Safety Systems (Systems), which are defined under California Vehicle Code sections 22425 – 22434 (Speed Safety System Pilot Program) as fixed or mobile radar, laser, or other automated devices used to detect speeding violations and capture clear images of vehicle license plates. The City's Automated Speed Enforcement (ASE) program collects and analyzes this data at designated locations across the city to support the City's Vision Zero initiative[4].

Speed safety systems have proven highly effective in cities nationwide at lowering average speeds, curbing dangerous driving, and improving road safety. For example, San Francisco reported an average of 72% reduction in speeding vehicles at 15 sites after the first six months of their speed safety systems program. When paired with public education and thoughtful street design, these systems reliably identify speeding vehicles, reduce dangerous driving, prevent crashes, and save lives. In 2017, the National Transportation Safety Board (NTSB) reviewed multiple studies on speed safety cameras and

[1] https://www.nhtsa.gov/risky-driving/speeding
[2] https://aaafoundation.org/impact-of-speeds-on-drivers-and-vehicles-results-from-crash-tests/
[3] Transportation Injury Mapping System (TIMS), Safe Transportation Research and Education Center, University of California, Berkeley. 2025
[4] Vision Zero is a global initiative to eliminate traffic-related fatalities.

found that they effectively lower average driving speeds, reduce excessive speeding and lessen the severity of crashes. The NTSB also urged all states to remove restrictions on their use and adopt clear laws permitting the deployment of speed safety systems without strict limits on location or operation.

Deploying speed safety systems on streets where speeding creates dangerous conditions is a cost-effective and proven way to prevent injuries and save lives.

Purpose of the System

Under California Assembly Bill 645 (AB 645), the purpose of these Systems is to reduce speeding and improve road safety in Los Angeles by automatically detecting vehicles exceeding posted speed limits, capturing clear images of their license plates, and using these data to levy civil penalties on those who are non-compliant with speeding laws. Specifically, the Systems are intended to:

- **Reduce crashes and injuries**: Lower average vehicle speeds and the likelihood of crashes resulting in severe injury or death.
- **Enforce traffic laws while maintaining civil liberties**: Ensure automated enforcement is conducted transparently, fairly, and with safeguards for privacy and proper use of collected data.
- **Encourage compliance with speed limits**: Through consistent enforcement and public awareness, reduce dangerous driving behavior over time.

Authorized Use of Technology and Data

Systems will be operated solely for purposes authorized under AB 645. The Los Angeles Department of Transportation (LADOT) shall use Systems technology only to:

- Detect violations of speed laws only on streets that are defined and communicated to the public, with documented excess speeding, safety concerns, and/or nearby vulnerable populations (e.g., school zones, senior centers, etc.) and in designated areas where there is not a reasonable expectation of privacy
- Capture clear photograph(s) of the speeding vehicle's license plate and the rear of the vehicle for the purposes of identifying make and model, excluding the rear windshield (note that photographs of people's faces will not be captured and AB 645 specifically prohibits use of facial recognition technology).
- Use the license plate data to identify the registered vehicle owner on file with the Department of Motor Vehicles (DMV)
- Document the vehicle speed detected by the System
- Document the date and time when the violation occurred

- Issue a notice of a civil, non-moving violation[5] (similar to a parking ticket) to the registered vehicle owner based on photographic evidence
- Monitor program effectiveness within defined, publicly available key performance indicators (e.g., speed reduction, safety outcomes) to assess traffic safety, impacts to civil rights and liberties, and additional locations for Systems technology

Systems and collected data shall not be used to surveil, harass, intimidate, or discriminate against any individual or group, nor for monitoring activities protected under the First Amendment of the United States Constitution. All use of Systems technology will comply with California Vehicle Code sections 22425 - 22434, including limitations on locations, and retention of and access to collected data.

Authorized Users

Authorized Users are LADOT staff and approved Contractors who may access program elements to perform or support services in carrying out an Authorized Use, as defined in this Policy. Contractors include technology providers and other vendors who assist LADOT in these operations. Access to Program data is limited to Authorized Users with a specific operational need, as determined by LADOT's General Manager or their designee. In compliance with AB 645, LADOT maintains a record of all Authorized Users and the specific purposes for which access is granted.

Authorized User Training Programs

To ensure responsible and secure use of LADOT's Systems, it is essential that all Authorized Users are properly trained before being granted access. Training provides users with the knowledge needed to comply with legal requirements, operate equipment correctly, and uphold strict data protection standards.

All Authorized Users shall receive training and necessary materials prior to being provided with access to Systems and Program data. LADOT will maintain a record of all completed training sessions. Training courses will cover the following:

1. Applicable federal and state laws;
2. Functionality and proper operation of the equipment;
3. Functions for which City staff will be responsible to review and/or testify to;
4. Overview of protocols for safeguarding access to the Systems, access to Program data; and
5. Overview of administrative, physical, technical, and operational procedures, including ethical responsibilities, conflicts of interest, and impartial handling of violations.

By establishing a consistent baseline of understanding, LADOT minimizes the risk related to system misuse, data breaches, or noncompliance with state and federal regulations.

[5] A civil, non-moving violation is a non-criminal offense handled through a civil process rather than the criminal court system. It does not add points to a driver's license, does not affect insurance, and is enforced through administrative penalties (e.g., fines and fees) instead of criminal charges to encourage compliance to rules.

System Hardware Management

LADOT applies administrative, operational, technical, and physical safeguards to manage System cameras and associated hardware. These safeguards ensure that all cameras are properly maintained, accurately positioned, and operated strictly for purposes authorized under AB 645, including speed limit enforcement, administrative review, and program evaluation.

To maintain reliable and accurate operation, LADOT will require regular maintenance, technical support, upgrades, calibration, and system updates to ensure all System cameras and related equipment function properly. The equipment contractor will be required to calibrate each speed safety system installation once every 60 days per the manufacturer's instructions and once per year by an independent calibration laboratory. Contractors supporting Systems deployment are required to comply with these standards and provide regular reports of maintenance activities to LADOT.

Data Collection, Handling, and Security

Data Types

System technology collects raw image data and related vehicle information, which may include limited "Personal Information," (see footnote below)[6] for the purpose of enforcing speed limits in compliance with AB 645. This Policy defines the types of data generated and its use in Systems operations (Table 1). Data types include Raw Image Data, Processed Data, Appended Data, and Derived Data. These data types are fully defined in Table 1.

- Raw Image Data: Unprocessed, unannotated visual or sensor data captured at the point of collection by a camera or associated sensors.
- Processed Data: Information produced by analyzing Raw Image Data.
- Appended Data: Supplemental information linked to Processed Data.
- Derived Data: Anonymized,[7] aggregated[8] information created by analyzing or combining, Raw Image, Processed, or Appended Data in a way that prevents identification of individuals.

[6] As defined by the California Consumer Privacy Act, "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

[7] Anonymized data removes or modifies all information that could reasonably link the data back to the individual.

[8] Aggregated data is processed, summary data that combines individual-level data. The primary purpose of aggregated data is to allow for analysis, trend recognition, and policy evaluation without focusing on a single person or vehicle.

Table 1: . Data Types and Details

Data Type	Description	Data Details
Raw Image Data	Unprocessed, unannotated, point of collection image, point cloud, infrared, or other data collected by System cameras or associated sensors.	• Presence of vehicles • Vehicle license plate images • Vehicle images • Metadata for Raw Image Data (e.g., location information, contextual data such as buildings and street-level block information, date and time of capture)
Processed Data	Information generated from Raw Image Data through analysis and manual review.	• Rear license plate only • Vehicle license plate number and issuing state • Inferred vehicle type and physical characteristics (e.g., make, model, year, color) • Vehicle speed • Event interpretation (e.g., speed of vehicle, speed classification) • Aggregated or macro-level information relevant to processing of the image
Appended Data	Additional information linked to the processed data by a System and manually by authorized personnel.	• Vehicle registration information (e.g., owner name, registered address, registration status) • Associated vehicle owner information (e.g., special designation or permit and other vehicle specification information such as year, propulsion information, weight, and registered use) • Event determination • Violation level (as determined by authorized personnel) • Whether the violation is a first offense • Administrative or enforcement determinations (manual or automated)
Derived Data	Any information derived directly or indirectly from analyzing, aggregating, visualizing, geo-locating, or modeling Raw Image, Processed, or Appended Data. Derived Data is anonymized and aggregated to prevent identification of individuals.	Examples include: • Counts of vehicles by speed bin • Trends (e.g., percent of speeding vehicles over time by corridor or area) • Operational insights • Other information

Data Restrictions

Certain types of data are strictly prohibited from being captured by Systems. The law forbids collecting identifying images of drivers, passengers, pedestrians, or other vehicles. It also restricts or regulates the use of video recording as opposed to still photography and expressly bans the use of facial recognition or similar biometric technologies. These limitations ensure that enforcement activities focus solely on vehicle speeds and compliance, while protecting individual privacy.

Data Designation, Storage, and Protection

Data from the Pilot Program will be classified by Data Type and designation in accordance with LADOT's existing Data Protection Principles, and Master Data License Protection Agreement, and the Information Technology Policy Committee (ITPC) Information Handling Guidelines[9], which together govern permissible access, use, and disclosure based on data sensitivity and purpose.

Restricted Information

Certain System events and related administrative, enforcement, or legal records may be designated as "Restricted Information" due to the potential legal, financial, or reputational risks of unauthorized disclosure. Restricted information is protected through enhanced security measures, including encryption in transit, at rest, and in use; multi-factor authentication; and secure physical locked storage of portable devices or media containing this data. Access is limited to Authorized Users with a direct operational or legally authorized need.

Confidential Information

Raw Image Data and Processed Data containing Personal Information are treated as "Confidential Information." LADOT and its contractors will implement and maintain administrative, technical, and organizational safeguards to prevent unauthorized access, disclosure, or misuse. All confidential Information at rest and in-transit must be encrypted using industry-standard methods or better, protected from cybersecurity threats such as hacking or malware, and stored on secure systems. Contractors, insofar as this is possible, shall use precautions, including, but not limited to, physical software and network security measures. Encryption should be certified per U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent or higher. Access is limited to Authorized Users for purposes related to enforcement, administrative review, or program evaluation.

Internal Information and Open Data Policy

LADOT anticipates that program data will yield critical operational and planning insights and trends that can inform program evaluation. Internal Information means Derived Data products, including insights,

[9] This document provides guidelines for how the City of Los Angeles classifies, stores, transmits, and protects different types of information (public information, open data, internal information, confidential information, and restricted information) to ensure compliance with legal requirements, safeguard sensitive data, and maintain information security. Access the report at https://cityclerk.lacity.org/onlinedocs/2019/19-1355_rpt_DOT_6-14-2020.pdf.

visualizations, models, and reports developed from aggregations and collections of Raw Image Data that are de-identified, aggregated, and cannot be reverse engineered to identify individual persons or vehicles. Such Derived Data may be designated as Internal Information or, consistent with the City of Los Angeles' Open Data Policy, released as Open Data, defined as non-confidential, non-personal data made publicly available in accessible formats for public use, subject to applicable privacy, security, and legal restrictions, and LADOT approval. All such data is stored securely, with all Personal Information removed to prevent identification of individuals or vehicles. Data minimization, aggregation, de-identification, and secure destruction will be applied to these datasets to ensure compliance with AB 645.

All program data must be stored securely within the continental United States, whether on City-owned servers, approved cloud services, and portable devices. Portable devices, including laptops, external drives, or other media must be:

- Registered with LADOT
- Encrypted and password-protected
- Restricted to Authorized Users only
- Equipped with remote-wipe capabilities if lost, stolen, or replaced

Portable devices may not leave the continental United States unless specifically approved, tracked through administrative controls, and secured according to these standards.

Data Processing, Enrichment, and Analysis

LADOT's Contractors may process, clarify, and analyze Raw, Processed, and Appended Data to produce Derived Data for purposes consistent with Authorized Uses.

This can include, but is not limited to, de-identifying and aggregating data, adding information from internal and external sources, comparing data sets to benchmark or ground truth datasets, and transforming data into reports, visualizations, maps, graphs, or other analytical products. LADOT may process and analyze Processed and Appended Data.

To the best of their abilities, LADOT and its contractors will ensure data subject to automated and manual processing is de-identified and cannot be reverse engineered to reveal individual vehicles, people, or other Personal Information. LADOT and its Contractors are prohibited from combining or treating data in any way that could identify individuals or track their movements. Additionally, LADOT and its Contractors shall not compile or aggregate locations, events, movement patterns, or any Raw Image, Processed, or Derived Data at the individual vehicle or person level that would enable LADOT to track, surveil, model, or predict the movement of individual vehicles or persons. The sole exception is aggregation of enforcement or administrative action history data that is relevant to specific vehicles and registered owners in line with this Policy's retention rules.

Data Ownership

For the purposes of this Policy, LADOT designates Processed and Appended data as "City Data", establishing ownership and assignment through contractual agreements with its Contractors. All City

Data transmitted to, stored, held, and in use by LADOT or its Contractors must follow ITPC Information Handling Guidelines (see Data Designation, Storage, and Protection Requirements section).

Ownership of derived data as produced through program interfaces and applications or through offline analysis using aggregations, compiling, decompiling, joins, and renderings of City Data may be assigned to LADOT or its Contractors depending on who processes or generates the data. LADOT ensures that contractual agreements with Contractors clearly define ownership and responsibilities for derived data.

Data Access

Access to Restricted or Confidential information is strictly limited to Authorized Users, which include only Contractor and LADOT employees, and only for the purposes permitted under this Policy, including enforcement, administrative review, program evaluation, or other legally mandated activities. Unauthorized access, use, or disclosure of Program data is prohibited. This includes access by other city, county, state and federal agencies, including law enforcement agencies except as noted below in the section on Data Sharing.

To maintain compliance, LADOT and its contractors will:

- Maintain access controls and review user permissions as needed.
- Require all Authorized Users to complete mandatory training on data handling and AB 645 requirements.
- Monitor and log all access to Program data and periodically audit these logs for compliance.
- Prohibit the use of unapproved devices, email, or storage systems for Program data.
- Immediately report and respond to any suspected or confirmed breaches of confidentiality.

Data Retention

As a general practice, LADOT archives, anonymizes, or destroys data once it is no longer required or after the applicable retention period has been met. AB 645 sets clear limits for how long speed camera data may be retained to protect privacy and ensure responsible use. Images that are captured and processed by a speed safety system that do not result in the issuance of a violation must be deleted within five (5) days from the date the photo was captured.

For all Program data and images downloaded to City servers that are associated with citations, infractions, or other pre-defined administrative actions, the records may be retained for up to 60 days after the final disposition of the notice of violation. Supporting administrative records, such as calibration logs, may be retained for up to 120 days. Once the retention period expires, all records must be securely destroyed. LADOT may retain information that a vehicle has been cited by the System and fined for a violation for up to three (3) years. All data retention practices as described under this Policy apply to LADOT and its Contractors.

Data Disposal

Data will only be kept for the time required by AB 645 and will be securely disposed of based on industry best practices once that period ends.

Disposal Process

Once the retention period expires, LADOT will securely destroy all Program data to prevent unauthorized access. This applies to both electronic and paper records, including files on computers, laptops, databases, hard drives, collaborative workspaces, on-site data storage, servers, and cloud storage. Acceptable disposal methods include shredding, incineration, overwriting, or physically destroying paper and physical records as well as electronic media. Electronic data is made unrecoverable through techniques such as overwriting, degaussing, or physical destruction. Any Information Technology hardware or documentation that contains sensitive data must be cleared and destroyed before it can be released.

All data destruction is documented, either electronically or manually, to ensure transparency and support auditing. Contractors follow the same standards, maintaining logs of both automated and manual data destruction in line with their contractual obligations.

Enforcement and Administrative Data Disposal

LADOT and its Contractors will ensure that essential enforcement and administrative data required for legally or operationally mandated retention periods are protected and not subject to disposal. Data that has been aggregated, anonymized, or made publicly available may be retained or disposed of in accordance with LADOT policy, provided that Personal Information is removed.

Data Disposal Schedule

LADOT follows a strict data disposal schedule in compliance with AB 645. Photographic evidence collected to issue a notice of speeding violation is retained for up to 60 days after the final disposition of the notice; that is, after the notice has received its official outcome or resolution. Photographic or related data not resulting in a notice of violation is retained for up to five days. Confidential Information received from the Department of Motor Vehicles for the purposes of issuing notices is retained for up to 120 days after the final disposition of the notice of violation. Restricted Information, Internal and Open Data, and data that has been aggregated or anonymized are not subject to specific retention periods but are disposed of or retained according to LADOT policy.

Data Incident, Breach, Notification, and Incident Response

A data incident occurs when confidential or restricted information is exposed or shared with unauthorized parties, lost, damaged, stored improperly, disposed of incorrectly, or discovered to be improperly stored or disposed of. Other types of data breaches may also fall under this category.

LADOT maintains a written log of all incidents and reviews each incident, considering the volume and sensitivity of the data, and determines appropriate notifications. If a breach results in unauthorized

disclosure of Restricted or Confidential Information containing Personal Information, LADOT notifies affected individuals as required by local, state, and federal laws, including the California Consumer Privacy Act (CCPA).

Data Sharing

Third Party Data Sharing

Data that has been aggregated or anonymized may be shared publicly and with other City departments to promote transparency, accountability, and community benefits. This data is only released after applying de-identification or other safeguards to ensure no individual can be identified.

LADOT and its Contractors will not share personally identifiable program data with commercial or private entities. Contractor agreements include confidentiality provisions prohibiting any use beyond the Authorized Use defined in this Policy. Program data may not be sold, published, exchanged, monetized, or disclosed for commercial purposes.

Access to Processed or Appended Data, including Restricted Appended Data, by local and federal law enforcement or other government agencies is not allowed except in the unusual case of a court order, subpoena, or other legal requirement. Such legal requirements do not supersede the retention guidelines noted above. LADOT and its Contractors will not share specific citation events with local external law enforcement agencies and will only provide data as required by law. In the event that the Contractor improperly shares, discloses, or otherwise distributes data, LADOT reserves the right to immediately terminate the contract.

Public Information & CCPRA

Under the California Public Records Act (CPRA, Government Code §§ 6250–6276.48), City records are generally public unless exempted by law. AB 645 specifies that photographic and administrative records from Systems are confidential. These records are not subject to public disclosure and may only be used for authorized purposes or to evaluate system performance. However, certain aggregated data, such as the number of violations issued or vehicle speeds for which violations were issued, is not considered confidential. Such program outcome data is not protected from disclosure under the law and can be disclosed in response to a public records request.

Requests for Public Information are reviewed by the LADOT Program Administrator, with select requests submitted to the City Attorney. All releases follow the Open Data Policy and CPRA while ensuring compliance with AB 645 protections.

Accountability, Oversight, and Auditing

At the direction of LADOT's General Manager, the City and designated staff will regularly conduct audits of the System and all relevant processes, including but not limited to the technology, data processing, data review, and citation processing and adjudication.

Contractors will provide monthly audit logs of overall usage of speed safety camera systems, including:

1. Number of violations detected;
2. Number of violations for which the City issued citations;
3. Geographic distribution of violations detected and issued;
4. Of the violations detected where a citation was not issued, the vendor shall report the reason for non-issuance (e.g., vehicle not actually speeding, license plate unidentifiable or read incorrectly);
5. Any malfunctions, days not in service due to malfunction, and days not in service due to other reasons; and
6. Date and time when Systems were last inspected.

LADOT will establish a clear feedback loop to ensure the Use Policy and System operations are followed, transparent, and continuously improved. A simple reporting process will allow the public, program partners, and staff to raise concerns or suspected violations, all of which will be documented and reviewed. On a regular basis, LADOT will also conduct an independent, third-party audit to assess compliance by LADOT and its contractors, review administrative appeals and outcomes, and identify improvements. Audit findings will inform updates to system operations and the Use Policy to reduce errors, improve fairness, and strengthen public trust over time. Summaries of audit findings will be publicly released.

Enforcement, Violations, Fines, and Appeals

Enforcement and Violations

Under AB 645, Systems issue civil penalties for detected speeding violations rather than criminal charges. A violation occurs when a vehicle exceeds the posted speed limit, and fines are assessed according to the following schedule in Table 2.

Table 2: Schedule of Fines

Fine	Violation
Fifty dollars ($50)	Speeds 11 to 15 miles per hour over the limit
One hundred dollars ($100)	Speeds 16 to 25 miles per hour over the limit
Two hundred dollars ($200)	Speeds 26 miles per hour or more over the limit
Five hundred dollars ($500)	Speeds of 100 miles per hour or more

For a first violation involving exceeding the posted speed limit by 11 to 15 miles per hour, a warning ticket must be issued. In cases where multiple System devices record violations within a 15-minute period, the violation with the highest civil assessment will be issued. Subsequent violations within the same 15-minute interval will result in warnings. No civil penalty will be assessed if the individual is already subject to criminal penalties for the same act, such as being issued a citation in person by an officer for the same speeding event.

Notices are mailed to the registered vehicle owner only, based on rear license plate images. Each notice must include details on the recorded speed, location where the violation occurred, and instructions for contesting the violation. These violations do not add points to the driver's DMV record and generally do not affect insurance. For the first 60 days after a new System is activated, only warning notices will be issued.

Equity Considerations and Alternative Programs

Individuals meeting specific income criteria may be able to pay reduced fines. Those below the federal poverty level may have their citation fines reduced by up to 80%. Individuals with incomes up to 250% of the federal poverty level may have fines reduced by up to 50%.

LADOT will provide a diversion program for eligible individuals, allowing community service in lieu of paying the civil penalty associated with a Systems violation. The program may also offer the option to pay fines over time through a monthly payment plan and income-based discounts, consistent with the income criteria set forth in the Government Code (Section 68632), with eligibility demonstrated through proof of household income at or below applicable thresholds or participation in means-tested public assistance or disability benefit programs recognized under state law.

Due Process and Appeals

AB 645 ensures that vehicle owners have the right to challenge a violation through a clear, transparent process:

- **Review of Evidence**: Vehicle owners may access photographic and event evidence related to the violation.
- **Initial Review**: Vehicle owners may request an initial review of a notice of violation within 30 calendar days of the notice being mailed, using phone, mail, electronic, or in-person methods.
- **Administrative Hearing**: If not satisfied with the outcomes of the initial review, vehicle owners may contest the violation in an administrative hearing within 21 calendar days of the review decision before a neutral decision-maker.
- **Deadlines**: The notice will clearly specify deadlines for submitting a contest or appeal.
- **Transparent Decision Criteria**: Decisions regarding appeals are made using predefined and publicly available standards to ensure fairness.

This process ensures that all Systems enforcement is transparent, accountable, and consistent, while providing drivers with the opportunity to exercise their rights and seek review if they believe a notice was issued in error. Language support is available through the Contractor administering the citation.