Attachment 2

City of Oakland

DRAFT Surveillance Technology Use Policy: Automated Speed Safety System

Description of the Technology

“Speed safety system" or "system" means a fixed or mobile radar or laser system or any other electronic automated detection equipment to detect a violation of speed laws and utilizes cameras to obtain a clear photograph of a speeding vehicle's rear license plate. These cameras are only triggered by speeding vehicles. They do not record data unless triggered by a speeding vehicle.

A. Purpose

The City of Oakland, Department of Transportation (“OakDOT” or “Department”) envisions, plans, builds, operates and maintains a transportation system for the City of Oakland, in partnership with local transit providers and other agencies, and assures safe, equitable, and sustainable access and mobility for residents, businesses and visitors.

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure the surveillance technology employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

B. Authorized Use

The authorized use of the surveillance technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Enforce speed limits on City streets in accordance with California Vehicle Code sections 22425- 22434 (Speed Safety System Pilot Program)
- Analysis of and reporting on speed enforcement, as required under the Speed Safety System Pilot Program.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

OakDOT may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.

C. Data Collection

Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including Personal Identifiable Information (PII), shall be classified according to the City's Data Classification Standard.

The Surveillance technology collects some or all of the following data type(s):

Data Type(s)	Format(s)	Classification
Digital Images of rear license plate	Photographic, JPEG	Level 3

D. Data Access

All parties requesting access must adhere to the following rules and processes:

- Authorized users must complete mandatory training and obtain login credentials.
- Only authorized users may use ASE technology or access data.
- Authorized users must log into tablet or computer, as applicable, to access ASE technology data.

a. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology but only may do so on a need- and right-to-know basis due to their direct involvement in the implementation of the program:

- Public Service Representative
- Senior Public Service Representative
- PSE 14
- Program Analyst I-III
- Project Manager I (Speed Camera Program Manager)
- Senior Transportation Planner (speed camera program management)

Commented [SA1]: does Oakland have one?

Commented [RC2R1]: @Ford, Michael can you help us with this please?

Commented [FM3R1]: We should consult with Felicia Verdan and the City's Privacy Advisory Commission for the latest

Commented [DJ4]: I want to make sure it doesn't appear as if any PSR can have access. only those with a need and right to know.

b. Members of the public

Department will comply with the California Public Records Act, the requirements of the federal and State Constitutions, federal and State civil procedure laws and rules, and the privacy provisions specified in Assembly Bill 645.

Collected data that is classified as Level 1- Public data - may be made available for public access or release. Members of the public may also request access by submission of a request through Oakland's NextRequest platform. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

E. Data Protection

Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity frameworks selected by the department.

Department shall ensure compliance with these security standards through the following:

Administrative Safeguards: The Department will secure any PII against unauthorized access, processing, disclosure, and accidental loss, destruction, or damage. ASE data collected and retained by the Department will be protected by the safeguards appropriate for its classification level(s).

To protect ASE data from unauthorized access and control, including misuse, the Department shall, at minimum, apply the following safeguards:

- Authorized users will use login credentials with MFA, if available, and use complex passwords to access the ASE technology.
- All access to and activity in the ASE system will be logged and be audited.

F. Data Retention

Data will be stored in the following locations and encrypted at rest (at the following locations):

|X| Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)

|X| Software as a Service Product

| |Cloud Storage Provider

The retention schedule for data generated by the surveillance technology is prescribed by California Vehicle Code section 22425(l), as follows:

Retention Period	Retention Justification
Photographic evidence: up to 60 days after final disposition of notice of speeding violation; up to five days if no notice of speeding violation is issued.	Retention period established under California Vehicle Code section 22425(I).
Confidential information received from the Department of Motor Vehicles to issue notice of violation: up to 120 days after final disposition of notice of speeding violation.	Retention period established under California Vehicle Code section 22425(I).

Exceptions to Retention Period – Department does not plan to retain data beyond what is described in the retention period above.

Data Disposal – Upon completion of the data retention period, Department shall dispose of data in the following manner:

- Upon completion of the applicable data retention period, the Department will automatically dispose of raw ASE data (e.g., ASE data that has not been anonymized or aggregated).
- In accordance with the California Vehicle Code section 22425(I)(3), photographic evidence and other confidential information from DMV will be destroyed in a manner that maintains the confidentiality of any person included in the record or evidence.

G. Public Access

See description in section D under “Members of the Public”.

H. Third Party Data Sharing

In accordance with California Vehicle Code section 22425(l)(1), data, including photographic or administrative records, made by the surveillance technology shall be confidential and shall not be shared unless required by law. The Department shall use and allow access to such data only for the purposes authorized under section 22425.

a. Internal Data Sharing:

The department will not share surveillance technology data with other departments or entities inside the City of Oakland, except for anonymized speed-related data with other

Safe Oakland Streets departments, such as the Oakland Police Department, the Department of Race and Equity, and the City Administrator's Office.

b. External Data Sharing:

The department will not share surveillance technology data externally with entities outside the City of Oakland unless a warrant/subpoena was issued.

I. Training

To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access will receive training on data security policies and procedures.

OakDOT shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses dictated by this policy. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

The Department will ensure employees and vendors are trained on how to use the ASE technology correctly and ensure ASE data is used for its intended use only.

Training includes explaining how employees and vendors can use data and how to report problems with the ASE system.

J. Auditing and Oversight

Department Compliance

The Department will assign the positions listed below to oversee, or assign staff members under their direction to oversee, compliance with this Policy:

- Project Manager/Director of Parking and Mobility Unit
- Project Manager, OakDOT Speed Safety Camera Program

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

In accordance with California Vehicle Code section 22425(l)(5), information collected and maintained by the Department using the surveillance technology shall not be disclosed to any other persons, including, but not limited to, any other state or federal government agency or official for any purpose, except as required by state or federal law, court order, or in response to a subpoena in an individual case or proceeding.

Oversight Personnel

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties.

- Project Manager/Director of Parking and Mobility Unit
- Project Manager, OakDOT Speed Safety Camera Program

Sanctions for Violations

Sanctions for violations of this Policy include the following:

- Violations of this Policy may result in disciplinary action commensurate with the severity of violation. Sanctions include written warning, suspension, and termination of employment.

K. Maintenance

OakDOT and its future vendor under contract to operate speed cameras will adhere to the data security requirements and PII collected under AB-645 as outlined above.