California Air Resources Board Automated License Plate Reader Privacy and Usage Policy

Introduction

The California Air Resources Board (CARB) collects emissions information for research and enforcement. Sometimes data is collected at the roadside from a large number of trucks. CARB is developing a new system, called the Portable Emissions AcQuisition System (PEAQS), which measures emissions as cars or trucks pass sensors. PEAQS is equipped with an Automated License Plate Reader (ALPR) and will be used to assess the distribution of emissions by model year, make/model, and technology type from cars and trucks. This is necessary for investigating tampered or malfunctioning vehicles air monitoring, fleet characterization, identifying the effectiveness of ARB regulations, and future policy recommendations. PEAQS will be used as a screening tool to identify high emitting vehicles for inspection in the field or a fleet-level investigation. If CARB expands the use of PEAQS beyond screening methods, it will do so following a public process.

The ALPR system component is a mobile or fixed camera that is combined with sophisticated computer software to capture and record a vehicle's license plate information. These systems typically operate by photographing an image of a license plate, using optical character recognition (OCR) software to convert the image into the alpha-numeric characters of the license plate, and then comparing the alpha-numeric data to data held in other databases. ALPR systems capture other data as well, including the geographic location of a license plate and the time and date that the license plate was scanned. The ALPR systems can also provide a "contextual" photo of the car itself, making information about car make and model, distinguishing features, state of registration, and driver and passenger potentially available. The ALPR system does not identify a specific person.

The photograph the system generates is not considered "personally identifiable information" (PII) because it does not contain an individual's first name or first initial and last name, and it is not paired with data elements such as an individual's social security number, or driver's license number. However, the data generated from the photograph with the use of an ALPR system can be linked to an identifiable person through a registration database, such as the Department of Motor Vehicles (DMV). When ALPR information is cross referenced with DMV registration data, it provides make/model, and model year along with the registered owner information. ARB has a long history of managing DMV data and adheres to DMV data management requirements as outlined in the DMV Information Security Agreement (DISA), and the ARB Information Security Manual (ISM).

Requirements

ARB's ALPR Privacy and Usage Policy incorporates the requirements of Civil Code sections 1798.29, 1798.82, and 1798.90.5, et seq., which requires all public agencies

that operate an ALPR system shall maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards to protect ALPR information from unauthorized access, destruction, use, modification or disclosure. At a minimum, public agencies must:

- Implement a usage and privacy policy that ensures all public agencies collect, use, maintain, share, and disseminate ALPR information in an authorized and secure manner.

- Disclose any breach of security of the data to any affected resident of California, consistent with the requirements of Civil Code section 1798.29.

- Provide an opportunity for public comment at a regularly scheduled public meeting before implementing the program.

The ALPR Privacy and Usage Policy is available to the public in writing, and is posted on ARB's Internet Web site at: https://www.arb.ca.gov/enf/policy2017.htm

Policy

- ALPR information will be collected only for the purposes of research, regulation development and implementation, emissions inventory, or enforcement.
- ARB will designate a custodian responsible for ALPR data and the effective implementation of this policy.
- Only trained and authorized staff will generate, store, access, or analyze ALPR information.
- ALPR information will be stored only on limited access and encrypted drives that meet state standards for storing data, including but not limited to NIST Cryptographic Module Validation Program or equally protective standards that are generally accepted.
- ARB staff will maintain records of each staff person that generates, stores, accesses, or analyzes ALPR data consistent with Civil Code section 1798.90.52.
- ARB will provide training to each staff person that ensures the security of the information and compliance with applicable privacy laws.
- ALPR information will not be sold, shared, or transferred to other persons outside of ARB, except for the following purposes:
    - Law enforcement agencies for authorized law enforcement purposes.
    - Public agencies that have signed a confidentiality agreement and agreed to keep the information confidential.
- ALPR information that has been cross referenced to DMV registration information will be treated as DMV registered data.
- ALPR information will be retained and destroyed consistent with ARB's file retention policy.

- Aggregate data, vehicle make, model, model year, and technology emissions information are not considered confidential information.

Procedures

- The assigned ALPR data custodian is ARB's Chief Information Officer (CIO), or designee. The ALPR custodian will monitor the ALPR system and ensure the security of the ALPR information by:
    - Maintaining a log for each time the ALPR information is accessed between operators and users.
    - Verifying only authorized users have access to ALPR information by conducting periodic audits of access and usage.
    - Ensuring each ALPR operator and user has taken all required training before accessing ALPR information.
- All authorized ALPR system operators, users, and custodians must receive training, which will be part of the DMV data security training and include:
    - A security briefing presentation.
    - A signed confidentiality acknowledgement form, which confirms that they have received and understand all ALPR policies and procedures.
- The custodian will keep a list of trained users and operators that includes name, title, and contact information and will be updated annually.
- ARB staff will view the image of the license plate and cross reference it with the information produced by the ALPR system to confirm that the image of the license plate was correctly recognized by the ALPR system. If a data error is found, ARB staff will correct the error in the database and notify management.
- All ALPR users, operators, and custodians must document access to ALPR information in a usage log and it must contain the following information:
    - The date and time the information is accessed.
    - The license plate number or other data elements used to query the ALPR system.
    - The username of the person who accesses the information.
    - The purpose for accessing the information.
- The log is maintained electronically at their workstation, and is submitted to the custodian on a quarterly basis.
- In the event of a data security breach involving ALPR data, ARB staff will notify ARB's ISO, who will take the following steps:
    - Notify the subject of the security breach in accordance with the requirements of section 1798.82 of the Civil Code.
    - Follow the procedural requirements of the Statewide Information Management Manual (SIMM).

Changes to the Policy

ARB reserves the right to revise this policy at any point in the future and such changes will be retroactively applicable to data collected prior to any revision of this policy. When ARB revises the ALPR Privacy and Usage Policy, the "last updated" date at the top of the ALPR Privacy and Usage Policy will reflect the date of the last change. We encourage visitors to review this ALPR Privacy and Usage Policy periodically.