City of Seattle

2020 Surveillance Impact Report Executive Overview

Automated License Plate Readers (ALPR) (Patrol)

Seattle Police Department

City of Seattle

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Police Department's (SPD) Automated License Plate Reader (ALPR) system. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

Note: All use of ALPR as described in this document and the SIR is governed by SPD Policy 16.170

1.0 Technology Description

The Seattle Police Department has nineteen vehicles with ALPR. Eleven of these are Patrol vehicles and three are Scofflaw Enforcement vehicles. ALPR hardware consists of high definition infrared digital cameras that are mounted on eleven Patrol cars (one of which is unmarked).

The high-speed cameras capture images of license plates as they move into view, and associated software deciphers the characters on the plate, using optical character recognition. This interpretation is then immediately checked against any license plate numbers that have been uploaded into the onboard, in-vehicle software system.

2.0 Purpose

Operational Policies:

> **ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:**
> 1. **Locating stolen vehicles;**
> 2. **Locating stolen license plates;**
> 3. **Locating wanted, endangered or missing persons; or those violating protection orders;**
> 4. **Canvassing the area around a crime scene; and**
> 5. **Locating vehicles under SCOFFLAW**

Seattle Police Department uses Automated License Plate Reader (ALPR) technology to recover stolen vehicles, to locate subjects of Amber and Silver Alerts and fugitives where vehicle license plate information is available, to assist with active investigations, to facilitate the flow of traffic (by monitoring and enforcing City parking restrictions) and for Scofflaw Ordinance enforcement.

Patrol ALPR assists the City in locating and recovering stolen vehicles. ALPR systems may assist with active investigations by helping to determine the location of vehicles of interest – specifically those that have been identified as being associated with an investigation. SPD uses ALPR to recover stolen vehicles, which are often used by thieves in committing other crimes.

3.0 Data Collection and Use

Operational Policy:

> **ALPR technology collects digital images of license plates and associated license plate numbers. The technology collects the date and time that the license plate passes a digital-image site where an ALPR is located.**

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location.

All ALPR-equipped vehicles upload a daily HotList from the Washington State Patrol that contains national stolen vehicle plate data published daily by the FBI. The Washington State Patrol places the HotList file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. The receiving local law enforcement may supplement the list with additional information, such as vehicles sought with reasonable suspicion that they are involved in an incident or vehicles sought pursuant to a warrant.

4.0 Data Minimization & Retention

Operational Policies:

> **ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.**

When the ALPR system registers a hit, a match to a license plate number listed on the HotList (as described in 2.3 above), the user must verify accuracy before taking any action. For instance, when the system registers a hit on a stolen vehicle, the user must visually verify that the system accurately read the license plate and, if so, must then contact Dispatch to verify accuracy of the hit – that the vehicle is actually listed as stolen. Only then does the user act.

Unless a hit has been flagged for investigation and exported from the database for this purpose, all captured data is automatically deleted after 90 days, per department retention policy. Data related to a flagged hit is downloaded and maintained with the investigation file for the retention period related to the incident type.

5.0 Access & Security

Operational Policies:

1. **Only Employees Trained in the Use of ALPR Equipment Will Use and Access ALPR Devices and Data**
2. **Employees Accessing ALPR Data Must Login Through the ALPR Password-Protected System**
3. **Employees Conducting Searches in the ALPR System Will Provide a Case Number and Justification for the Search**
4. **Employees Will Not Share ALPR Passwords and Login Credentials**
5. **The Department will store ALPR data in a secured law enforcement facility with multiple layers of security protection. Firewalls, authentication and other reasonable security measures will be utilized. Only trained Department employees can access stored ALPR data and all data search requests are logged within the system.**
6. **ALPR data maintained on BOSS will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:**
   (a) **Search of specific or partial plate(s) and/or vehicle identifiers as related to:**
   (b) **A crime in-progress;**
   (c) **A search of a specific area as it relates to a crime in-progress;**
   (d) **A criminal investigation; or**
   (e) **A search for a wanted person; or**
   (f) **Community caretaking functions such as, locating an endangered or missing person.**
   (g) **Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.**
   (h) **Administration and maintenance**

Access

Prior to gaining access to the ALPR system, potential users must be trained by other trained officers. Once this training has been verified with the ALPR administrator, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remained logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable. Officers are assigned the vehicles to use while on-shift.

Security

All data collected from the ALPR system is stored, maintained, and managed on premises. ALPR systems maintain access logs on backend servers that are accessible for audit The Office of Inspector General may access all data and audit for compliance at any time.

City of Seattle

6.0 Data Sharing and Accuracy

Operational Policy:

> **ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.**

SPD has no data sharing partners for ALPR. No person, outside of SPD, has direct access to the PIPS system or the data while it resides in the system or technology. ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. SPD does not pool its ALPR data with any other agency's data.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed by the Legal Unit pursuant to the applicable Rules of Civil or Criminal Discovery or the Washington Public Records Act, **Chapt. 42.56 RCW**. The Legal Unit will maintain requests for ALPR data by non-law enforcement or non-prosecutorial agencies.

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

7.0 Equity Concerns

Operational Policy:

> **ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.**

ALPR is content-neutral; it does not identify the race of the driver or the registered owner of the vehicle. To ensure that SPD continues to build trust with community members and increase racial equity, SPD must continue to follow its policy of limiting use of the ALPR cars to strictly routine patrol and use of collected ALPR data to specific criminal investigations or community caretaking functions, as well as limiting access to the ALPR system to authorized SPD personnel. Further, SPD must also continue to audit the system on a regular basis to provide a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity and minimize perceived oversurveillance of areas where historically targeted communities reside or congregate.