Policy Revision Request

Requestor Name Jerry Cantu Emp # 6111

This revision applies to Existing Policy

If new, recommended section

This revision is necessary to comply with Best Practices

Whom does this revision affect? Department

This revision has an unbudgeted financial impact of $

Brief reason for the revision:
The revision is needed to ensure alignment with the resolutions and to incorporate updated documentation and contact information.

---

344 Automatic License Plate Reader

344.1 PURPOSE AND SCOPE

To provide rules and guidance for capturing, storing, and using digital data obtained through Automated License Plate Reader systems. This General Order incorporates the safeguards and restrictions mandated by City of Austin Resolution 20220915-056 and 20230608-085.

344.2 DEFINITIONS

(a) **Automated License Plate Reader (ALPR)** - A camera system that automatically photographs and stores license plate numbers, date, time, and location information. ALPRs may be permanently fixed, portable trailer-mounted, or vehicle-mounted.

(b) **Chief Security Officer (CSO)** - Responsible for receiving daily alerts on login attempts, limiting access to the license plate database for only permissible use, and/or regularly monitoring access to data stored under this General Order.

(c) **Hot List** - A cross-reference from vehicle license plate scans with information associated with vehicles of interest. This list includes information entered by the Department or provided by the Texas Law Enforcement Telecommunication System (TLETS) and maintained by the Texas Department of Public Safety. The information on the hotlist is limited to license plates listed as stolen, BOLOs issued by APD only, SILVER, and AMBER alerts, wanted individuals with any Class A offense or greater warrant, Class B and Class C hate crimes, or Class B and Class C sex crimes (DOC Window Peeping, Indecent Exposure.)

344.3 PROCEDURE

344.3.1 MANAGEMENT OF ALPR

(a) The Auto Theft Interdiction Unit will manage the ALPR program.
    1. The Chief Security Officer is the ~~Sergeant~~ Lieutenant of the Auto Theft Unit.
(b) Operators encountering problems with ALPR equipment or programs shall notify the CSO.

344.3.2 ASSIGNMENT, USE, AND LOCATIONS OF ALPR SYSTEMS
(a) Real time Crime Center (RTCC) personnel will:
    1. ~~personnel will m~~Monitor all ALPR systems.
    2. ~~All RTCCpersonnel will b~~Be trained in the use~~ing~~ of ~~and interpreting~~ ALPR systems; along with Austin Regional Intelligence Center (ARIC).
    3. ~~RTCC will e~~Either dispatch alerts received, generally broadcast (GB) them, or notify patrol.
    ~~1.~~4. Receive license plate information for entry in to the Hot List, ensure the entry complies with this order limitations specified in 344.2 (c), and enter all customized ALPR entries in to the Hot List, including BOLOs issued by APD only.
(b) An ALPR alert alone, including an alert sent by RTCC, does not create reasonable suspicion to justify a traffic stop or the detention of an individual. Before making a stop or detention, the officer shall:
    1. Make a visual confirmation that the license plate actually matches the information captured by the ALPR and reported in the corresponding alert.
    2. Confirm the license plate information with the National and Texas Crime Information Centers (NCIC/TCIC).
    ~~2.~~3. Officers will only take enforcement action after they have confirmed that the hit complies with the limitations specified in this order and the City of Austin Resolutions 20220915-056 and 20230608-085.
    ~~3.~~4. In the absence of exigent circumstances and if it is safe and reasonable at the time, a second officer at any rank shall verify that the license plate matches the suspect vehicle before taking any enforcement action or entering into the hotlist.
        (a) Investigators conducting follow-up investigations shall always use a second officer to verify the license plate match before taking any action.
    5. Officers conducting a traffic stop based on a confirmed ALPR alert shall consider the level of risk associated with the nature of the offense and ensure that their response complies with all applicable laws and General Orders.
(c) Employees shall adhere to the following documentation guidelines:
    1. Utilizing the ALPR Dashboard Smartsheet located in SharePoint, the employee shall submit one of the following forms:
        (a) ALPR Hit Stop Form
            1. When an officer uses ALPR to conduct or attempt a stop, the officer shall write a report and submit an ALPR Hit Stop Form. In the Versadex report, the officer should reference a Smartsheet form that was submitted.
        (b) ALPR Manually Entered LP Form
            1. Only a Real Time Crime Center (RTCC) Lieutenant can enter a license plate into a Hot List.
            2. This form is used when an employee requests a license plate be entered into the Hot List. The employee requesting and the employee approving the request shall write a supplement to the case number.
        (c) ALPR Sharing and Preservation Requests Form
            1. Employees receiving ALPR sharing and preservation requests shall follow 344.5 Release of Data.

2. This form is used when an employee receives a request for ALPR sharing and preservation of data. If the request is regarding an APD case, the employee shall write a supplement.

~~(c)~~(d) The Chief Security Officer, along with the Police Technology Unit (PTU) and Research and Planning, shall place permanent ALPR cameras at different locations across the city, ensuring that their deployment does~~n't~~ not disproportionately target any group or segment of our community.

344.4 SAFEGUARDS

(a) Prohibited uses:

1. When using ALPR systems, officers shall not target any person based on their actual or perceived race, color, religion, creed, sex, gender, gender identity, sexual orientation, age, national origin, ethnicity, disability, veteran status, marital status, partnership status, pregnancy status, political affiliation or beliefs, and, to the extent permitted by law, alienage or citizenship status.
2. Users shall not employ ALPR systems to intimidate or harass any individual or group.
3. Employees shall not obtain, attempt to obtain, or convert any data obtained with ALPR for their personal use or the unauthorized use of another person. Department personnel shall only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this General Order.
4. Unless there is a criminal nexus, officers shall not use the ALPR system or use, retain, or transmit license plate reader data to investigate persons who are, or were, exercising their First Amendment right, including freedom of speech, assembly, association, and exercise of religion, such as attending political rallies, organizational meetings, public demonstrations, and religious gatherings.
5. The Department shall not use or operate ALPR systems or data for warrant round-up operations, operations focused on collecting past due traffic fines, Class C Misdemeanors (other than those listed in this order 344.4 (c)), or any other similar purpose of generating revenue or collecting money owed by the public.
6. The Department shall not use ALPR systems or data to conduct criminal investigations on immigration status or access to reproductive health services to the extent legally possible.
7. Any alleged misuse or inappropriate application of ALPR operations, information, data, or software is investigated per GO 902 Administrative Investigations and subject to appropriate disciplinary action if the allegation is substantiated.
8. The Department shall only use ALPR systems and data for offenses limited to license plates listed as stolen, BOLO, SILVER, and AMBER alerts, wanted individuals with any Class A offense or greater warrant, Class B and Class C hate crimes, or Class B and Class C sex crimes (DOC Window Peeping, Indecent Exposure.)

(b) If any officer or employee reasonably believes that another law enforcement agency has used or is using APD ALPR systems or data in a manner that violates the "Prohibited Uses" identified herein, the officer or employee shall report that information to the Auto Theft Interdiction Unit Lieutenant. The Lieutenant shall review the possible violation and determine if sharing ALPR data with the outside agency will continue.

(c) The Chief Security Officer shall oversee access to the ALPR database and shall limit roles and access and the need for access. The CSO shall closely coordinate with CTM to ensure the implementation of the best data security and storage practices for all ALPR

data. The Department shall store all collected ALPR data on a designated ALPR server unless investigators retain and save the data for a criminal investigation.

(d) Server operators shall purge ALPR data from the designated ALPR server seven (7) days after an ALPR collects it. The retention period for ALPR data shall comply with state law. All logins and transactions are logged within the ALPR system and audited to ensure proper use and whether there is a criminal predicate.

(e) For ALPR data related to ongoing criminal investigations or criminal investigations that contain ALPR as evidence, investigators shall download and record the relevant ALPR data into the case file.

(f) The Department shall retain all ALPR data related to an endangered person, missing person, or criminal investigation for a period consistent with the City Code, Chapter 2-11, and any applicable City Records Control Schedules and/or the State Local Government Retention Schedules.

(g) When an officer takes any action due to an ALPR alert, but it is later discovered that they acted on the wrong vehicle due to an error in data entry, fictitious or swapped license plates, or interpretation of the license plate, the officer shall email the incident details to their supervisor and Risk Management at apdriskmanagment@austintexas.gov before the end of their shift. Risk Management shall include this data in the next quarterly audit, per GO 344.6 Audit.

344.5 RELEASE OF DATA

(a) ALPR data shall not be distributed, sold, or transferred to any non-law enforcement entities.

(b) To the extent legally possible, data sharing with other law enforcement agencies shall only occur for offenses limited to license plates listed as stolen, BOLO, SILVER, and AMBER alerts, wanted individuals with any Class A offense or greater warrant, Class B and Class C hate crimes, or Class B and Class C sex crimes (DOC Window Peeping, Indecent Exposure~~.)~~

(c) Requests for ALPR data shall be processed in accordance with the Texas Government Code, Chapter 552, and GO 116 Security and Release of Records and Information. If required by law to share or disclose this data, the Department shall supply the requested information for a specific case or investigation only to the extent legally required.

~~(c)~~(d) ~~An o~~Outside users requesting information outside of regular business hours~~,~~ will contact ~~the Real Time Crime Center (~~RTCC~~).~~ ~~If your~~ Outside users requesting information ~~falls inside~~ during regular business hours ~~, then~~ shall contact the ~~Austin Regional Intelligence Cetner (~~ARIC~~).~~

~~(d)~~(e) If any employee receives a request from an outside agency broader than a specific case or investigation, they shall report that request to the Chief Security Officer. The CSO shall follow the direction outlined in Austin City Council Resolution 20220915-056 section 3.

(f) Before receiving any license plate reader data, a requesting agency must execute an agreement or memorandum of understanding to abide by the requirements of the Austin Police Department (APD) written administrative policy and procedure for license plate readers and the APD General Orders in the use, handling, and preservation of the data, including but not limited to the limitations on the sharing of the data, and agree that all data received will be promptly destroyed upon the conclusion of an active criminal or missing or endangered person case and that notice of such destruction shall be promptly provided to APD.

344.6 AUDIT

The Risk Management Unit will conduct audits of the ALPR system. They will present the audit results to the Chief of Police or their designee, which may be public information as allowed by law. At minimum:

(a) The Risk Management Unit will perform a quarterly random audit of the system to ensure compliance with policies and procedures.

(b) This audit shall include, but is not limited to:
   1. The number of license plates scanned.
   2. The names of the lists against which captured plate data were checked, and the number of confirmed matches and the number of matches that, upon further investigation, did not correlate to an alert.
   3. The number of matches resulted in the arrest, prosecution, or the location of a missing or endangered person.
   4. The number of preservation requests received broken down by the number of requests by a governmental entity versus by a defendant.
   5. The number of data sharing requests received, granted, and denied broken down by agency and offense.
   6. The number of data sharing requests resulting in arrest, prosecution, or the location of a missing or endangered person.
   7. The number of manually-entered license plate numbers under Austin City Council Resolution 20220915-056 Section 1, broken down by reason justifying the entry, and the number of confirmed matches and the number of matches that, upon further investigation, did not correlate to an alert broken down by user access roles.
   8. Any changes in department policy that affect privacy concerns.
   9. License plate hits, categorized by zip code and sector, and the type of camera that captured the data.
   10. Data gathered during a detention that does not result in an investigation of this order 344.4(g).
   11. Information regarding the race and gender of the driver of any vehicle detained as a result of ALPR action.
   12. Information regarding the race and gender of the reported victim of the crime as a result of ALPR action.
   13. Information regarding the offense under investigation as a result of ALPR action.

(c) The Risk Management Unit will assist the City Auditor or an external party directed by the City Auditor with Audits. Information shared for the purposes of this audit is not subject to section 344.5 (a) above.

344.7 TRAINING

(a) Any personnel utilizing the ALPR system shall complete annual training on the policies and restrictions regarding ALPR use, data handling, and processing requests for ALPR data. Among other topics, this training shall cover:
   1. Appropriate use and collection of ALPR data and emphasize the requirement to document the reason for the inquiry;
   2. General Order 344.4 Safeguards;
   3. Examples of negative consequences resulting from misuse; and
   4. A clear explanation and warning indicating that the person currently operating the vehicle may not be the individual associated with the Hot List alert, despite the license plate's inclusion in the list.

(b) Employees shall only access, use, view, or otherwise participate in the ALPR program when the employee completes this annual training. Employees who have previously completed the training but fail to timely complete subsequent annual training shall have their access to ALPR systems revoked until they complete the required training.