OFFICE OF
POLICE OVERSIGHT

TO: Jesús Garza, Interim City Manager

FROM: Sylvia Hardman, Interim Director

DATE: March 31, 2023

SUBJECT: **Preliminary Analysis of APD's Proposed License Plate Reader Policy and Processes**

In accordance with directives from the City Manager's Office in relation to Resolution No. 20220915-056 (Resolution 56), the Office of Police Oversight (OPO) has conducted a preliminary analysis of the proposed policy for Automatic License Plate Readers (ALPRs), which the Austin Police Department (APD or the Department) provided to OPO on Thursday, March 16, 2023. As part of this process, OPO met and communicated with APD to discuss our questions, concerns, and recommendations.

In summary, OPO finds that the proposed ALPR policy and processes are still in a state of development and may not yet be ready to support the use of ALPR systems in accordance with the letter and intent of Resolution 56. As a result, OPO recommends that APD take additional time to develop its policy and processes, focusing on areas including, but not limited to, the following:

- Adherence to Resolution 56, especially the incorporation of meaningful community input and the 11 enumerated safeguards;
- Further development and implementation of front- and back-end solutions to mitigate and analyze disparate impacts from the placement and use of ALPRs;
- Clear processes and accountability for all APD personnel handling ALPR systems and data; and
- Balance between enhanced protocols for data privacy and the need for effective audits.

Attached to this memorandum is OPO's preliminary assessment, which includes our initial findings, recommendations, and remaining questions. We have also provided a copy of APD's proposed policy.

In conclusion, additional time may be necessary to fully assess and execute the remaining actions necessary to realize the letter and intent of Resolution 56. Please contact OPO if you have any questions or would like additional information.

Enclosures:
1. OPO's analysis of APD's proposed ALPR policy
2. APD's proposed ALPR policy

cc: Bruce Mills, Interim Assistant City Manager
Joseph Chacon, Chief of Police
Jeff Greenwalt, Assistant Chief

OFFICE OF
POLICE OVERSIGHT

Analysis of the Austin Police Department's Proposed Policy on Automatic License Plate Readers (General Order 344)

Introduction

Based on Resolution No. 20220915-056 (Resolution 56), the City Manager's Office directed APD "to re-evaluate its former policy and/or procedure on license plate readers; work with the Office of Police Oversight and coordinate a minimum of two community input sessions related to the policy; and take appropriate steps to ensure the policy and/or procedure includes, but is not limited to," 11 enumerated safeguards.[1] Resolution 56 also directed that the City of Austin Chief Security Officer be consulted in the development of these provisions.[2]

OPO conducted a preliminary review of APD's proposed ALPR policy and procedures based on the following:

A. The meaningful solicitation and incorporation of community input;
B. The 11 enumerated safeguards from Resolution 56;
C. Additional safeguards based on OPO's research into best practices;
D. The potential for APD to acquire Axon Fleet 3 dashboard cameras, which are equipped with ALPR technology that APD has reported it will utilize if approved by City Council;
E. Miscellaneous areas for policy language improvement; and
F. Unanswered questions after meeting with APD.

What follows is a discussion of the proposed ALPR policy and procedures as they relate to each of these considerations.

A. Community Input

Resolution 56 directed APD to "work with the Office of Police Oversight and coordinate a minimum of two community input sessions related to the policy."[3] In accordance with Resolution 56, OPO did advise APD on the planning of its community input sessions, and APD independently executed the sessions. However,

[1] Resolution 20220915-056, Austin City Council (September 15, 2022), accessed March 27, 2023, https://www.austintexas.gov/edims/document.cfm?id=392730.
[2] Resolution 20220915-056.
[3] Resolution 20220915-056.

the execution of the community input sessions significantly limited the community's ability to provide meaningful input on the ALPR policy.

February 7th Meeting[4]

APD hosted the first community meeting virtually via Zoom on February 7, 2023, and approximately eight to ten community members attended. Importantly, the Zoom link promoted on social media did not work properly; OPO staff, the Vice Chair of the Public Safety Commission, and one community member all reported that they could not join the meeting with the link provided. Since the link was not working correctly, it is likely that other community members were unable to participate due to their inability to access the meeting.

Additionally, this meeting was "Zoombombed" by bad actors who disrupted APD's presentation by screen-sharing pornographic images and sending obscenities via the chat function. While APD staff regained control of the meeting, they subsequently limited access to the microphone and chat functions as a precaution. As a result, community members could not ask questions directly, which impacted their ability to get answers and engage in substantive dialogue during the meeting.

The full length of the meeting was under 30 minutes.

As planned, this meeting was recorded. However, it was ultimately not shared publicly.
The planned purpose for sharing the recording was to make information accessible to those who were unable to attend the meeting and (1) generally wanted to be informed or (2) wanted to be informed in preparation for the second meeting.

Unfortunately, the second meeting was negatively impacted by the fact that neither the event recording nor the PowerPoint slides were shared publicly after the meeting.

February 22nd Meeting

APD hosted the second meeting in person at the Permitting and Development Center on February 22, 2023, and approximately five community members attended. This meeting was meant to be a continuation of the February 7th meeting and focus on gathering input about the ALPR policy language.

APD shared a draft of the ALPR policy with attendees at the meeting, however, the February 7th meeting recording was not shared publicly and APD did not review the information provided at the first meeting or share a copy of the PowerPoint presentation from that meeting. Additionally, OPO can only confirm that one person attended both meetings, and some community members told OPO that they lacked the background information required to have an informed opinion on the policy.

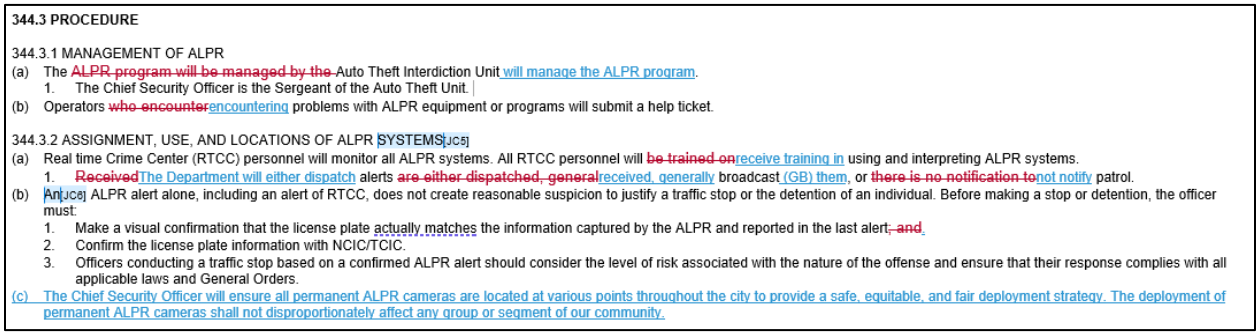
In summary, the two events fell short of the community input requirements outlined in Resolution 56.

[4] Initially, the first meeting was planned as an in-person event to be held on January 31, 2023. This event would have been followed by a final meeting on February 7, 2023. The January 31st event was cancelled due to the winter storm.

Changes Made to Policy After Community Input Meetings

As part of OPO's review, we compared the draft policy presented at APD's community meetings and the policy sent to us for review. While changes were made to the policy, there were few substantive changes. Most of the changes rephrased old language for grammatical purposes. Below are a few examples.

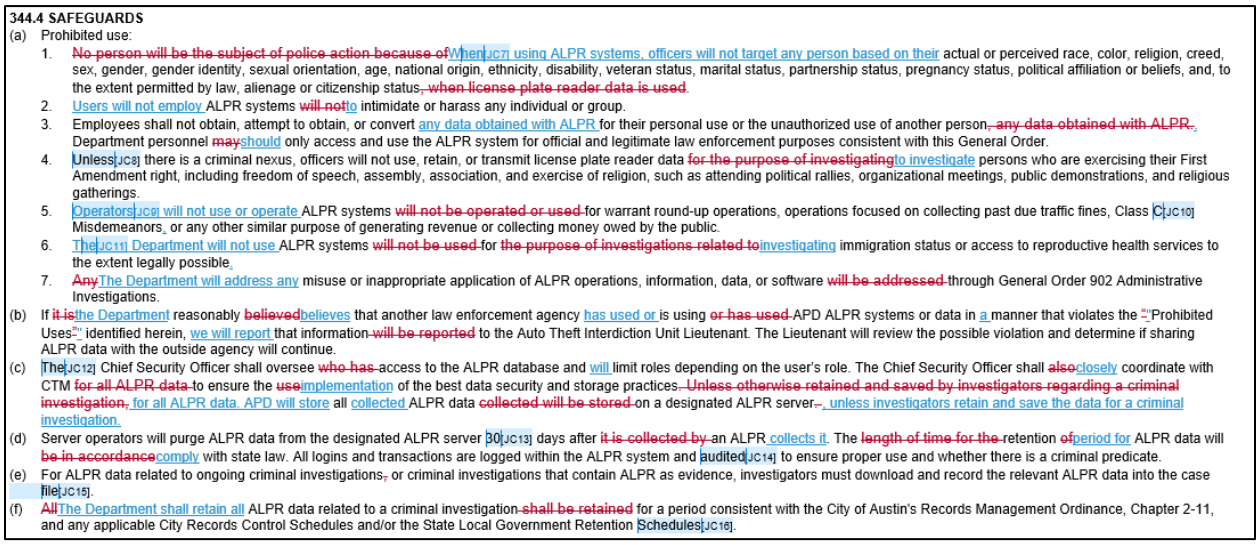
Key:
~~Text~~ = Policy language presented to the community and removed from draft sent to OPO
Text = Policy language added after policy was presented to the community



344.3 PROCEDURE

344.3.1 MANAGEMENT OF ALPR
(a) The ~~ALPR program will be managed by the~~ Auto Theft Interdiction Unit will manage the ALPR program.
1. The Chief Security Officer is the Sergeant of the Auto Theft Unit.
(b) Operators ~~who encounter~~encountering problems with ALPR equipment or programs will submit a help ticket.

344.3.2 ASSIGNMENT, USE, AND LOCATIONS OF ALPR SYSTEMS[JC5]
(a) Real time Crime Center (RTCC) personnel will monitor all ALPR systems. All RTCC personnel will ~~be trained on~~receive training in using and interpreting ALPR systems.
1. ~~Received~~The Department will either dispatch alerts ~~are either dispatched, general~~received, generally broadcast (GB) them, or ~~there is no notification to~~not notify patrol.
(b) An[JC6] ALPR alert alone, including an alert of 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 must:
1. Make a visual confirmation that the license plate actually matches the information captured by the ALPR and reported in the last alert~~, and~~.
2. Confirm the license plate information with NCIC/TCIC.
3. Officers conducting a traffic stop based on a confirmed ALPR alert should 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) The Chief Security Officer will ensure all permanent ALPR cameras are located at various points throughout the city to provide a safe, equitable, and fair deployment strategy. The deployment of permanent ALPR cameras shall not disproportionately affect any group or segment of our community.



344.4 SAFEGUARDS
(a) Prohibited use:
1. ~~No person will be the subject of police action because of~~When[JC7] using ALPR systems, officers will 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~~, when license plate reader data is used~~.
2. Users will not employ ALPR systems ~~will not~~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~~, any data obtained with ALPR~~. Department personnel ~~may~~should only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this General Order.
4. Unless[JC8] there is a criminal nexus, officers will not use, retain, or transmit license plate reader data ~~for the purpose of investigating~~to investigate persons who are 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. Operators[JC9] will not use or operate ALPR systems ~~will not be operated or used~~ for warrant round-up operations, operations focused on collecting past due traffic fines, Class C[JC10] Misdemeanors, or any other similar purpose of generating revenue or collecting money owed by the public.
6. The[JC11] Department will not use ALPR systems ~~will not be used~~ for ~~the purpose of investigations related to~~investigating immigration status or access to reproductive health services to the extent legally possible.
7. ~~Any~~The Department will address any misuse or inappropriate application of ALPR operations, information, data, or software ~~will be addressed~~ through General Order 902 Administrative Investigations.
(b) If ~~it is~~the Department reasonably ~~believed~~believes that another law enforcement agency has used or is using ~~or has used~~ APD ALPR systems or data in a manner that violates the "~~"~~Prohibited Uses~~"~~ identified herein, we will report that information ~~will be reported~~ to the Auto Theft Interdiction Unit Lieutenant. The Lieutenant will review the possible violation and determine if sharing ALPR data with the outside agency will continue.
(c) The[JC12] Chief Security Officer shall oversee ~~who has~~ access to the ALPR database and will limit roles depending on the user's role. The Chief Security Officer shall ~~also~~closely coordinate with CTM ~~for all ALPR data~~ to ensure the ~~use~~implementation of the best data security and storage practices. ~~Unless otherwise retained and saved by investigators regarding a criminal investigation,~~ for all ALPR data, APD will store all collected ALPR data ~~collected will be stored~~ on a designated ALPR server~~.~~, unless investigators retain and save the data for a criminal investigation.
(d) Server operators will purge ALPR data from the designated ALPR server ~~30~~[JC13] days after ~~it is collected by~~ an ALPR collects it. The ~~length of time for the~~ retention ~~of~~period for ALPR data will ~~be in accordance~~comply with state law. All logins and transactions are logged within the ALPR system and audited[JC14] 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 must download and record the relevant ALPR data into the case file[JC15].
(f) ~~All~~The Department shall retain all ALPR data related to a criminal investigation ~~shall be retained~~ for a period consistent with the City of Austin's Records Management Ordinance, Chapter 2-11, and any applicable City Records Control Schedules and/or the State Local Government Retention Schedules[JC16].

OPO found that approximately three substantive changes were made to the policy language. These changes included the following:

1. The addition of a provision stating, "APD will not distribute, sell, or transfer data to any non-law enforcement entities."
    - This language was added from Section 344.2.1 of APD's 2021 policy.

2. The addition of a provision stating, "The Chief Security Officer will ensure all permanent ALPR cameras are located at various points throughout the city to provide a safe, equitable, and fair

deployment strategy. The deployment of permanent ALPR cameras shall not disproportionately affect any group or segment of our community. "

- OPO discussed this provision with APD and has remaining concerns about whether there are front- and back-end procedures in place to support this commitment.

3. The addition of a provision stating that audits of ALPR systems will review "[l]icense plate hits, categorized by zip code and sector, and the type of camera that captured the data."
    - OPO's understanding is that this provision was added after a discussion with Joyce James Consulting. This was separate from planned community events.

Recommendations

1. **OPO recommends that APD work with OPO and the Communications and Public Information Office (CPIO) to coordinate at least two additional meetings to (1) gather richer feedback, (2) engage with more community members, and (3) ensure that events are executed according to community engagement best practices.**

2. **OPO also recommends that APD document all qualitative data collected at the meetings, as well as the methodology and findings of any subsequent data synthesis and analysis. This information should be included in the report to City Council.**

B. Safeguards Enumerated in Resolution 56

Safeguard #1

Per Resolution 56, the license plate reader program's exclusive functions shall be as follows:

Resolution 56	*To retain and query historical data for the investigation of exclusively the crimes and emergencies specified below unless otherwise required by state or federal law:* *A. Vehicles that have been reported as stolen* *B. Vehicles registered to an individual for whom there is an outstanding felony or Class A misdemeanor warrant* *C. Vehicles associated with missing or endangered persons* D. *Vehicles where the vehicles or individuals associated with the license plate numbers are relevant and material to an active, ongoing criminal investigation of felonies, Class A misdemeanors, and/or hate crimes.*

Analysis	APD's proposed policy states that, "[d]epartment personnel should only access and use the ALPR system for official and legitimate law enforcement purposes consistent with [the policy]. However, the proposed policy does not explicitly limit the use of ALRP systems based on the above criteria. **<u>Recommendations</u>** **1. OPO recommends that APD revise the policy to adhere to the limitations outlined above.** **2. OPO also recommends that any restrictions outlined in policy be stated using the word "shall" as opposed to "should." Section 106.2.3(b)(4)(a) of the APD General Orders states that, "[t]he words 'shall,' 'will,' and 'must' are mandatory in intent and are used to specify a required action, while "[t]he word 'should' is advisory in intent;" it is not mandatory.[5]**

Resolution 56	*To scan vehicle license plates and cross reference the license plate with information on the license plate reader "hot list" containing information relating to certain vehicles. The information about these vehicles may be gathered from The Texas Department of Motor Vehicles* *Texas Department of Public Safety* *including the State Network and its Alert Programs* *the state Criminal Justice Information System* *Texas Department of Family and Protective Services* *the Texas Center for the Missing* *the National Crime Information Center* *the National Center for Missing & Exploited Children* *the FBI Kidnappings and Missing Persons list* *or entered by the Austin Police Department.*
Analysis	Section 344.2(c) of the proposed policy defines a "hot list" as "a cross-reference from a vehicle license plate scans with information associated with vehicles of interest. This list includes but is not limited to license plates listed as stolen, B.O.L.O., SILVER and AMBER alerts, or wanted individuals with a Class A offense or greater warrant." **<u>Recommendations</u>** **1. OPO recommends that proposed policy be revised to include additional details from this provision of Resolution 56.** **2. OPO also recommends that the definition of "hot list" be revised for clarity.**

[5] Austin Police Department, "106.2.3 Grammatical Construction of Manuals," *Austin Police Department General Orders,* accessed March 30, 2023, https://www.austintexas.gov/sites/default/files/files/Police/General%20Orders/GO%2012.05.22/APD%20General%20Orders%20Issued%2012-05-22.pdf .

Per Resolution 56, the Austin Police Department must document and preserve the following information:

Resolution 56	*The reason for the entry* *When the entry was made* *The amount of time requested for the entry to remain in the system and why; and* *When the manual entry was or will be destroyed*
Analysis	Section 344.6(c)(7) of APD's proposed policy states that audits will look at data related to "[t]he number of manually-entered license plate numbers…, 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." Section 344.6(d) of the proposed policy states, "[a]ll logins and transactions are logged within the ALPR system and audited to ensure proper use and whether there is a criminal predicate." The policy does not outline (related to audits or otherwise) a requirement for APD to specifically document and preserve (1) when the entry was made, (2) the amount of time requested for the entry to remain in the system and why; and (3) when the manual entry was or will be destroyed. **<u>Recommendations</u>** **1. OPO recommends that the policy be revised to explicitly state the four documentation and preservation requirements above, and that these requirements be outlined in a separate provision titled "Documentation Requirements" or similar. While the data should certainly be part of any audit and it may be something that "is logged within the ALPR system and audited," it is unlikely that officers could be held accountable based on the current language. If the intent of Resolution 56 is to ensure officer accountability for documenting and preserving this information, then APD's policy must specifically direct personnel to document and preserve the information.** **2. OPO also recommends that APD consider whether data based on the four requirements above would be available in future audits or whether such data might end up being purged before an audit based on the Resolution 56 requirements to purge certain ALPR data after 30 days unless an exception applies. In other words, OPO recommends that APD further consider (1) the data from the ALPR system that needs to be preserved to allow for thorough audits and (2) how it can be preserved in accordance with Resolution 56.**

Safeguard #2

Resolution 56	*Data used for the license plate reader program will be kept for a maximum of 30 days and destroyed thereafter. License plate reader data may not be retained or transmitted unless it matches with a vehicle on a hot list or is related to an active criminal case or investigation, in which case it may be stored in a criminal case folder for that case or investigation for longer periods and, to the extent it does not conflict with APD's retention policy for criminal cases, is destroyed at the conclusion of:* *A. An investigation that does not result in any criminal charges being filed; or* *B. The final disposition of any criminal charges filed, including but not limited to dismissal, acquittal, or conviction; or* *C. A missing or endangered person investigation.* *Such data may also be preserved pursuant to a court order or a preservation request from a governmental entity or defendant in a pending criminal case until a court of competent jurisdiction determines the data are relevant and material to such case or otherwise orders the data preserved. If a court of competent jurisdiction determines there is no need to preserve the data, or if the criminal case is finally disposed without the court ruling on such preservation, the data will be destroyed as soon as practicably possible and by no later than the expiration of 7 days following the court's ruling or final disposition of the case. One year from the passage of this Resolution, the Austin Police Department will return to Council to provide an evaluation of the 30-day data retention policy and its effectiveness.*

Analysis	Section 344.4(d) of the proposed policy states, "Server operators will purge ALPR data from the designated ALPR server 30 days after an ALPR collects it. The retention period for ALPR data will 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." Section 344.4(e) states, "For ALPR data related to ongoing criminal investigations or criminal investigations that contain ALPR as evidence, investigators must download and record the relevant ALRP data into the case file." Section 344.4(f) states, "The department shall retain all ALPR data related to a criminal investigation for a period consistent with the City of Austin's Records Management Ordinance, Chapter 2-11, and any applicable City Records Control Schedules and/or the State Local Government Retention Schedules." Section 344.5(c) states, "The Department will process public requests for ALPR data records in accordance with Texas Government Code, Chapter 552, and General Order 116 (Security and Release of Records and Information). If required by law to share this data, APD will supply the requested information for a specific case or investigation to the extent legally required." The policy does not specifically discuss missing or endangered person investigations in the context of data retention, but rather data sharing. Section 344.5(b) states, "[d]ata sharing with other law enforcement agencies will only occur for vehicles on the hot list due to locating missing or endangered persons or due to a documented ongoing criminal investigation." The policy also does not discuss the Resolution 56 requirement for data to be, "…destroyed as soon as practicably possible and by no later than the expiration of 7 days" after the determination by a court of competent jurisdiction that there is no need to preserve the data, or the case is finally disposed without the court ruling on such preservation. **<u>Recommendations</u>** 1. **OPO recommends that the policy be revised to specifically discuss records retention for missing or endangered person investigations. If, on the other hand, Section 344.(f) is meant to cover endangered or missing person investigations, then OPO recommends that this section be revised for clarity.** 2. **OPO also recommends that APD engage in further discussions and planning around this safeguard and, where needed, request additional information and clarification. OPO recommends that such discussions touch on how this safeguard may align with any applicable records control or retention schedules.**

Safeguard #3

Resolution 56	*Data sharing with another government agency will only occur for investigating and/or prosecuting criminal activity for APD as permitted under Safeguard #1 above or locating missing or endangered persons. If a circumstance arises where the City is required by state or federal law to share the information at the request of a state or federal agency for another law enforcement purpose, then APD will not grant direct access to the database, but will only supply the requested information for a specific case or investigation that is under its custody and control and is responsive, relevant, and material to the request or only to the extent legally required. If the City receives a request for information that is broader than a specific case or investigation, then APD will report the request to the Office of Police Oversight, Mayor, and Council and may not share the information requested, except to the extent legally required. 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 written administrative policy and procedure for license plate readers and the Austin Police Department 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.*
Analysis	This safeguard is only partially addressed in the proposed policy. The proposed Section 344.5(b) states, "[d]ata sharing with other law enforcement agencies will only occur for vehicles on the hot list due to locating missing or endangered persons or due to a documented ongoing criminal investigation." Section 344.5(d) states that "The Chief of Police, or a designee, will be promptly notified if a request for information is broader than a specific case or investigation. This notification will enable APD to fulfill its obligation to report that request to the Office of Police Oversight, Mayor, and Council prior to sharing any information." The proposed policy does not address the Resolution 56 requirements for a prerequisite agreement or memorandum of understanding for any broad data sharing. APD has reported to OPO that this scenario is not covered in the proposed policy because there would be no circumstances in which this issue would come up. **Recommendations** 1. **OPO recommends that APD engage in further discussions and planning around this safeguard and, where needed, request additional information and clarification. OPO recommends that such discussions touch on how the proposed memoranda of understanding would be enforced in practice. If it is the case that APD could and would categorically refuse a request that is broader than a specific case or investigation, then OPO recommends that APD revise its policy to include a provision that explicitly outlines the Department's commitment to refusing such requests.**

Safeguard #4

Resolution 56	*Annual training of all Austin Police Department personnel will be conducted on the policies and restrictions concerning license plate reader camera use and data, including how to properly respond to requests for data from other law enforcement agencies. No APD personnel is permitted to participate in the license plate reader program or access, view, or use any license plate reader program or access, view, or use any license plate reader data until such training has been successfully completed, and continued participation and access is contingent upon successful completion of training each calendar year.*
Analysis	Section 344.7 of the proposed policy discusses training and states that all "members" of APD "will utilize ALPR equipment or software and shall completed required training." Under Section 106.2.1 of the General Orders, "members" are "all persons employed by the Austin Police Department," including "sworn officers, civilian employees, unpaid interns and volunteers." The policy complies with Council's directive to annually train all APD personnel, but by using the term "members," the policy also states that all persons employed by APD, regardless of role, will utilize ALPR equipment, which is perhaps not accurate. Section 344.7 states that ***annual*** training "will include restrictions on using ALPR data and how to respond to a request for data." This policy provision is only partially in compliance with Council's directive to annual train all APD personnel. The proposed policy does not mandate annual training of all APD personnel on the policies and restrictions concerning license plate reader camera use and data. Rather, the policy discusses required training on o "appropriate use and collection of ALPR data" with an emphasis on "the requirement to document the reason for the inquiry; o Section 344.4 Safeguards o Examples of negative consequences resulting from misuse The proposed policy does not state that APD personnel is not permitted to participate in the license plate reader program or access, view, or use any license plate reader program or access, view, or use any license plate reader data until required training has been successfully completed, or that continued participation and access is contingent upon successful completion of training each calendar year. Notably, this limitation on use of ALPRs was part of APD's 2021 policy and is required under Resolution 56. **Recommendations** **OPO recommends that APD further revise its policy to include the following safeguards:** **1. A clear statement that all personnel will receive annual training and, in accordance with Resolution 56, indicate who (based on role within the Department) will utilize ALPR equipment and software, and what additional training would be necessary based on whether the user is an end-user, operator, administrator, etc.** **OPO recommends that APD revise the policy to include language stating that access and use is contingent upon successful completion of training.**

Safeguard #5

Resolution 56	The City Manager will post the Austin Police Department's usage and privacy policy regarding license plate readers on the City's website.
Analysis	The proposed policy does not outline a commitment to making available the current ALPR usage and privacy policies on the City's website. **Recommendations** **1. OPO recommends that APD further revise the policy to include an ongoing commitment to posting (or making available to the City Manager for posting) the following:** **A. The most current usage and privacy policies for ALPRs on the City's website;** **B. To the extent legally possible, the most current data privacy policy for the vendors(s) with whom APD contracts for ALPR services;** **C. The current number of APD-owned cameras, and whether they are fixed/stationary, semi-stationary, or mobile;** **D. Information about APD's ability to access data from other law enforcement entities and privately owned cameras** **2. OPO recommends that all policies, information, and data related to ALPRs be made available in a way that meets language access and disability access needs.**

Safeguard #6

Resolution 56	No person will be the subject of police action because of 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, when license plate reader data is used.
Analysis	Section 344.4(a)(1) of the proposed policy prohibits officers from targeting any person based on any of the above. The proposed policy does not discuss actionable steps outside of discipline that the Department will take to hold itself and its members accountable. **Recommendations** **OPO recommends that APD further revise the policy to include the following safeguards:** **1. Specific front-end processes (e.g., enabling/disabling technological functions of the ALPR systems) and back-end processes (e.g., audits) to mitigate and identify targeting based on any of the above.**

Safeguard #7

Resolution 56	Unless there is a criminal nexus, officers will not use, retain, or transmit license plate reader data for the purpose of investigating persons who are exercising their First Amendment rights, including freedom of speech, assembly, association, and exercise of religion, such as attending political rallies, organizational meetings, public demonstrations, and religious gatherings.
Analysis	The proposed policy states the above prohibition verbatim. **Recommendations** **OPO recommends that APD further revise the policy to include the following safeguards to enhance the efficacy of the policy:** **1. Ensure that the policy applies to past and current First Amendment activities. For example, revise the policy to state, "Unless there is a criminal nexus, officers will not use, retain, or transmit license plate reader data for the purpose of investigating persons who are or were exercising their First Amendment rights…"** **2. Ensure that the policy applies to ALPR data and systems. For example, revise the policy to state, "Unless there is a criminal nexus, officers will not use ALPR systems or use, retain, or transmit license plate reader data…"**

Safeguard #8

Resolution 56	A license plate reader alert alone, does not create reasonable suspicion to justify a traffic stop or the detention of an individual. Before making a stop or detention, the officer must: 1. Make a visual confirmation that the license plate matches the information captured by the license plate reader and reported in the last alert; and 2. Confirm the license plate information matches information in the hot list.
Analysis	Section 344.3.2 of the proposed policy outlines the above requirements to make a stop or detention. **Recommendations** **1. OPO recommends that APD consider additional safeguards for cross checking information, such as utilizing a two-employee verification system. For example, the Metro Nashville Police Department utilizes a "two-prong verification system to ensure the accuracy of any 'hit' identified by the fixed position ALPR systems. When the ALPR system alerts MNPD to a "hit", an employee will first cross check the image taken to the information ran through the database. If the employee confirms the information to be accurate [a] second employee will then verify and confirm the information prior to giving authorization to conduct a vehicle stop."[6]**

Safeguard #9

Resolution 56	The license plate reader data collected by the Austin Police Department will not be used for the purpose of investigations related to immigration status or reproductive health services to the extent legally possible.
Analysis	Section 344.4(a)(6) of the proposed policy states, "The Department will not use ALPR systems for investigating immigration status or access to reproductive health services to the extent legally possible." **Recommendations** **1. OPO recommends that the policy be revised to prohibit the use of ALPR systems *and* data, and that the prohibition clearly apply to both the Department and Department personnel.**

[6] Metro Nashville Police Department, "License Plate Reader Pilot Program Frequently Asked Questions," Nashville.gov, Metropolitan Government of Nashville & Davidson County, accessed March 27, 2023, https://www.nashville.gov/departments/police/crime-control-strategies/license-plate-reader/lpr-pilot-program-faq.

Safeguard #10

Resolution 56	The license plate reader data collected by the Austin Police Department will not be used for the purpose of collecting traffic fines, Class C misdemeanors, warrant roundups, or any other similar purpose of generating revenue or collecting money owed by the public. APD will not use license plate reader data for the purpose of conducting its own criminal investigations related to immigration status or access to reproductive health services.
Analysis	Section 344.4(a)(5) of the proposed policy states, "Operators will not use or operate ALPR systems for warrant round-up operations, operations focused on collecting past due traffic fines, Class C Misdemeanors, or any other similar purpose of generating revenue or collecting money owed by the public." Section 344.4(a)(6) of the proposed policy states, "The Department will not use ALPR systems for investigating immigration status or access to reproductive health services to the extent legally possible." **Recommendations** **1. OPO recommends that these sections be revised to prohibit the use of ALPR systems *and* data, and that they be revised to clearly apply to both the Department and Department personnel.**

Safeguard #11

Resolution 56	The Austin Police Department will use best practice and data security including, but not limited to: A. Role-based access to limit database access to specific officers, who are ordered to operate in compliance with policy or else be subject to disciplinary action; and B. Designation of a Chief Security Officer with responsibility for the following: receiving daily alerts on attempts to log in, limiting access to the license plate database for only permissible use, and/or regularly monitoring access to data stored under this provision; and C. Other best practice provisions related to data security for data storage, including the most secure options available for maintaining data.

Analysis	Section 344.2(b) of the proposed policy defines the Chief Security Officer as "[r]esponsible for receiving daily alerts on login attempts, limiting access to the license place database for only permissible use, and/or regularly monitoring access to data stored under this General Order." Section 344.3.1 states that "[t]he Auto Theft Interdiction Unit will manage the ALPR program," and, "[t]he Chief Security Officer is the Sergeant of the Auto Theft Unit." Section 344.4(c) states, "The Chief Security Officer shall oversee access to the ALPR database and will limit roles depending on the user's role. The Chief Security Officer shall closely coordinate with CTM to ensure the implementation of the best data security and storage practices for all ALPR data. APD will store all collected ALPR data on a designated ALPR server, unless investigators retain and save the data for a criminal investigation." **Recommendations** **1. OPO recommends that APD reconsider the plan to make one person, in this case the sergeant over the Auto Theft Interdiction Unit, solely responsible for coordinating with Communications and Technology Management (CTM) to ensure the implementation of best practices in data security and storage. Given the importance of this task and the likelihood that additional approvals may be needed from others in the chain of command, OPO recommends that this be a broader coordination effort involving APD command- and executive-level staff, as well as the City of Austin Chief Security Officer, as outlined in Resolution 56.** **2. OPO also recommends that, to improve clarity, APD revise the proposed Section 344.4(c) related to role-specific access to ALPR data.**

C. Other Necessary Safeguards

In accordance with Resolution 56, OPO has identified the following additional safeguards to improve the policy. This is a non-exhaustive list and represents two of the more pressing concerns.

1. Goal: Protecting against unauthorized access to or misuse of data while allowing for review by the City Auditor or an appointed third party.

APD's current policy states that ALPR data will not be shared with non-law enforcement entities, and there is no caveat based on the provisions of Resolution 56 that direct the City Auditor to review or hire an external party to audit APD's license plate reader audit process and review the license plate reader data and program. Per Resolution 56, this review is to be done "with assistance from the Austin Police Department, and to the extent allowed by law, information obtained by the audit and review will be shared with the City Council's Public Safety Committee, the Office of Police Oversight, and the Public Safety Commission."

Recommendations

OPO recommends that APD further revise the policy to balance the need for data privacy protections and the need for the Office of the City Auditor (or its designee) to conduct an authorized review of the data and the program and for other City entities to access information

obtained by the audit and review. In particular, Section 344.5(a) should be revised to state that APD will not distribute, sell, or transfer data to any non-law enforcement entities *except as outlined in Section 344.6*, which discusses audits by the City Auditor and review by other City of Austin entities.

OPO also recommends that, as outlined in the analysis of Safeguard #1, APD consider whether pertinent data would be available for audits or whether such data might end up being purged before an audit based on the Resolution 56 requirements to purge certain ALPR data after 30 days unless an exception applies. In other words, OPO recommends that APD further consider (1) the data from the ALPR system that needs to be preserved to allow for thorough audits and (2) how it can be preserved in accordance with Resolution 56.

2. **Goal: Meaningful development and implementation of front-end and back-end solutions to mitigate and analyze disparate impacts to Austin communities and community members from the placement and use of ALPRs, and reference to those solutions in the policy language.**

   Recommendations

   OPO recommends that the policy be revised to reference the processes that APD will utilize to mitigate disparate impacts from the placement and use of ALPRs. In developing these processes, OPO recommends that APD work with OPO and the Equity Office to identify experts equipped to conduct an equity-based assessment related to current plans for placement of ALPRs. This work should also include the development of research questions for future assessments/audits, which is a necessary first step in identifying the data to be analyzed.

D. Axon Fleet 3 Dashboard Cameras

APD has reported to OPO that the proposed policy is not tailored to specific equipment (e.g., fixed ALRPs) because the Departments wants it to be all-encompassing, such that it could cover ALPR equipment of any type (e.g., fixed/stationary, semi-stationary, or mobile) and from any vendor.

APD has also communicated a desire to bring on at least 450 Axon Fleet 3 dashboard cameras, which APD would use to progressively replace current dashboard camera equipment once it reached "end of life." These cameras are equipped to function as mobile ALPRs, which would mean that an approval from the Austin City Council to utilize the ALPR function of the Axon Fleet 3 cameras would result in 450 mobile ALPRs coming online at some point in the future.

Based on OPO's conversations with APD, there is still much work to be done to prepare the policy and procedures for such an event. OPO asked APD whether this equipment (or any of APD's proposed equipment) would be able to be singularly activated or deactivated, whether APD had considered randomized activation and deactivation to help mitigate disparate use, whether APD was familiar with functions of the Fleet 3 cameras, such as "long tracking," that could help identify potential misuse. Unfortunately, APD was not able to provide OPO with definitive answers to these and other related questions.

Recommendations

1. **OPO recommends that APD spend additional time developing its policy and procedures before bringing ALPR systems online. The policy does not currently lay out any specific front-end processes to help avoid disparate use of the devices, and the back-end procedures outlined in policy are still very high-level, and direct discussions about such procedures with APD did not result in more detailed information.**

E. Other Miscellaneous Areas for Improvement

1. "Automatic License Plate Readers" versus "Automated License Plate Readers"
    a. The proposed General Order 344 is titled "Automatic License Plate Readers," but Section 344.2 defines "Automated License Plate Reader." Both terms are used in the industry, but APD's policy should identify one and ensure that only one term is used throughout.

2. Purpose & Scope Section
    a. The proposed Purpose & Scope section is weaker now than in 2021 version of the policy. Specifically, the 2021 policy described the reason APD has an ALPR program whereas the proposed policy shared with OPO briefly states the purpose of having a policy, which does not add the same value.

3. Clarification Regarding Processes and Procedures
    a. The processes and procedures regarding how and where to submit a help ticket should be revised for clarity. (See Section 344.3 Procedure)
        i. APD's 2021 policy directed ALPR users to "contact CTM" whereas the proposed policy only states that they should "submit a help ticket."
    b. The policy should be revised to clarify processes and procedures related to potential misuse of ALPR systems and data, including (1) who is responsible for reporting potential misuse by another law enforcement agency and (2) who will be held accountable if reporting does not happen. Currently, the policy says, "If the Department 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, we will report that information to the Auto Theft Interdiction Unit Lieutenant. That Lieutenant will review the possible violation and determine if sharing ALPR data with the outside agency will continue." Here, it is unclear who "we" is, and how this procedure would play out in practice.

F. Unanswered Questions After Meeting with APD

On March 29, 2023, OPO and APD met to discuss APD's proposed ALPR policy and procedures, specifically (1) the safeguards enumerated in Resolution 56 and (2) the potential for APD to acquire 450 Axon Fleet 3 dashboard cameras with ALPR capabilities. APD provided answers to many of OPO's questions, but several

questions were also left unanswered because they required follow-up from APD personnel who were not present at the meeting.

What follows are OPO's unanswered questions. OPO may have additional questions based on APD's responses to these questions.

1. **Consultation with City of Austin Chief Security Officer (CSO)**
    - Resolution 56 directed that City of Austin CSO be consulted in the development of policy provisions related to ALPRs.
        - What has this looked like in practice between APD and the CSO? Can you give us an overview of the discussions on data privacy best practices and what to-do items are still outstanding?
        - One of the things discussed in the policy is that there will be a separate server for ALPR data, but then there is another provision that discusses the data being movable by detectives for purposes of an investigation. What data security protections are in place for data that is pulled from the ALPR server for investigation purposes?
        - What about data security when entities outside of APD access the data (e.g., the City Auditor)?
        - Have there been discussions with the City of Austin CSO and the City Auditor about what that would entail? What was the outcome of any such discussions?

2. **Axon Fleet 3**
    - With the contract for Axon Fleet 3 cameras for 450 devices, what percentage of police units would that cover?
    - Per Axon, the Fleet 3 cameras are at some point going to support automatic hit validation (if they don't already). How would that impact the requirement for (and ability of) officers to manually cross-check the information?
    - How would the Axon Customer Experience Improvement Program (ACEIP) impact APD's data sharing? Is it required for APD to sign up for the ACEIP? Axon says they ask each Fleet 3 ALPR customer to sign up for it at the tier 2 level, which allows Axon to use "anonymized data collected by the agency to support continuous product improvements. The data includes the plate crop and metadata such as date, time, read confidence score, and correct/incorrect determination. Axon will not collect GPS location, hot list information, or any agency input into the record, other than correct/incorrect determination." We understand that a plate crop is a cropped picture showing the actual image of the license plate.

3. **Audits and the 30-day purge**
    - In thinking about this audit as it is, how might it be impacted by the 30-day purging outlined in Resolution 56? What data will the Auditor have access to?
        - What about the data that leads to a hit or a detention but not an investigation (e.g., "police events")? How will that be part of the anticipated audits by the Auditor? In summary, is there data that would be related to contacts that APD had with community members, or that would capture APD's use of ALPR systems, that may be unavailable to the Auditor (or to APD in quarterly audits) because of the 30-day purge?

4. **Singular activation/deactivation**
    - Does the technology that APD is looking into from Flock Safety (or Vigilant or others) support turning one camera on or off at a time?

5. **Viewing data from other agencies' ALPRs**
    - Does APD automatically get access to other law enforcement agency feeds/data? If so, which agencies?

6. **Viewing data from privately owned ALPRs**
    - You shared that APD would have access to data from privately owned ALPRs (at least if APD was working with Flock Safety). You also said that if the data generated a lead, then an audit would generate where that camera was.
        - Can you define what you mean by a lead in this context? We think this goes back to the question we had about the 30-day purge and what would be purged versus saved.
        - Under what circumstances would APD be pulling data from privately owned ALPRs?
        - When you say that the audit would generate where that camera was, would it be clearly and conspicuously flagged as a camera that wasn't an APD-owned camera? Or would it be up to the auditor(s) to compare against a list of APD camera locations?

7. **Working relationship between the Police Technology Unit and Auto Theft Interdiction Unit**
    - You mentioned that only the Police Technology Unit can turn on/off the ALPR function. You also said that the Auto Theft Interdiction Unit is responsible for the maintenance and ongoing responsibilities related to ALPRs.
        - Can you say more about how these two units are working together on ALPRs and what their unique responsibilities will be?
        - If there is an issue with the function of the ALPRs, would that be immediately apparent to both units or just one? If just one unit, which one?
        - What approvals are necessary to turn on/off the ALPR function? Here, we're asking about approvals within APD as opposed to City Council. In other words, who is the individual with decision-making authority? Is it a multi-level approval?

344 Automatic License Plate Reader (ALPR)

344.1 PURPOSE AND SCOPE

To provide rules and guidance for capturing, storing, and using digital data obtained through Automatic License Plate Reader systems.

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 –** 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 but is not limited to license plates listed as stolen, B.O.L.O., SILVER and AMBER alerts, or wanted individuals with a Class A offense or greater warrant.

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 of the Auto Theft Unit.
(b) Operators encountering problems with ALPR equipment or programs will submit a help ticket.

344.3.2 ASSIGNMENT, USE, AND LOCATIONS OF ALPR SYSTEMS

(a) Real time Crime Center (RTCC) personnel will monitor all ALPR systems. All RTCC personnel will receive training in using and interpreting ALPR systems.
    1. The Department will either dispatch alerts received, generally broadcast (GB) them, or not notify patrol.
(b) An ALPR alert alone, including an alert of 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 must:
    1. Make a visual confirmation that the license plate actually matches the information captured by the ALPR and reported in the last alert.
    2. Confirm the license plate information with NCIC/TCIC.
    3. Officers conducting a traffic stop based on a confirmed ALPR alert should 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) The Chief Security Officer will ensure all permanent ALPR cameras are located at various points throughout the city to provide a safe, equitable, and fair deployment strategy. The deployment of permanent ALPR cameras shall not disproportionately affect any group or segment of our community.

344.4 SAFEGUARDS

(a) Prohibited use:

1. When using ALPR systems, officers will 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 will 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 should 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 will not use, retain, or transmit license plate reader data to investigate persons who are 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. Operators will not use or operate ALPR systems for warrant round-up operations, operations focused on collecting past due traffic fines, Class C Misdemeanors, or any other similar purpose of generating revenue or collecting money owed by the public.
6. The Department will not use ALPR systems for investigating immigration status or access to reproductive health services to the extent legally possible.
7. The Department will address any misuse or inappropriate application of ALPR operations, information, data, or software through General Order 902 Administrative Investigations.

(b) If the Department 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, we will report that information to the Auto Theft Interdiction Unit Lieutenant. The Lieutenant will 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 will limit roles depending on the user's role. The Chief Security Officer shall closely coordinate with CTM to ensure the implementation of the best data security and storage practices for all ALPR data. APD will store all collected ALPR data on a designated ALPR server, unless investigators retain and save the data for a criminal investigation.

(d) Server operators will purge ALPR data from the designated ALPR server 30 days after an ALPR collects it. The retention period for ALPR data will 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 must download and record the relevant ALPR data into the case file.

(f) The Department shall retain all ALPR data related to a criminal investigation for a period consistent with the City of Austin's Records Management Ordinance, Chapter 2-11, and any applicable City Records Control Schedules and/or the State Local Government Retention Schedules.

344.5 RELEASE OF DATA

(a) APD will not distribute, sell, or transfer data to any non-law enforcement entities.

(b) Data sharing with other law enforcement agencies will only occur for vehicles on the hot list due to locating missing or endangered persons or due to a documented ongoing criminal investigation.

(c) The Department will process public requests for ALPR data records in accordance with Texas Government Code, Chapter 552, and General Order 116 (Security and Release of Records and Information). If required by law to share this data, APD will supply the requested information for a specific case or investigation to the extent legally required.
(d) The Chief of Police, or a designee, will be promptly notified if a request for information is broader than a specific case or investigation. This notification will enable APD to fulfill its obligation to report that request to the Office of Police Oversight, Mayor, and Council prior to sharing any information.

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) The Risk Management Unit will assist the City Auditor or an external party directed by the City Auditor with Audits.
(c) 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 that resulted in the arrest, prosecution, or 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 defendant.
    5. The number of data sharing requests received, granted, and denied.
    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 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.
    8. Any changes in Austin Police 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.

344.7 TRAINING

(a) All members of the Austin Police Department will utilize ALPR equipment or software and shall complete the following required training:
    1. Will include the appropriate use and collection of ALPR data and emphasize the requirement to document the reason for the inquiry.
    2. Annual training for all APD officers will include restrictions on using ALPR data and how to respond to a request for this data.
    3. Shall cover GO 344.4 Safeguards.
    4. Training shall include examples of negative consequences resulting from misuse.