DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: 14 AUG 24
Coordinator: Information Technology Unit

This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

A. Definitions

A - 1. Automated License Plate Reader (ALPR)

A device that uses cameras and computer technology to compare digital images of vehicle license plates to lists of known information of interest.

A - 2. Hot List

A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to the Stolen Vehicle System (SVS), NCIC, and local BOLO alerts.

A - 3. Hit

Alert from the ALPR system that a scanned license plate may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person or domestic violence protective order.

B. Description of the Technology: *Information describing the surveillance technology and how it works.*

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images. There are two components to the ALPR system:

1. Automated License Plate Readers

Device components include cameras which can be attached to vehicles or fixed objects and a vehicle-based computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hot lists. Data are transmitted for comparison (the hot lists are downloaded to the vehicle at the start of the patrol shift and then compared from that list). Authorized/designated personnel can also manually enter license plates to internal OPD generated hot lists only accessible to personnel authorized/designated to access the OPD ALPR system.

2. ALPR Database

A central repository stores data collected and transmitted by the Automated License Plate Readers.

C. Purpose of the Technology

ALPR technology works by automatically and indiscriminately scanning all license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against Hot Lists, and stores the characters along with the date, time, and location where the photograph was taken. This process allows for two functions by ALPR:

- Immediate (real time) comparison of the license plate characters against Hot Lists listing vehicles that are stolen or sought in connection with a crime and/or with OPD-generated internal lists.
- Storage of the license plate characters – along with the date, time, and location where the photography was taken – in a database that is accessible to enforcement agencies with authorized access (as defined in "Authorized Use" below) for investigative query purposes.

D. Authorized Uses

The specific uses that are authorized, and the rules and processes required prior to such use.

D - 1. Authorized Users

Personnel authorized/designated to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians (PST), or other authorized/designated Department personnel may use the technology. Authorized users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

D - 2. Authorized Use

- **Real-Time Identification**

The sworn personnel/technician shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before possibly taking enforcement action that is based solely on an ALPR alert.

Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle.

Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been fully validated, by visually verifying that the license plate characters on the vehicle match those in the database, and that the make, model, color and all other known identifying characteristics likewise match.

- **Hot Lists**

The Department shall only use the following hot lists: Stolen Vehicle System ("SVS"), National Crime Information Center ("NCIC") lists, CA DOJ lists, Amber and Silver alerts, and custom BOLO lists pertaining solely to missing or at-risk persons, witness locates, burglaries, grand

theft, and violent crime investigation. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's ALPR system will not have access to real time data. Occasionally, there may be errors in the ALPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

Department members will document all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action on a computer generated spreadsheet that **shall include** at minimum;

1. the Department member's name that responded to the alert,
2. the justification for responding to the alert,
3. the related case number,
4. the disposition code,
5. time and date of the response, and
6. any known next steps or follow up (e.g. forwarding case to District Attorney, alerting owner to recovered stolen vehicle).

- **Database Investigative Queries**

  Historical searches of scanned plates is permissible solely for missing or at-risk persons, witness locates, burglaries, grand theft, violent crime investigation, and in response to any subpoena, warrant, or other court order. Accessing the data shall be based on a standard of Reasonable Suspicion or greater. For each query, the Department **shall** record;

  1. the date and time the information is accessed,
  2. the license plate number or other data elements used to query the ALPR system,
  3. the username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated, and
  4. the purpose for accessing the information. These records shall be attached to the annual report required by O.M.C. 9.64 et seq.

- **General Hot Lists** (such as SVS and NCIC) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

D - 3. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate

general offense report. All entries shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles of interest that might have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

1. Entering Department member's name.
2. Related case number.
3. Justification for entering the plate and/or other identifying information onto the Hot List.
4. Date and time of entry.

E. Restrictions on Use

E - 1. Permitted/Impermissible Uses

All ALPR recordings collected from ALPR cameras installed on Oakland property are the property of the Oakland Police Department. Department personnel may only access and use the ALPR system consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

- **Invasion of Privacy**: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment). OPD shall make reasonable efforts to restrict the usage of the ALPR technology to the public right of way and other public property in alignment with this restriction.
- **Harassment or Intimidation**: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
- **Use Based on a Protected Characteristic**: It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Personal Use**: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
- **First Amendment Rights**: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

- **Medical Rights**: No data from ALPR shall be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive health care services, to ensure that medical rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.

  The Oakland Police Department or the City of Oakland shall solicit written documentation from the requesting agency confirming that the requested data from ALPR is not intended to be used for the prohibited purposes set forth herein. Such information shall be provided to all OPD sworn personnel responsible for providing the requested data.

  Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code §798.90.51.; Civil Code § 1798.90.53).

  1. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
  2. No ALPR operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section E "Data Access" below.
  3. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

F. Data Collection

The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters (as well as vehicle attributes such as vehicle color or make and model with some ALPR systems) against specific databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database.

G. Data Access

The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.

Department sworn personnel, police service technicians, or other authorized/designated Department personnel may use the technology. Authorized/designated users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

Data may not be shared with out of state or federal agencies, per California law.

The Oakland Police Department does not permit the sharing of ALPR data gathered by the city or its contractors/subcontractors for purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered by the ALPR are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request.

H. Data Protection

The safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose. (Civil Code § 1798.90.52).
2. Data will be transferred from ALPRs to the designated storage per the ALPR technology data transfer protocol.

I. Data Retention

The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

All ALPR data uploaded to the server shall be purged from the server at the point of 30 days from initial upload. ALPR information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations
2. Missing or at-risk Persons Investigations
3. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

J. Public Access: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Requests for ALPR information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Civil Code § 1798.90.55, Government Code § 7920.000 et seq., this policy, and applicable case law and court orders.

K. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

ALPR server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the ALPR are for the official use of this Department.

OPD has executed an MOU that grants CHP access to OPDs ALPR data for the duration of the MOU.

OPD personnel may share ALPR server data when there is a legal obligation to do so, such as a subpoena, court order or warrant to share such information, such as the following:

- a District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

When there is no legal obligation to provide the requested data, requests for ALPR server data from other California law enforcement agencies shall be made in writing and may only be approved by the BOS Deputy Director/Chief or designee per the 3-step protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized/designated OPD personnel who will extract the required information and forward it to the requester.

1. The requesting party shall have a right to know, and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The Department shall record the requesting party’s name and document the

right and need to know the requested information.

3. The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

L. Training: *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.*

The Training Section shall ensure that members receive department-approved training for those authorized/designated to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees shall include the following:

- Applicable federal and state law
- Applicable policy
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

M. Auditing and Oversight

The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of Database Investigatory Queries, Third Party Data Sharing, and Hot List entries shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

ALPR system audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits, and reviews of training records. The size of these audits shall be large enough to provide a statistically significant representation of the

data collected.

N. Maintenance

The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

N - 1. ALPR Administration

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the BOS. The BOS may contract with an ALPR service provider for installation and maintenance assistance.

N - 2. ALPR Administrator

The BOS Deputy Director/Chief shall be the administrator of the ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The BOS Deputy Director/Chief is responsible for ensuring systems and processes are in place for the proper collection, and retention of ALPR data.

N - 3. ALPR Coordinator:

The title of the official custodian of the ALPR system is the ALPR Coordinator.

N - 4. Monitoring and Reporting

The Oakland Police Department will ensure that the system is remains functional according to its intended use and monitor its use of ALPR technology to ensure the proper functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.

N - 5. The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology Ordinance).

By Order of,

Floyd Mitchell
Chief of Police

Date: 8-14-24

CITY OF OAKLAND

MEMORANDUM

TO: PAC **FROM:** OPD

SUBJECT: ALPR Annual Report **DATE:** APRIL 24, 2025

Background

Oakland Municipal Code (OMC) 9.64.040: Oversight Following City Council Approval requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for the Privacy Advisory Commission (PAC). After review by PAC, city staff shall submit the annual surveillance report to City Council. The PAC shall recommend to City Council that:

- The benefits to the community of the surveillance technology outweigh the costs, and civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Department General Order I-12 titled *Automated License Plate Readers* (DGO I-12) is the policy that provides guidance on the use of Automated License Plate Readers (ALPR) at the Oakland Police Department. This DGO was reviewed by the PAC and approved by City Council on July 16th, 2024.

2024 Annual Report Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

How the Technology is Used

The Oakland Police Department (OPD) utilizes Flock Safety (Flock) camera technology to power its Automated License Plate Reader (ALPR) system. These cameras are mounted on pre-existing city infrastructure, such as light poles or traffic light poles, or they can be mounted utilizing a pole provided by Flock. Once mounted, these cameras take still photos which focus on a vehicle to ensure a clear view of the license plate.

The Oakland Police Department primarily utilizes the Flock system in two ways.

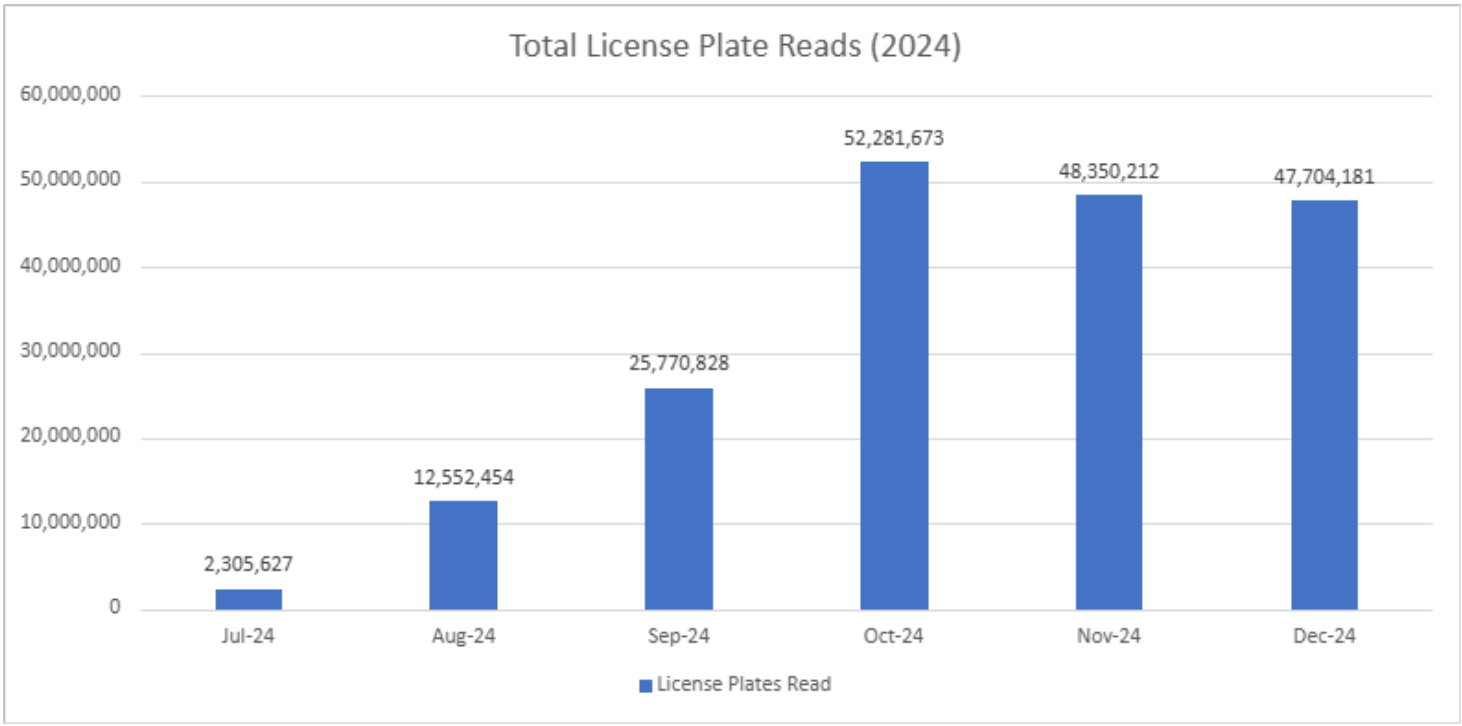
1. To assist in active criminal investigations which have just occurred. The OPD will utilize ALPR to search where a crime just occurred. OPD personnel can enter a vehicle's license plate (if one was provided) or enter a partial license plate (if one was provided) or search a camera location (if no license plate is provided) and attempt to identify the suspect vehicle(s) or vehicle(s) of interest. The vehicle's images are then distributed to OPD Officers via interdepartmental email in attempt to locate and stop and detain any occupant(s). These vehicles are then hot listed via Flock in order to notify/alert officers when the vehicle passes an ALPR. Officers can respond to the location of the alert(s) in an attempt to locate the vehicle.

2. To assist in follow-up criminal investigations which have occurred in the past (30) thirty days. OPD will search ALPR locations of areas where crimes have occurred to attempt to identify vehicle(s) of interest that were involved in previous crimes. When vehicle(s) of interest are identified, images are distributed via interdepartmental email in attempt to locate and stop and identify any occupant(s). These vehicle(s) are then hot listed in order to notify/alert officers when the vehicle(s) passes an ALPR. Officers can respond to the location in attempt to locate the vehicle.

Type and Quantity of Data
Photos of vehicle license plates is the primary data that is collected. This data is retained for 30 days, as required by DGO I-12.

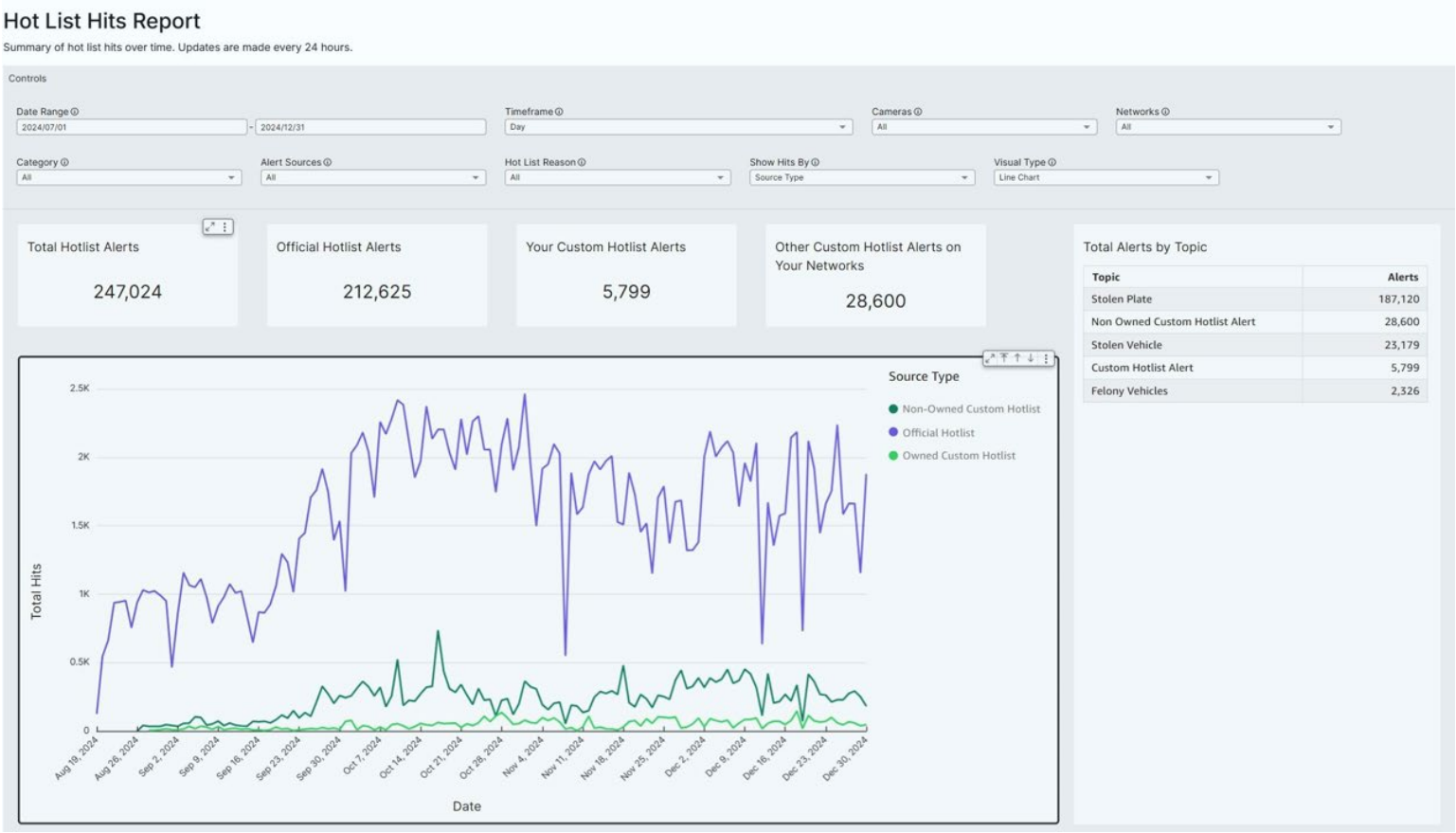
Figure A below shows the amount of license plate reads, month over month. Please note that the same license plate can be read multiple times a day, if that license plate passes by the same or different cameras during its travel. From July 2024 through December 2024, there was a total of 188,964,975 license plate reads by Flock cameras assigned to OPD in the City of Oakland.

Figure A



For hotlists, there was a total of 247,024 hotlist alerts, with 212,625 alerting from an official hotlist, 5,799 alerting from an OPD custom hotlist, and 28,600 custom hot list alerts created by other departments that utilized OPDs Flock images, from July 1st, 2024, through December 31st, 2024. This data is visualized in ***Figure B*** below.

Figure B.



The top five alert types were stolen plate (187,120), non-owned custom hotlist alert, which is an alert created by another agency using Flock and shared with OPD (28,600), stolen vehicle (23,179), an alert from an OPD custom hotlist (5,799) and 2,326 felony vehicles.

Consulting with outside larger agencies, OPD discovered that larger agencies turned off “stolen plate” and “stolen vehicle” alerts for several reasons. The number of alerts were astronomical compared to other types of alerts and the staffing and resources within the department did not allow for proper response to these alerts/notifications. OPD did consider having Flock enable alerts for “stolen plate” and “stolen vehicle” during concentrated times (e.g., early hours between 0100 hours and 0400 hours when calls for service might be less than regular business hours). Flock is still attempting to configure this feature within the product. Without proper staffing or a concentrated configuration within Flock, OPD cannot respond to such alerts given the number of calls for service (e.g., priority calls and emergency calls) OPD receives daily.

When alerts for felony vehicles are received, OPD Officers will either broadcast or distribute email notifications via interdepartmental emails in order for officers to respond to the location and conduct an area check. At times, OPD will also request plain clothes officers, and/or air support (Argus) to respond to the location to assist with locating the felony vehicle(s). A multitude of officers within OPD have been provided ALPR training and been provided access; these officers range from Patrol, Community Resource Officers (CRO), Crime Reduction Team (CRT), Ceasefire (CF), Walking Units, Argus, Traffic, and Investigations.

Custom hot lists can have a variety of responses. They range from responding to conducting an enforcement action or identifying the reads and alerts to further one's investigation.

Outside agencies do not always provide OPD with a response or notify OPD of their hot lists and outcomes. Each agency has access to their own Success Stories feature via the Flock 'Edit Outcome' link; which allows agencies to document their enforcement actions.

Quarterly, there are Flock meetings where Bay Area agencies come together to discuss success stories and improvements which can be made to the Flock products and areas where they would like to see the system improved. At times, outside agencies will share their success stories, such as the one listed here:

- SLPD was dispatch to an armed robbery (firearm) at the Quick Stop located at 1001 MacArthur Blvd in San Leandro. Recorded video surveillance was obtained from the interior and exterior of Quick Stop. The Primary Officer recognized the suspect vehicle associated with a vehicle burglary from February 13, 2025. A records check showed the suspect vehicle was reported stolen to the Oakland Police Department on January 28, 2025. (OPD Case 25-4569). Detectives utilized both San Leandro Flock and Oakland Flock. The Oakland Flock (Camera #194) was utilized as it led detectives to the area of Fruitvale Avenue and E 27th Street. Detectives canvassed this area waiting for additional Flock hits. SLPD Detectives located the suspect vehicle (Toyota Tacoma CA <**redacted**>) parked and occupied at 2301 Foothill Blvd. OPD's Argus Unit (helicopter) responded and assisted SLPD detectives. The suspect was safely taken into custody. The suspects clothing worn during the armed robbery, cash from the robbery, beanie worn during the armed robbery and firearm were all located on the suspect person and in the stolen Tacoma.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The Oakland Police Department has shared our Flock ALPR Data with the following entities in 2024:

Alameda (City) Police Department
Alameda County Sheriff's Office
Alameda County Sheriff's Office- Dublin Police
Burlingame Police Department
CA State Parks
Cal Fire - Law Enforcement
California Highway Patrol
Campbell PD
Colma Police Department
Concord (CA) PD
Daly City Police Department
Danville PD
Dixon Police Department
East Bay Regional Park District Police
East Palo Alto Police Department
El Cerrito PD
Emeryville Police Department
Fairfield California Police Department

Fremont Police Department
Hayward Police Department
Livermore Police Department
Los Altos PD
Marin County Sheriff's Office
Mountain View Police Department
Napa County Sheriff's Office
Northern California Regional Intelligence Center (NCRIC)
Newark (CA) Police Department
Novato PD
Piedmont Police Department
Pleasant Hill Police Department
Pleasanton Police Department
Redwood City PD
Richmond (Calif) Police Department
Sacramento County Sheriff's Office
San Bruno Police Department
San Francisco Police Department
San Leandro Police Department
San Mateo County Sheriff's Office
San Mateo Police Dept
San Ramon Police Dept.
Santa Barbara Sheriff's Office
Santa Clara County Sheriff's Office
Santa Clara Police Department
SF District Attorney's Office
Solano County Sheriff's Office
Sunnyvale Department of Public Safety
Union City PD
Vacaville Police Department
Vallejo Police Department
Watsonville Police Department

To obtain access to our Flock database, each organization had to fill out a permission form and agree to the following questions:

- Do you agree to the following: I confirm, on behalf of my agency or department, in compliance with state law, OPDs ALPR data SHALL NOT be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive or gender affirming health care services, to ensure that the medical and legal rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.
- Do you agree to the following? I confirm, on behalf of my agency or department, that anytime we access OPDs ALPR data, there will be a need to know and right to know.
- Do you agree to the following? I confirm, on behalf of my agency or department, that anytime we access OPDs ALPR data, we will document the following: PC/VC related to the incident, and the department incident or administrative investigation number.

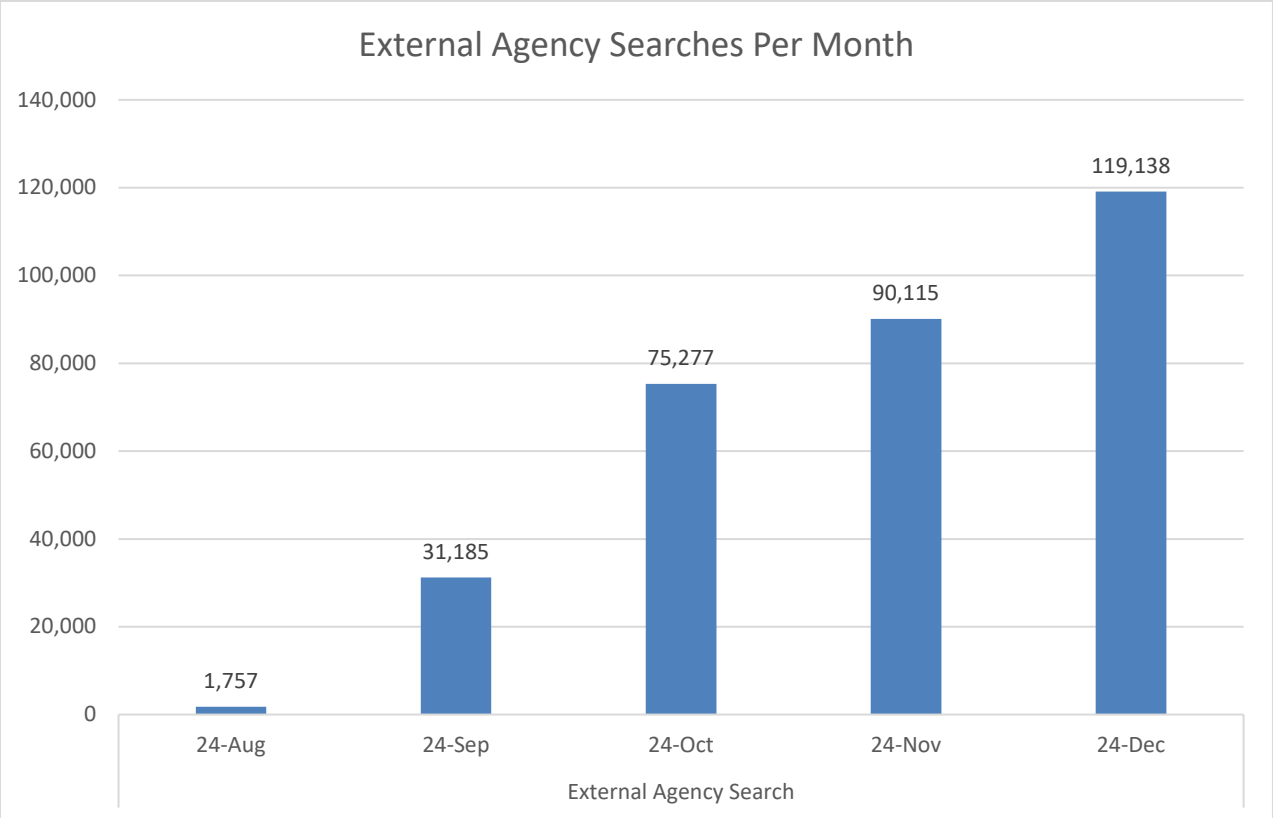
After agreeing to those three questions, the requesting agency was granted access, with approval being logged in a spreadsheet. This information is in ***Attachment A – PAC 2024 Annual Report Data*** on the tab called "Third Party Data Sharing". Any time our information is accessed, a log is created and kept in the Flock system. The second question in the permission form states that agencies will only request to search against

our database if they have the need to know and right to know, therefore, any searches the agency completes after signing the permission form meets the obligations required with DGO I-12. This permission form was reviewed and approved by the PAC Chair, Brian Hofer, on July 9th, 2024.

OPD is working with Flock to distribute the OPD Permission form to agencies who have not received it. Each agency, like OPD, have Flock administrators, who will fill out the form. Of note, OPD has discovered that other agencies have begun to similarly send their own respective permission forms to grant access to their information.

Figure C shows the number of searches that have been done against our data, month over month, in 2024. All the entities listed previously can execute searches against our data. If there is a match in our system, they will be presented with a screenshot which shows the following information:

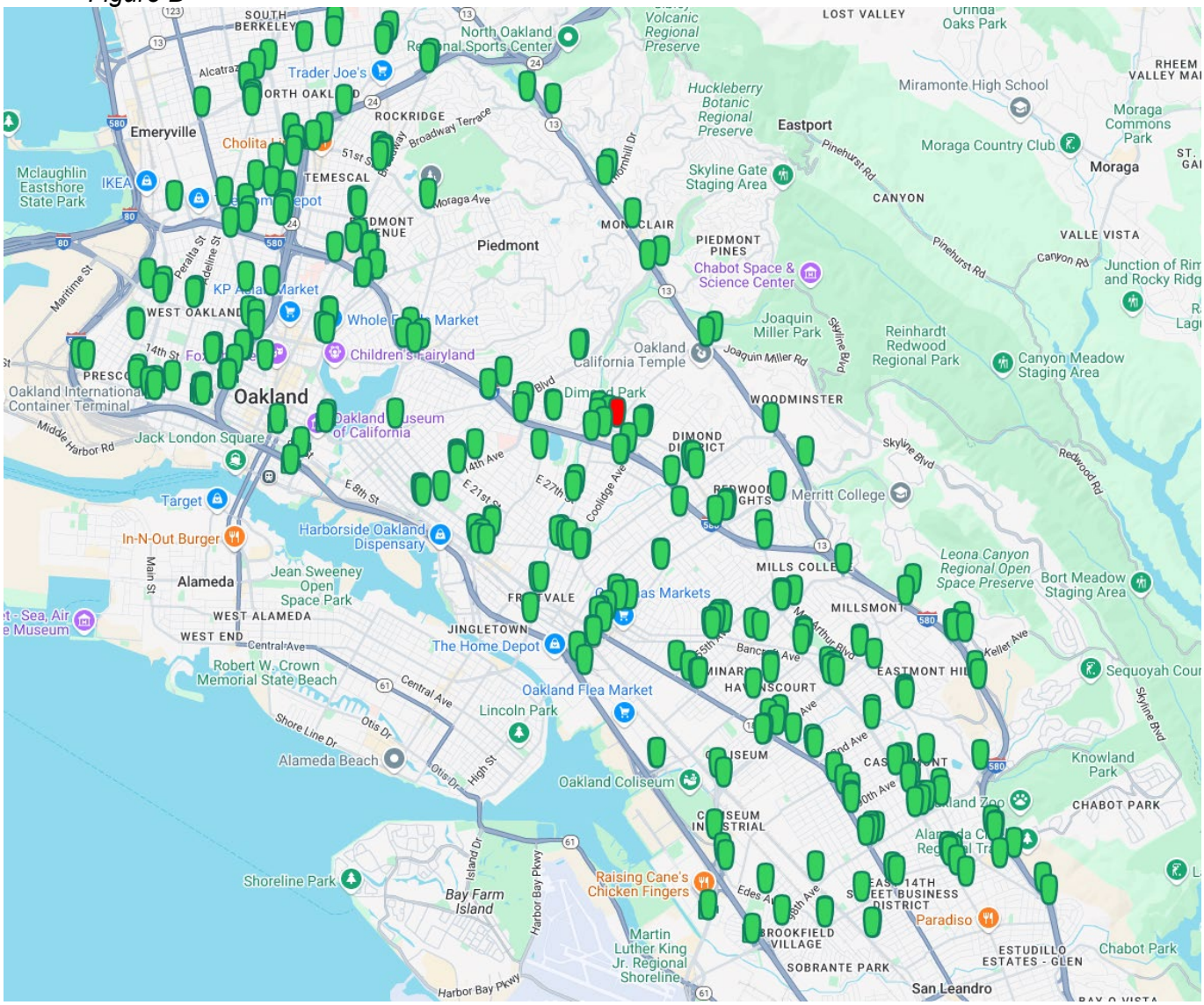
Figure C



C. <u>Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to</u>:

Working in conjunction with the OPD, Flock analyzed heat maps as it relates to violent crime and property crime (stolen vehicles, burglaries, and grand theft) and identified the main egress and ingress locations to these hot spots. As a result, 290 locations were selected for camera placement. These cameras are currently the only source of data, that are OPD assigned, feeding into the Flock system. Further information is provided below in ***Figure D***:

Figure D



D. <u>Where applicable, a breakdown of where the surveillance technology was deployed geographically by each police area in the relevant year</u>:

A total of 290 ALPR cameras were funded and deployed throughout the City of Oakland. There are six geographical policing areas that OPD identifies: Area 1 – Area 6.[1]

Based on crime data and identifying the main egress and ingress locations to these hot spots, the 290 cameras were deployed within the respective six areas as follows:

- Area 1: 44
- Area 2: 57
- Area 3: 23
- Area 4: 55
- Area 5: 51
- Area 6: 60

[1] City of Oakland | Oakland Police Areas

E. A summary of community complaints or concerns about the surveillance technology and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

The Oakland Police Department requests a waiver of this requirement, as Flock Cameras cannot determine the race of an individual, since the primary focus is on capturing the vehicle license plate. In addition, OPD has not received specific feedback from the public on the ALPR system in 2024, outside of PRR requests, which are summarized in Section I.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

The Oakland Police Department is not aware of any violations or potential violations of the Surveillance Use Policy.

Per DGO I-12, "the records of database investigatory queries, third party data sharing, and hot list entries shall be incorporated into the annual report…".

In addition, "ALPR system audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits and reviews of training records".

To satisfy the first requirement, please see ***Attachment A – PAC 2024 Annual Report Data***. In this spreadsheet, there are several tabs that house the specific data being requested. The tab labeled Third Party Data Sharing lists all the organizations which have access to search against OPDs database of images in Flock. The tab labeled Hot List Entries has the hot lists which OPD created. Finally, the database investigative queries were split into two tabs, Database Queries (AugSepOct), which houses all investigative queries from August, September and October in 2024 and Database Queries (NovDec), which houses all investigative queries performed in November and December 2024. While cameras were first installed in July, OPD started training in August and that is when searches began.

The audit information begins on the tab labeled Database Queries Audit. This audit was done by doing a randomized audit of 398 records. Originally, 400 records were selected, but one was a test search and the other generated an error upon data extraction and had to be removed from the dataset. OPD then looked at the "reason" provided for the search. Per DGO I-12, there are several elements that are required to perform a database investigative search: the date and time the information is accessed, the license plate number or other data elements used to query the system, the username of the person who accesses the information, and the purpose for accessing the information.

This information is labeled as the Database Queries Audit Tab in the spreadsheet. The fields labeled as RD/LP Included and Type of Crime Included were the basis of the audit. Since the Flock system logs of all the other information by default when a user initiates a database investigative query, the users are left to enter their reasons manually.

To meet the requirements defined in DGO I-12, OPD has asked staff to standardize their reason to include the report number or incident number, which can start with RD (which stands for Records Division) or LOP (which designates the CAD incident as bellowing to Law – Oakland Police). In addition, we ask that users put in the crime associated with the search, preferably in the form of the penal code or vehicle code, but a written crime reason is also acceptable. Based on this criteria, 398 records were evaluated. Below are the results of the audit, which show that OPD had a report or incident number included in 99% of the audited files and had the crime included in 97% of the audited files.

Total RD/LP "Yes"	395
Total RD/LP "No"	3
Total Type of Crime "Yes"	388
Total Type of Crime "No"	10
RD/LP Iincluded - Audit Pass Rate	99%
Crime Included - Audit Pass Rate	97%

While DGO I-12 only calls for an annual audit, OPD began auditing records to meet these standards immediately. During the first few months of training, OPD sent out weekly or bi-weekly emails identifying users who had incomplete search parameters. This tenacity ensured that our new users understood the requirement and reinforced the importance of properly documenting database investigative queries, as required by DGO I-12. Emails are still sent out periodically to remind individuals of the requirements.

DGO I-12 also calls for a review of training records to ensure that only authorized users are utilizing the ALPR system. Please refer to the tab labeled Training Roster to see a list of all individuals at OPD who have been trained on the policy and use of the Flock ALPR system. There are approximately 246 people who have been trained as of the writing of this report. A random selection of 25 users was selected from those who were audited in the Database Queries Audit. Of the 25 selected users, all 25 were found to have completed training.

As it relates to user/access management, OPD does not manually disable users who separate from the department, as Flock utilizes single sign on with the City of Oakland's Microsoft Office 365 application. When a member or employee separates from the department, the Information Technology Department (ITD) is responsible for disabling the Microsoft Office 365 account, which will, in turn, disable the Flock account.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

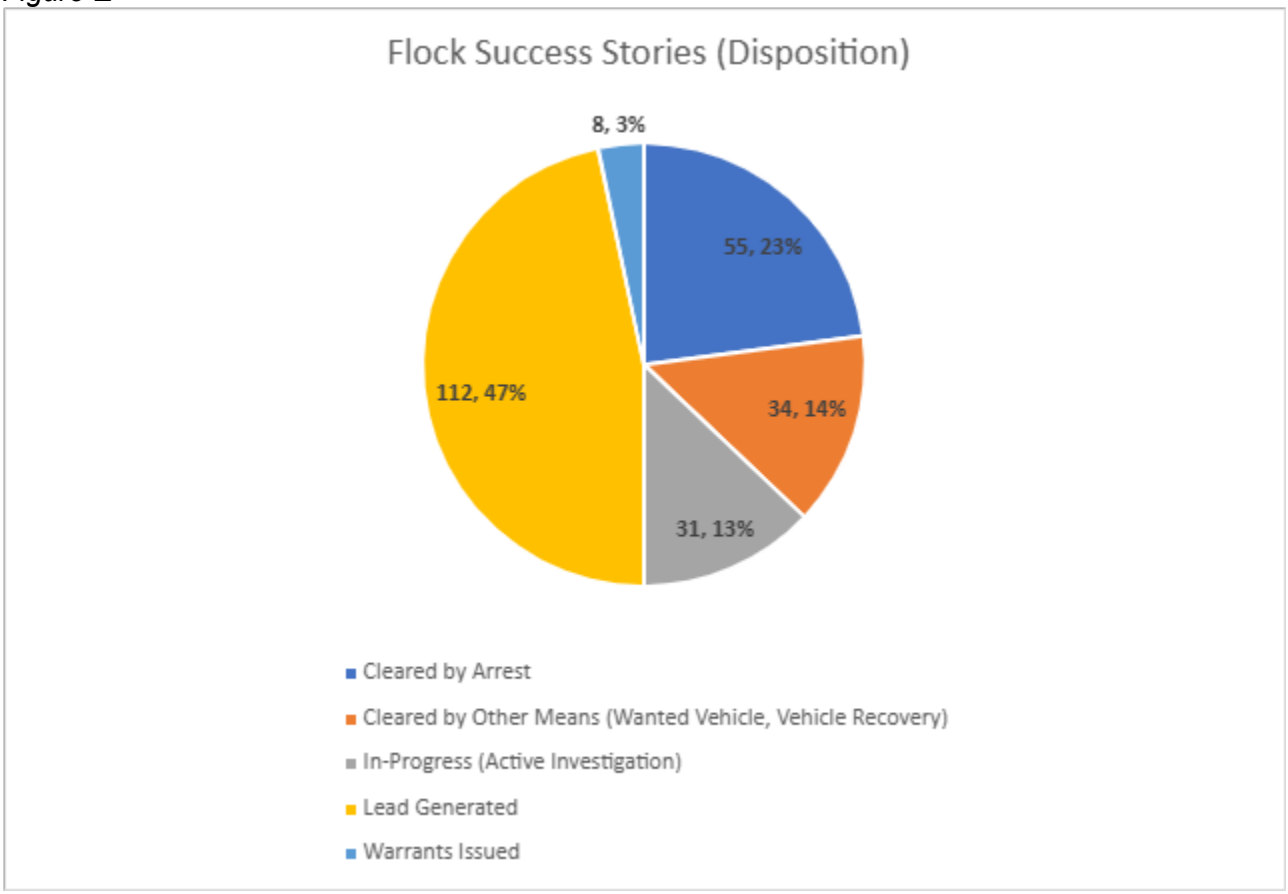
The Oakland Police Department reached out to Flock and on January 14th, 2025, received a response from Flock attesting that "Flock did not suffer any security breaches as it relates to our infrastructure, [or] unauthorized access to data collected by the surveillance technology". The Director of Risk and Compliance at Flock was copied on the response, which was authored by our Customer Success Manager at Flock.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

OPD was also able to better track the outcomes of utilizing ALPR as an investigative tool. All the information that follows can be found on the tabs labeled Flock Outcomes (Enforcement) and Flock Outcomes Metrics in the PAC 2024 Annual Report Data spreadsheet.

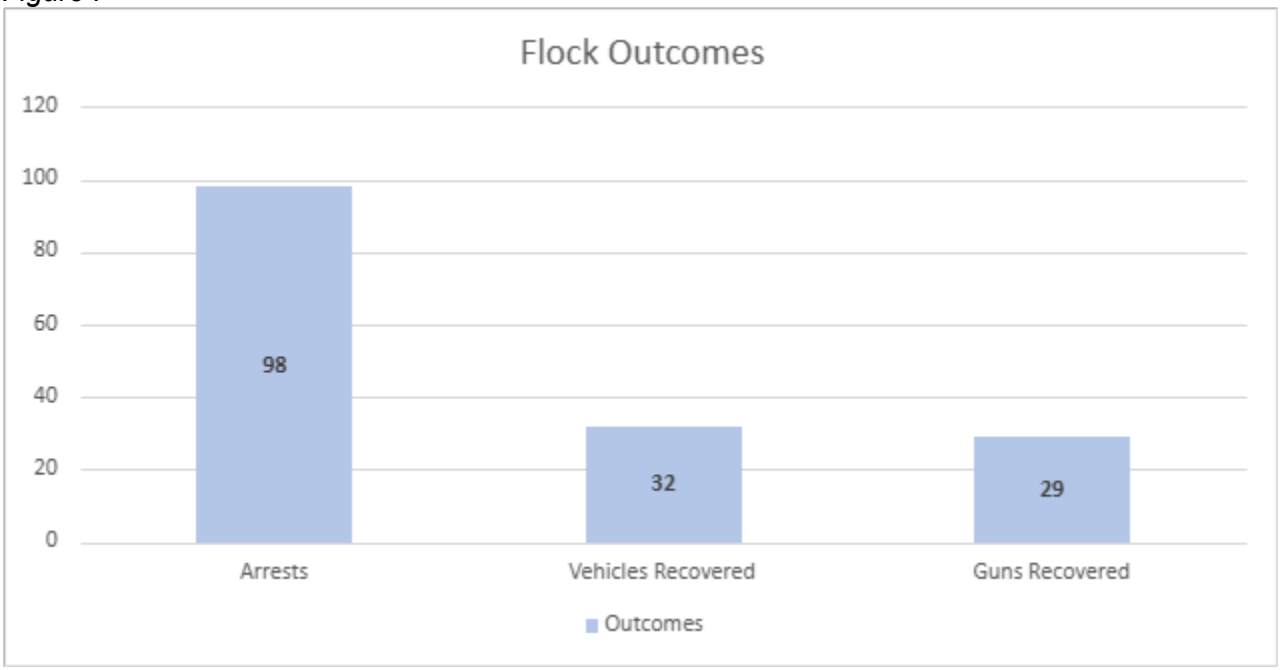
As shown in ***Figure E*** below, OPD logged a total of 240 enforcement actions in Flock from August 2024 through February of 2025. Based on these actions, OPD was able to generate 112 leads, 55 were cleared by arrests, 34 were cleared by other means such as vehicle recovery, 31 are in-progress investigations, and 8 warrants were issued.

Figure E



Summarization of all outcomes shows that OPD made 98 arrests, recovered 32 vehicles, and recovered 29 guns, as seen in ***Figure F*** below:

Figure F



OPD, through a manual review of the data, was able to determine the offense linked to each of these outcomes as listed below in ***Table A***. Some areas of note are Robbery+, which includes elements such as armed robbery or a strongarmed robbery, which had 38 arrests, 17 vehicles recovered, and 4 guns recovered. In addition, Flock was used to make 7 arrests, recover 2 vehicles, and recover 8 guns in homicide/murder/manslaughter investigations. Moreover, for Robberies, OPD made 15 arrests, recovered 2 vehicles and 3 guns. Finally, for aggravated assault, OPD recorded 10 arrests, and 6 guns recovered. In the short few months that OPD has had Flock, it has proved an invaluable investigative tool.

OPD has quickly identified vehicle(s) of interest related to crimes and quickly identified vehicle(s) utilized in a series of crimes. These still images are sent via email to officers and hot listed and officers have had quickly solved cases.

Table A

Offense	**Arrests**	**Vehicles Recovered**	**Guns Recovered**
Aggravated Assault	10	0	6
Burglary	2	2	0
Carjacking	3	2	0
Criminal Threats/Domestic Violence	2	0	0
Felony Evading	5	0	0
Homicide	3	2	5
Motor Vehicle Theft	5	5	0
Human Trafficking	3	0	1

Murder/Manslaughter	4	0	3
Prostitution	1	0	2
Rape	1	0	0
Robbery	15	2	3
Robbery +	38	17	4
Weapons Possession	1	0	2
Weapons Possession +	4	0	2
Other	1	2	1
Total	**98**	**32**	**29**

Finally, here are three example cases that demonstrate the usefulness of Flock cameras to OPD:

- RD#24-044602: On 06 Sep 24, a robbery occurred in the area of 3315 High St. Surveillance cameras captured the suspect vehicle. Investigators utilized FLOCK technology to help identify recent locations for the suspect vehicle. Within 6 hours, Ceasefire officers and the OPD helicopter located the vehicle and some of the suspects in the act of committing another robbery. The helicopter's presence interrupted that robbery and then followed the suspects throughout the city, eventually arresting two suspects near the Rockridge BART station. Additional suspects were identified and warrants for their arrests have been obtained. This is still an active investigation. The suspects referenced herein are male, adult, Oakland residents.

- RD#24-044939: On 08 SEP 24, around 1830 hours, a road rage incident occurred in the area of 19th Street and Market St. The two involved drivers exited their vehicles and engaged in an argument. One of the two drivers fired a gun towards the other driver. The other driver was not injured. The suspect fled the scene. Nearby surveillance cameras captured images of the suspect's vehicle. Investigators utilized FLOCK technology to alert nearby law enforcement agencies as to the description of the vehicle. On 13 Sep 24, officers with the Newark Police Department located and arrested the suspect based on the alerts disseminated by OPD. The arrestee was a male, juvenile, in possession if a handgun.

- RD# 24-045769: A PC246 (Shooting at a Building) occurred on 12 Sep 24, at about 1824 hours in front of 8501 International Blvd (Allen Temple Baptist Church). Surveillance video captured images of a suspect vehicle. On 14 Sep 24, investigators utilized FLOCK technology to identify a possible match, sharing that information with field units. Within 12 hours, OPD officers had located the suspect vehicle and arrested the driver in possession of a firearm. The driver provided a statement to investigators linking him to the shooting of the Church. The arrestee is a male, adult, Oakland resident.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

OPD received four (4) Public Records Requests (PRRs) in 2024 that were related to ALPR technology, three are responded to and one awaits completion of our response. The requests are summarized below:

- 24-10626 – Requesting a list of all Flock camera locations
- 24-1170 – Requesting the names of agencies with whom OPD shared Flock data, the agencies from which OPD receives Flock data, the names of agencies with whom OPD shared hotlist information and the names of

agencies from which OPD received hotlist data from. The request also asked for the number of total plate detections and total hotlist detections for 2024.

- 24-12841 – which asked for all records related to any surveillance technology – this is still pending due to large of amount of data it will generate
- 24-5161 – which asked for any ALPR logs, names of agencies who we receive data from, names of agencies who receive hotlist information from OPD, hits or detections from hotlists, and any communications between OPD and Kaiser Permanente relating to ALPR

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

The estimated cost for Flock for the first year is approximately $500,000, due to the way that cameras were prorated based on their use in the first contract year. OPD anticipates that the next year of Flock service will cost approximately $1,000,000 and this will come out of the Oakland Police Department's budget. Funds will be allocated from the General-Purpose Fund (1010), Information Technology Unit Org. (106410), Contract Services Account (54919), Administrative Project (1000008), Agency-wide Administrative Program (PS01).

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

OPD has no requests at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact, Dr. Carlo M. Beckman, at cbeckman@oaklandca.gov.

Respectfully submitted,

Dr. Carlo M. Beckman, Project Manager II
OPD, Bureau of Risk Management, Information Technology & Fleet

---

Reviewed by:
Dr. Tracey Jones, Police Services Manager I
OPD, Bureau of Risk Management, Research & Planning

Prepared by:
Dr. Carlo M. Beckman, Project Manager II
OPD, Bureau of Risk Management

Lt.. Omar Daza-Quiroz
OPD, Bureau of Investigations

A/Lt. Gabriel Urquiza
OPD, Bureau of Investigations, Real-Time Operations Center

Immigration

415.1 PURPOSE AND SCOPE

The purpose of this immigration policy is to provide guidance and direction to the members of the Oakland Police Department (OPD) on Federal, State, and local immigration laws.

The responsibility for enforcement of immigration laws rests solely with the U.S. Immigration and Customs Enforcement agency (ICE) under the direction of the United States Department of Homeland Security (DHS), and not with local or state law enforcement agencies. OPD is committed to equal enforcement of the law and equal service to the public regardless of a person's immigration status. This commitment increases our effectiveness in protecting and serving the entire community.

415.2 DUE PROCESS RIGHTS OF ALL PERSONS

OPD shall not provide federal immigration agencies access to individuals solely for the purpose of immigration enforcement.

If OPD receives a federal immigration detainer request for an individual in OPD custody, Officers shall provide the individual with a copy of the request.

Officers shall not inquire or request proof of immigration status or citizenship when providing services or benefits except where the receipt of such benefits or services is contingent upon one's immigration status, such as in the processing of a U visa or T visa.

Individuals with limited English proficiency must be given access to translation or interpretation and must receive documents in their native language if available.

415.3 FEDERAL LAW

The responsibility for enforcement of immigration laws rests solely with ICE, under the direction of DHS.

Immigration detainers or requests, sometime called "ICE holds," are not compulsory. Instead, they are merely requests enforceable at the discretion of the agency holding the arrestee. Federal regulations define immigration detainers as "requests" rather than commands.[1] Courts have also held that ICE detainers are voluntary requests that "do not and cannot compel a state or local law enforcement agency to detain suspected aliens subject to removal."[2] Thus, local agencies are "free to disregard [an] ICE detainer."[3]

[1] 8 C.F.R. § 287.7(a).
[2] *Galarza v. Szalczyk*, 745 F.3d 634 (3rd Cir. 2014); *see also Flores v. City of Baldwin Park*, No. CV 14-9290-MWF, 2015 WL 756877, at *4 (C.D. Cal. Feb. 23, 2015) ("federal law leaves compliance with immigration holds wholly within the discretion of states and localities").
[3] *Galarza*, 745 F.3d at 645.

The mere fact that an individual is unlawfully in the United States is not a criminal offense.[4] Thus, unlawful presence in the United States, by itself, does not justify continued detention beyond that of an individual's normal release date. This applies even where ICE or United States Customs and Border Protection (CBP) provide an OPD officer with administrative forms that use the terms "probable cause" or "warrant." A lawful detention under the Fourth Amendment must be supported by probable cause that a person has committed a crime.[5]

415.4 CITY POLICY

Members of OPD shall not:

- Enforce or assist ICE in the enforcement of violations of civil immigration laws
- Initiate investigations or use personnel or resources where the only objective is to discover whether an individual is in violation of a civil immigration law
- Detain individuals for a violation of civil immigration law[6]

415.5 REQUESTS FOR ASSISTANCE FROM DHS OR ICE

Unless the circumstances present an imminent danger to officer or public safety, requests by DHS or ICE for any operational assistance from OPD (including but not limited to ICE detainer requests), shall immediately be directed to the watch commander on duty for approval, who in turn shall immediately notify the Chief of Police, or the Chief's designee.

In the event a determination needs to be made about whether an ICE detainer request should be fulfilled, the Chief of Police, or the Chief's designee, shall consider the merits of each request carefully. In making this determination, the Chief, or Chief's designee, shall comply with the California TRUST Act,[7] assess whether the individual poses a risk to public or officer safety, and consider the availability of OPD personnel and resources necessary to comply with the request.

415.6 INFORMATION SHARING

OPD does not collect any information regarding a person's immigration status, unless the information is gathered specifically for the purposes of completing U visa or T visa documents.

Officers shall not share non-public information about an individual's address, upcoming court date, or release date with ICE or CBP. Officers shall respond to an ICE or CBP request for non-public information only when a judicial warrant accompanies the request.

---

[4] *Arizona v. United States*, 567 U.S. 387, 132 S. Ct. 2492, 2505 (2012); *Melendres v. Arpaio*, 695 F.3d 990, 998, 1000 (9th Cir. 2012).

[5] *Gerstein v. Pugh*, 420 U.S. 103, 120 (1975).

[6] *See* November 29, 2016, Oakland City Council "Resolution Denouncing Tactics Used to Intimidate Immigrants Residing in Oakland and Re-affirming the City's Declaration as a City of Refuge" (Resolution No. 86498).

[7] *See* Gov't Code, §§ 7282, 7282.5. The TRUST Act limits the discretion of law enforcement officials to detain an individual pursuant to a federal immigration detainer request, should an agency choose to do so, unless two conditions are met. First, the continued detention must "not violate any federal, state, or local law, or any local policy," and second, the detainee must have a qualifying criminal history as enumerated in Government Code section 7282.5(a) or be the subject of an outstanding federal felony arrest warrant.

415.7 U VISA AND T VISA NONIMMIGRANT STATUS

Under certain circumstances, federal law allows temporary immigration benefits, known as a U visa, to victims and witnesses of certain qualifying crimes. Similar immigration protection, known as a T visa, is available for certain qualifying victims of human trafficking.

Any request for assistance in applying for a U visa or T visa should be forwarded in a timely manner to the Special Victims Section (SVS) Lieutenant for review and endorsement. The SVS Lieutenant may consult with the assigned investigator to confirm the applicant is cooperative with the investigation.

The SVS Lieutenant or their designee shall approve or deny the request and complete the certification or declaration, if appropriate, within the time frame required under Penal Code § 679.10(h).[8] The instructions for completing certification and declaration forms can be found on the U.S. Department of Homeland Security (DHS) website and under Penal Code § 679.10.

The OPD website has information regarding the U visa or T visa application process as well as a non-profit organization that can assist with the application process.

[8] "A certifying entity shall process an I-918 Supplement B certification within 90 days of request, unless the noncitizen is in removal proceedings, in which case the certification shall be processed within 14 days of request." Penal Code § 697.10(h).

Oakland Police Department
Media Team

For Immediate Release: July 14, 2025
OPD News:

An article released today by the *San Francisco Standard* initially stated, *"Oakland cops gave ICE license plate data."* It went on to say, *"Oakland Police fulfilled a request related to an ICE investigation on one occasion."* Both versions are misleading and do not accurately reflect the Oakland Police Department's data-sharing agreement with other California and local law enforcement agencies.

To be clear, **no member of the Oakland Police Department was involved in this alleged sharing of ALPR information with Immigration and Customs Enforcement (ICE).**

Oakland began using its current Automated License Plate Reader (ALPR) system in July 2024. ALPR cameras capture and read license plate information to aid in the investigative process. This system has become a valuable tool in helping our officers solve crimes more efficiently, locate homicide and robbery suspects, and recover firearms. By providing timely and accurate information, ALPR technology helps our officers respond quickly to public safety threats.

Consistent with SB 34, OPD shares ALPR data with more than 80 California local and state law enforcement agencies. All of these agencies, including OPD, are subject to the California Values Act, which prohibits agencies from using resources for immigration enforcement purposes.

In compliance with city policy, OPD does not enforce or assist Immigration and Customs Enforcement (ICE) officials in enforcing civil immigration law violations.

Additionally, ALPR data captured within the City of Oakland shall not be used in violation of Oakland's Sanctuary City Ordinance.

In OPD’s data sharing request form, we require all agencies using our system to “be in compliance” with state law.

As it relates to the sharing of data with any federal agency, OPD is verifying that any access conducted by its members related to APLR data remains consistent with state law, including SB 34 (California Civil Code section 1798.90.5 et seq.) and the California Values Act (Gov Code section 7284 et seq.).

We (OPD) are very conscientious and sensitive to the use of emerging technology while continuing to explore solutions to support public safety, protect people's right to privacy, and build community trust.

We are committed to transparency, accountability, and maintaining the trust of our community. We value our relationship with our media partners and want to ensure and encourage that the information they provide is accurate.