CITY OF OAKLAND

Privacy Advisory Commission

April 4, 2019 5:10 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Agenda

Commission Members: ***District 1 Representative:*** *Reem Suleiman,* ***District 2 Representative:*** *Chloe Brown,* ***District 3 Representative:*** *Brian M. Hofer,* ***District 4 Representative:*** *Lou Katz,* ***District 5 Representative:*** *Raymundo Jacquez III,* ***District 6 Representative:*** *Vacant,* ***District 7 Representative:*** *Robert Oliver,* ***Council At-Large Representative:*** *Vacant,* ***Mayoral Representative:*** *Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:10pm: Call to Order, determination of quorum
2. 5:15pm: Open Forum/Public Comment
3. 5:20pm: Review and take possible action on the OPD Automated License Plate Reader Anticipated Impact Report and draft Use Policy.
4. 6:00pm: Review and take possible action on the OPD Remote Camera Impact Report and draft Use Policy.
5. 7:00pm: Adjournment

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Automated License Plate Reader

1. Information Describing the Automated License Plate Reader (ALPR) and How It Works

ALPR technology consists of cameras that can automatically scan license plates on vehicles that are publicly visible (in the public right of way and/or on public streets). The Oakland Police Department (OPD) uses only ALPR cameras mounted to patrol vehicles so that license plates can be photographed during routine police patrol operations. Each camera housing (two housings per vehicle) consists of a regular color photograph camera as well as an infrared camera (for better photography during darkness). ALPR reads these license plates with a lens and charge-coupled device (CCD) that sense and records the image (can be parked or moving vehicle plates) and connects the image to an optical character recognition (OCR) system that can connect the image to that actual license plate characters.

The ALPR system in a patrol vehicle is turned on automatically when authorized personnel turn on their vehicle-based computer at the beginning of a police patrol shift. Once initiated, the system runs continuously and photographs vehicles until turned off manually[1]; ALPR cameras typically records hundreds of license plates each hour but exact recording rates depend on vehicle activity and how many vehicles are encountered. The system compares license plate characters against specific databases, and stores the characters along with the date, time, and location of the license plate in a database. Authorized personnel within OPD can also enter specific license plate numbers into the system so that active vehicle ALPR systems will alert the officer in the vehicle if there is a real-time match between the entered license plate and the photographed license plate. OPD personnel will contact OPD Communications Division (dispatch) anytime the ALPR system signals that a license plate on a database has been seen; OPD personnel always personally check with Communications before actually stopping a vehicle based on a ALPR license plate match.

The platform software allows authorized personnel to query the system to see if a certain license plate (and associated vehicle) have been photographed. The system will show the geographic location within Oakland for license plates that have been photographed, as well as time and date. Authorized personnel can see the actual photographs that match a particular license plate

[1] Data captured by the ALPR system will be uploaded onto the OPD ALPR database when the computer is turned off – typically at the end of a patrol shift.

query – the OCR system can incorrectly match letter and digit characters so the actual photographs are vital for ensuring the accuracy of the license plate query.

2. Proposed Purpose

OPD uses ALPR for two purposes:

1. The immediate (real time) comparison of the license plate characters against specific databases such as those provided by the California Department of Justice listing vehicles that are stolen or sought in connection with a crime or missing persons; and
2. Storage of the license plate characters – along with the date, time, and location of the license plate – in a database that is accessible by law enforcement (LEA) agencies for investigative purposes.

3. Locations Where, and Situations in which ALPR Camera Technology may be deployed or utilized.

OPD owns 35 sets (left and right) of ALPR vehicle-mounted cameras. Authorized personnel (as described in the Mitigations Section below) may operate ALPR camera technology on public streets in the City of Oakland.

4. Impact

ALPR technology helps OPD personnel to leverage their street presence and to more effectively use their limited time for more critical activity. The technology can alert officers to vehicles that are stolen or connected to a serious felony crime (e.g. aggravated assault, homicide, robbery, sexual assault) immediately (by automatically connected to criminal databases). Officers can then use the information to notify OPD personnel and/or stop the vehicle as justified by the information. The automatic process can free officers from laborious data entry processes allowing more time for observing public activity and speaking with members of the public.

ALPR also provides an important tool for criminal investigations. The information collected by analysts and investigators can locate locations where a plate has been in the past, which can help to confirm whether or not a vehicle has been at the scene of a crime. Additionally, accurate photos of vehicle from the ALPR system make searching for vehicles much easier – how the vehicle differs from every other vehicle of the same make and model. The photos frequently show distinctive dents, scratches, stickers, etc. ALPR also allows investigators to review photos which depict what the vehicle looks like, or more importantly, how the vehicle differs from every other vehicle of the same make and model. The photos frequently show distinctive dents, scratches, stickers, etc. Investigators can also confirm that the vehicle matches the licenese plate and whether the license plate has been switched from a different vehicle.

Formatted: List Paragraph, Right: 0", Space After: 8 pt, Line spacing: Multiple 1.05 li, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Arial, Font color: Black, Pattern: Clear (White)

Formatted: Font: (Default) Arial, Font color: Black

Formatted: Indent: Left: 0"

Such information may help personnel to find new leads in a felony crime investigation.

OPD has not historically tracked ALPR usage for vehicle stops, nor for later criminal investigations[2] in a way that easily allows for impact analysis. However, OPD's Criminal Investigations Division (CID), in preparation for this report, has found cases where ALPR license plate locational data was instrumental in the ultimate arrest and arraignment of at least two homicide suspects, and with the conviction of at least one of them. CID investigators use ALPR almost every day on investigations each year to investigate the locations of suspects in major violent crimes including homicide, robbery and aggravated assault; OPD's IT unit found 147 cases where investigators asked OPD IT to query ALPR for specific license plates related to criminal investigations. There are also documented cases where other LEA contact OPD to make specific queries regarding serious crimes which have occurred in their jurisdictions. OPD personnel believe that ALPR has provided critical information for many other felony cases but cannot currently document them.

OPD recognizes that the use of ALPR technology raises significant privacy concerns. There is concern that the use of ALPR technology can be utilized to ascertain vehicle travel patterns over periods of time. Research shows that "meta data", individual data points such as phone numbers called, and time of day or vehicle locations can be combined to create patterns that identify individuals. Using a simple algorithm, Stanford lawyer and computer scientist Jonathan Mayer was able to accurately identify 80% of the volunteers in his study, using only open source databases such as Yelp, Facebook, and Google3.

OPD can use the ALPR technology to see if a particular license plate (and thus the associated vehicle) was photographed in particular places during particular times; however OPD can only develop such by manually querying the system based upon a right to know (see Mitigation Section 5 below. OPD also recognizes that ALPR cameras may photograph extraneous data such as images of the vehicle, the vehicle driver and/or bumper stickers or other details that affiliate the vehicle or driver with particular groups. As explained in the Description Section (1) above and the Mitigation (5) section below, authorized personnel can only manually query the ALPR system for particular license plates (or all plates within a defined area) and only for particular reasons as outlined in OPD policy. Therefore, technology cannot be used to query data based upon vehicle drivers, type of vehicle, or based on any type of article (e.g. bumper sticker) affixed to a vehicle. Additionally, OPD has instituted many protocols (see Mitigation section below) to safeguard against

[2] Current policies mandate documenting reasons for vehicle stops and reported race and gender persons stopped. OPD is reviewing how to ensure that investigators note when ALPR was instrumental in criminal investigations for documenting ALPR impact.

[3] Today, data scientists can accurately identify over 95% of individuals based solely on four geospatial (time, location) data points.

the unauthorized access to any ALPR data.

There is concern that ALPR camera use may cause disparate impacts if used more intensely in certain areas such as areas with higher crime and greater clusters of less-advantaged communities. OPD does not affix ALPR cameras to fixed infrastructure. OPD deploys ALPR camera-affixed vehicles through every area of Oakland[4], even though there may be times when OPD Commanders request that ALPR cameras be used in particular areas for short periods of time to address crime patterns. Additionally, ALPR usage does not lead to greater levels of discretionary police stops; ALPR use leads to vehicle stops only where a real-time photographed license plate matches a stop warrant for a stolen vehicle or serious crime in a criminal database.

Databases such from the State of California Department of Justice (DOJ) can contain some outdated or inaccurate data. ALPR systems, just as in the case of a_-manual query in a police vehicle computer, will provide the license plate data from the related database. ALPR systems simply make the query faster. In such cases personnel will follow standard policies and procedures for stopping a motorist and requesting personal identification (explained on page 1 above).

Formatted: Indent: Left: 0.49"

5. Mitigations

Privacy advocates note that people are generally creatures of habit and often drive in their vehicles the same way to work, house of worship, and neighborhood grocery store. OPD recognizes that Oakland residents and visitors have hold an expectation of privacy and anonymity, even though OPD as well as members of the public have a right to photograph State-issued license plates. In recognition of these concerns, OPD ALPR policy provides several mitigations which limit the use real-time and aggregated ALPR data.

OPD's ALPR system, (as mentioned in Section 1 above), uses OCR to capture license plate data. ALPR cameras are designed to focus on license plates cameras, and the OCR only records the license plate characters. Extraneous data (e.g. human faces, car type, bumper stickers, ect.) may be captured in an ALPR image capture. However, only OCR data (letters and numbers) will be entered into OPD's ALPR database. Therefore, only OCR character data can be queried by OPD.

ALPR can only be used for serious and documented crimes which are captured in databases such as DOJ; therefore, OPD cannot use ALPR to track low-level misdemeanor crimes. Additionally, OPD conducts annual system audits (see Section 6 "Data Types and Sources" below to ensure proper system use. Audit data will be included in the annual surveillance technology report provided to the City's Privacy Advisory Commission (PAC).

[4] OPD often must use ALPR camera-equipped vehicles for standard patrol activity regardless of location because of limited fleet reserves.

OPD audit data will not be purged - only the plates and images associated to them are purged. The ALPR coordinator can create a log query which will document aspects of use activity (time, date, and what is searched).

Formatted: Indent Left 0"

OPD's Direct General Order (DGO) "I-12: Automated License Plate Readers" Policy Section "B-2 Restrictions on Use," provides a number of internal safeguards, including:

1. 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 court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53);
3. Personnel must complete equipment-specific training prior to use;
4. No ALPR operator may access department, state or federal data unless otherwise authorized to do so;
5. Consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents;
6. ALPR shall only be used for official LEA business; and
7. If practicable, agency personnel should verify ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert (Section 1 above explains that personnel shall contact Communications prior to making a vehicle stop based on ALPR matches).

OPD requires ALPR training of all personnel authorized to access the ALPR system. This training includes subjects such as:

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

6. Data Types and Sources

ALPR data is composed of photographs of license plates, which can be linked through OCR software to identify license plate letter and digit characters. License plate photographs, as detailed in Section One above, may contain images of the vehicle with particular visual details of the vehicle (such as vehicle make or model or bumper stickers). Photographs may also contain images of the vehicle driver. However, the ALPR system only annotates photographs based on license plate characters; therefore, authorized personnel can only query license plate numbers – there is no way to query the system based on type of vehicle, vehicle details (such as bumper stickers) or individuals associated with a vehicle.

OPD is currently seeking legal guidance regarding State of California law which relates to ALPR and other data retention requirements (-specific plates cannot be marked and kept in the system beyond the retention values set in the device settings). Users would have to make screenshots or use some other tool outside of BOSS to do this.

Formatted: Font: (Default) Arial

OPD shall permanently maintain ALPR data when connected to one of the following situations:

1. A criminal investigation;
2. An administrative investigation;
3. Research;
4. Civil litigation;
5. Training[5]; and/or
6. Other Departmental need.

7. Data Security

OPD takes data security seriously and safeguards ALPR data by both procedural and technological means. OPD will 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 data downloaded to the mobile workstation and in storage 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. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate LEA purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

The OPD ALPR system is not-cloud based; ALPR-camera equipped vehicle

[5] OPD may keep ALPR footage permanently as part of training modules to train personnel in how to use the ALPR system.

computers can download (not upload) State DOJ databases as described above, but OPD ALPR data is stored only on OPD in-building servers. Very limited individuals have access to OPD computers with access to ALPR data; the ALPR coordinator is responsible for providing training including the verification of potentially malicious email or other forms of computer hacking. OPD also conducts regular ALPR system audits to ensure the accuracy of ALPR data.

8. Costs

OPD spent $293,500 in 2014 to purchase the ALPR system from 3M. Neology later purchased the ALPR product line from 3M. OPD however does not have a maintenance contract with Neology and therefore relies on EVO for ALPR maintenance. OPD has spent approximately $50,000 annually with EVO-Emergency Vehicle Outfitters Inc. for ALPR vehicle camera maintenance. OPD relies on EVO to outfit police vehicles with many standard police technology upgrades (e.g. vehicle computers) as well as ALPR camera maintenance. However, OPD's current ALPR camera fleet are no longer covered by a maintenance contract and OPD now only spends approximately $3,000 annual for software support.

9. Alternatives Considered

OPD officers and investigators rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

ALPR technology provides LEA personnel with a fast and efficient way to connect vehicles to violent and felonious criminal activity. This tool helps OPD's authorized personnel increase their ability to find wanted suspects and help solve crimes in a way that is unique – by creating a time map of vehicle locational activity. OPD recognizes the privacy concerns inherent in such a technology but has in place the numerous mitigations and data security protocols described in sections five and seven above respectively. However, OPD believes that the alternative to ALPR usage would be to forgo its observational and investigatory benefits. OPD LEA personnel, without access to ALPR data, would rely patrol officer observations and other basic investigatory processes. OPD data suggest that some future violent felonies would remain unsolved if only for the inability to use ALPR technology.

10. Track Record of Other Entities

Commented [BS1]: I have calls into Beverly Hills PD and Orinda PD which have been postponed; I have reached out to several police agencies for comment.

Numerous local and state government entities have researched and evaluated the use of ALPR cameras. The International Association of Chiefs of Police (IACP) documents many recent reports[6]. The AICP report, "News Stories about Law Enforcement ALPR Successes September 2017 - September, 2018"[7] presents scores of cases from different national LEA jurisdictions where ALPR data helped lead to the capture of violent criminals. A July 2014 study[8] from the Rand Corporation research organization found that ALPR cameras have proven useful for crime investigations in numerous cities and states, and that systems with the most database access and longest retention policies provide the greatest use in terms of providing real-time information as well as useful investigation data. This report also find that privacy mitigations are critical to ensuring legal use of ALPR and public privacy protections. The RAND report, in considering privacy concerns discusses the difference between collecting only license plate data and other personally identifiable information (PII); OPD ALPR system does not collect PII. The RAND report also cites a 2013 ACLU report (page 17) which raises First Amendment concerns and that such concerns are increased in proportion to longer data retention periods (increased potential for tracking vehicle travel patterns and locations) as well as less controlled database access (greater risk of improper use).

[6] https://www.theiacp.org/projects/automated-license-plate-recognition

[7] https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf

[8] https://www.rand.org/pubs/research_reports/RR467.html

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Commented [BS1]: Correct?

Effective Date: XX Mar 19
Coordinator: Information Technology Unit

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. 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.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

A. Description of the Technology

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images.

A – 1. How ALPR Works

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against specific databases, and stores the characters along with the date, time, and location of the license plate in a database. This process allows for two functions by ALPR:

1. Immediate (real time) comparison of the license plate characters against specific databases such as those provided by the California Department of Justice listing vehicles that are stolen or sought in connection with a crime or missing persons.
2. Storage of the license plate characters – along with the date, time, and location of the license plate – in a database that is accessible by law enforcement agencies for investigative purposes.

Commented [BS2]: Database itself is NOT accessible....be more descriptive....

A – 2. The ALPR System

There are two components to the ALPR system:

1. Automated License Plate Readers: These devices include cameras attached to vehicles, trailers, or poles and a corresponding device that transmits collected data to various state databases for comparison and a central repository for storage and later retrieval.

2. ALPR Database: This central repository stores data collected and transmitted by the Automated License Plate Readers.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Such personnel shall be limited to designated sergeants, officers, police service technicians, and parking enforcement personnel unless otherwise authorized.

B – 2. Restrictions on Use

1. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53); authorized purposes consist only of queries related to criminal investigations~~.~~

Commented [BS3]: Ok to say? PAC wanted more definition here.

2. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

3. No ALPR operator may access department, state or federal data unless otherwise authorized to do so pursuant to Section D1 below.

4. While ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during Whenever practicable, agency personnel should verify ALPR response through the OPD Communications Section (which accesses -California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

Commented [BS4]: Do we also go to CLETS required? Do we call communication ALWAYS first, and commulcations can ask CLETS?

Formatted: List Paragraph, Right: 0", No bullets or numbering

Formatted: Indent: Left: 1.01", Hanging: 0.5", No bullets or numbering

~~4.~~

5. major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

6. ALPR shall only be used for official law enforcement business.

7. ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR to scan license plates or collect data.

8. 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 court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.

C. ALPR Data

C – 1. Data Collection and Retention

1. Transfer of Data

   Data will be transferred from vehicles to the designated storage in accordance with department procedures.

2. Data Retention

   All ALPR data downloaded to the server shall be stored for six months, unless required for:

   a. A criminal investigation;
   b. An administrative investigation;
   c. Research;
   d. Civil litigation;
   e. Training; and/or
   f. Other Departmental need.

Commented [BS5]: Can we delete – do we really need ALPR for training?

Commented [BS6]: They see this as a loop hole.... "other departmental needs" Can we delete this?

C – 2. Data Security

All data will be closely safeguarded and protected by both procedural and technological means. OPD will 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 data downloaded to the mobile workstation and in storage 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. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

3. ALPR system audits shall be conducted on a regular basis by the Bureau of Services. The purpose of these audits is to ensure the accuracy of ALPR Information and correct data errors.

C – 3. Releasing or Sharing ALPR Data

ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the ALPR data that includes:

a. The name of the requesting agency.
b. The name of the individual making the request.
c. The intended purpose of obtaining the information.

2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

Commented [BS7]: Can this be captured in an annual report? How will this be recorded. Can PAC see approved requests?

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-9.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

D. ALPR Administration

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Bureau of Services.

D – 1. ALPR Administrator

The Bureau of Services Deputy Chief or Deputy Director 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 Bureau of Services Deputy Chief is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of ALPR data.

D – 2. ALPR Coordinator

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

Commented [BS8]: Questions from PAC (that we should address in annual report:
* Can someone in OPD alter data... can data be manipulated?
* Can we get exact count per last few months?
* SB 34 – we need record of who is accessing / what are we doing w/ audits? How many queries???
* How many stolen cars???

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of ALPR technology to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of times the ALPR technology was used.
2. A list of agencies other than the Oakland Police Department that were authorized to use the equipment.
3. A list of agencies other than the Oakland Police Department that received information from use of the equipment.
4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

Commented [BS9]: Need to buff out geography, list of times a fed agency….annual report…..say annual report:

Total scans, total hits, add false positives, false errors / misreads. Number times used in investigation. What happens with out of state plates, paper dealer plates…delete what is in annual report already.

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized 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 authorized in ALPR Users Section include completion of training by the ALPR Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

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

Training updates are required annually.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for Remote and Mobile Cameras

1. Information Describing Remote and Mobile Cameras and How They Work

OPD utilizes different types of cameras to capture single image and video data. Cameras that are strictly manually operated are not considered "surveillance technology" under the Oakland Surveillance Ordinance No. 13489 C.M.S. However, some RMCs allow for real-time remote access viewing of activity captured by the RMC lens. Single image and video RMCs may be manufactured with data transmitting technology or be outfitted by OPD with separate camera transmitters. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Mobile functionality allows RMCs to be moved and positioned as the need requires.

RMCs may have their own power supply or attached to a utility pole so as to utilize electricity for power. In either case, RMCs offer personnel critical situational and evidentiary information in a safe way.

RMCs store visual (and sometimes audio) data with either internal storage and/or by transmitting data in real-time to a remote OPD location.

2. Proposed Purpose

RMCs are used by OPD authorized personnel to gather evidence during undercover operations as well as during mass-events personnel are deployed to observe and promote public safety. Live stream image and video capture allow investigators to observe activity related to suspected criminal activity.

3. Locations Where, and Situations in which GLD System may be deployed or utilized.

A RMC may be used anywhere in the public right of way within the City of Oakland. Personnel may use hand-held cameras with live-viewing capabilities within in the public right of way within the City of Oakland; however, these cameras are generally only used for mass-person events to as to provide situational awareness during events where public safety must be monitored (e.g. large protests or parades). RMCs may also request that a utility company install a RMC to a utility pole for powered live-remote viewing. OPD will only request to install a RMC to a utility pole with a court order allowing the utility company to install the camera.

4. Impact

RMCs offer evidentiary and situational awareness in numerous ways that challenge measurement. Mass events where thousands of people gather require that police personnel see where people are moving in real-time to better ensure that resources are provided as needed to ensure public safety.

OPD's Criminal Investigations Division (CID) and Intel Unit occasionally need to monitor street locations with remote live-view cameras to gather evidence related to suspects in criminal cases. RMCs can provide useful evidence about particular suspects relating to violent criminal activity.

OPD recognizes that any use of cameras to record activity which occurs in the public right of way raises privacy concerns. There is concern that the use of RMCs can be utilized to identify the activity, behavior, and/or travel patterns of random individuals. However, OPD does not randomly employ this technology throughout the City. Rather, RMCs installed on utility poles (after obtaining a court order) are used in specific situations to gather evidence about particular individuals connected to particular criminal investigations. The scope and use of such technology is narrow and limited. Therefore, OPD believes that the impact to public privacy is similarly narrow and limited.

5. Mitigations

All RMCs shall be housed and secured within IT Unit or Intel Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data shall be uploaded onto secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

OPD will consider providing RMC data to other law enforcement (LE) agencies if and when such agencies make a written request for the RMC data that includes:

a. The name of the requesting agency.
b. The name of the individual making the request.
c. The intended purpose of obtaining the information.

Such requests will be reviewed by the Bureau of Services Deputy Chief/

Deputy Director or designee and approved before the request is fulfilled. Approval requests shall be retained on file. Requests for RMC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

OPD will monitor its use of RMCs to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits. The RMC System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period following a reporting structure agreed upon by the Privacy Advisory Commission.

6. Data Types and Sources

RMCs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.

RMCs can be mounted to telescoping monopods to simply extend the range of a RMC. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.

RMCs may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

7. Data Security

All RMCs shall be housed and secured within IT Unit or Intel Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data shall be uploaded onto secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

8. Costs

TBD

9. Third Party Dependence

TBD

10. Alternatives Considered

OPD officers and personnel rely primarily on traditional policing techniques to monitor large events and to gather evidence related to criminal investigations. For decades evidence gathering also includes the use of cameras, sometimes with live-stream transmitters, to record images, video and audio. Police personnel must maintain some level of situational awareness when hundreds and thousands of people gather on public streets and threats to public safety increase. Alternatives to live-stream camersa would include having more officers and personnel deployed during every mass-event. Such a deployment extends beyond OPD budget capacity.

OPD relies on remote view cameras for investigations as described above. There is no clear alternative to capturing actionable image, video and/or audio.

11. Track Record of Other Entities

TBD

DEPARTMENTAL GENERAL ORDER

~~I-20~~: REMOTE AND MOBILE CAMERAS (RMC)

Effective Date:
Coordinator: Information Technology Unit, Bureau of Services Division

The Oakland Police Department (OPD) uses technology to more effectively promote public safety; OPD also strives to institute policies that promote accountability and transparency. This policy provides guidance and procedure for the use, documentation, and auditing of live-stream mobile cameras.

All data, whether sound, image, or video data, generated by OPD's RMC systems are for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Description of the Technology

OPD uses different RMC systems to observe and/or record activity to promote public safety. Some RMCs allow for real-time remote access viewing of activity captured by the RMC lens. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Mobile functionality as well as battery power allows RMCs to be moved and positioned as the need requires.

A – 1. How Remote and Mobile Cameras (RMC) Work

Some RMCs are standard consumer-type cameras that can be held and operated by personnel. RMCs may also be affixed to a variable lens's for different views. RMCs can be attached to a camera monopod and used like a standard digital video camera; the monopod in this case extends the cameras perspective beyond arms reach so that personnel extend the range of view (beyond corners, above head-level in a crowd, or in other related situations). RMCs attached to monopods/tripods provide greater viewing access and promote safety where personnel may need to exercise caution before moving into unknown situations. RMCs may also be attached to utility poles for real-time and long-term remote viewing. In such cases RMCs may be powered through electricity of the utility pole or via portable battery power. In either case, RMCs offer personnel critical situational and evidentiary information in a safe way.

RMCs may also be connected to portable devices that stream live audio and video to remote locations. Such devices provide critical situational and evidentiary information during large-scale mass events.

A – 2. RMC Systems

RMCs can be self-contained devices that record audio and video, which either:

1) store data onto an internal storage device; or 2) transmit data in real-time through various digital transmission formats.

1. RMCs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.
2. RMCs can be mounted to telescoping monopods to simply extend the range of a RMC. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.
3. RMCs may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use RMCs or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.

B – 2. Restrictions on Use

1. Department members shall not use, or allow others to use RMC equipment, software or data for any unauthorized purpose.

2. No member of this department shall operate RMC equipment or access the internally stored RMC data without first completing department-approved training.

3. The RMC systems shall only be used for official law enforcement purposes.

4. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's Information Technology Unit and Criminal Investigations Division (CID) investigators, Internal Affairs Division personnel, crime analysts, the Office of the District Attorney) will have access to RMC audio and video data and system applications.

5. Accessing data collected by RMC systems requires 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, or case law. A need to know is a compelling reason to request information such as direct involvement in an criminal or administrative investigation.

C. RMC Data

C – 1. Data Collection and Retention

RMC system data is maintained both by currently maintained by either: 1) the OPD Information Technology (IT) Unit within in the Bureau of Services (BOS); or 2) by the Intel Unit. Personnel using RMCs from the Intel Unit shall return RMCs at the end of their shift. The Intel Unit RMC Coordinator shall download the data onto secure Intel Unit computers within 24 hours of receiving returned RMC equipment.

The Intel Unit shall maintain all RMC data for 30 days unless notified by the Chief of Police or designee (e.g. Internal Affairs Captain or Criminal Investigations personnel) that the image and video data is needed for an investigation. The OPD Unit and/or assigned personnel issued the RMC is responsible for recovering the data from the RMC.

Data that is part of an investigation shall be provided to the appropriate personnel as a separate digital data file, kept permanently as part of the official investigation record.

The Intel Unit shall delete all RMC data left on installed on Intel Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.

C – 2. Data Security

All RMC data will be closely safeguarded and protected by both procedural and technological means:

1. All RMCs shall be housed and secured within IT Unit or Intel Unit lockers. All RMC data downloaded from RMCs shall be uploaded onto secure user and email password protected IT Unit computers and / or Intel Unit computers.
2. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Those are the protocols used PEU or IAD or RMM systems.

3. Members approved to access RMCs under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data related to an administrative or criminal investigation, or for training purposes.

C – 3. Releasing or Sharing RMC System Data

RMC system data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the RMC data that includes:

   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of obtaining the information.

2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

Requests for RMC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

D. RMC System Administration

OPD's RMC system oversight as well as data retention and access, shall be managed by OPD's Information Technology Unit under the BOS, or designee.

D – 1. RMC System Coordinator

The title of the official custodian of RMC System Coordinator is .....

D – 2. RMC System Administrator

The RMC System Coordinator shall administer all RMC systems, implementation and use, in collaboration with OPD's Criminal Investigations Division (CID). The RMC System Coordinator, or designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The RMC System Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of RMC system data.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of the RMC system to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The RMC System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of times a RMC was deployed, and type of deployment.
2. The number of times RMC data was used as part of an investigation.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of the equipment.
4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D – 4. Training

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

Training requirements for employees authorized to use the GLD system include completion of training by the GLD System Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

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

Trainings for Communications personnel (dispatchers and operators) may include training on how to acknowledge the GLD system activations and how to use the system software to identify activation locations so as to provide information to responding officers.

Training updates are required annually.

By Order of

DEPARTMENTAL GENERAL ORDER ~~I-20~~ Effective Date________
OAKLAND POLICE DEPARTMENT

Anne E. Kirkpatrick
Chief of Police

Date Signed: