CITY OF OAKLAND

Privacy Advisory Commission

April 4, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
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. 5:00pm: Call to Order, determination of quorum

2. 5:05pm: Open Forum/Public Comment

3. 5:10pm: Review and approval of the draft March 7 meeting minutes

4. 5:15pm: Federal Task Force Transparency Ordinance – OPD – presentation of inaugural annual report for FBI/JTTF, review and take possible action.

5. 5:25pm: Surveillance Equipment Ordinance – OPD – Automated License Plate Reader Anticipated Impact Report and draft Use Policy – review and take possible action.

6. 6:00pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and draft use Policy – review and take possible action.

7. 6:20pm: Surveillance Equipment Ordinance – UC Berkeley/Steve Trush – Review of Surveillance Acquisition Technology Questionnaire revisions

8. 6:50pm: Review of Old Business and take possible action
    a. City Attorney opinion re applicability of SB 1160 (BART jammer bill) to cell-site simulator use
    b. City Attorney opinion re applicability of SB 178 (CalECPA) to cell-site simulator use (PC 1546.2 notice provision)

c. JTTF MOU review
d. City Attorney opinion re PC 832.7 and SB 1421 (Skinner) in context of federal transparency task force ordinance annual report (potential violations)

9. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

March 7, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor
Meeting Minutes

***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. 5:00pm: Call to Order, determination of quorum

Members present: Hofer, Suleiman, Katz, Jacquez, Oliver, and Patterson.

2. 5:05pm: Open Forum/Public Comment

There were no open forum speakers.

3. 5:10pm: Review and approval of the draft February 7 meeting minutes

The minutes were approved unanimously.

4. 5:15pm: UC Berkeley's Samuelson Law, Technology & Public Policy Clinic – presentation of draft Privacy Principles; review and take possible action.

Courtney Reed and Amisha Gandhi from the Samuelson Clinic presented the draft principals they have been developing. They described the process that was undertaken including interviewing staff from the Cities of Seattle, WA and Portland, OR to learn about their processes. They also met with key City staff including the Race and Equity Director, Chief Privacy Officer, and City Clerk staff members. They interviewed PAC Members and some outside organizations. They will continue to meet with more City departmental leadership in the coming month and return to the PAC later in the spring.

5. 5:30pm: Federal Task Force Transparency Ordinance – OPD – presentation of inaugural annual reports (FBI/JTTF, ATF, DEA, US Marshals task forces), review and take possible action.

Bruce Stoffmacher first presented the US Marshall Service (USMS) Report and discussed the importance of the relationship with the USMS to the City's successful Cease Fire Program. This program targets those involved in the most serious violent felonies and offers them services to help them change course. For those that continue to engage in violent activity, the consequences are more steep and can involve federal charges. The USMS has been critical in helping track down known suspects and bring them to justice when they flee out-of-state.

The PAC had some clarifying suggestions including adding more narrative language and clarity on the number of hours the OPD officer works with the Task Force. Th report was approved for forwarding to the City Council.

Regarding the JTTF Report, Bruce Stoffmacher indicated that OPD wished to ask the FBI for more information but was not inclined to have to go through a Freedom of Information Act (FOIA) request as suggested by the FBI. He noted that this does not preclude the PAC from filing a FOIA request.

Two Public Speakers again noted their concern that OPD is not providing enough information and that their desire is focused on the work of the whole JTTF, not individual officers.

Bruce rearticulated the department's concern about releasing info that would potentially "out" the officer assigned to the task force since only one OPD officer is involved. Any reporting on violations by that individual would be obviously associated with them. This could put OPD in the position of making public something that could potentially be a confidential personnel matter.

PAC members expressed frustration that due to the stance of the FBI and OPD, the report does not provide any of the information they are interested in assessing. The item was tabled to the April meeting.

6. 5:45pm: Presentation by Electronic Frontier Foundation's Senior Investigative Researcher Dave Maas – use and risks of Automated License Plate Readers

Dave Maas provided a PowerPoint and discussed his extensive research on ALPRs, their use and limitations. The presentation discuss various data retention limits of different agencies and the concerns about how some agencies share data.

7. 6:00pm: Surveillance Equipment Ordinance – DOT – Automated License Plate Reader Anticipated Impact Report and draft Use Policy – review and take possible action.

The PAC began to discuss the Impact Assessment and Use Policy for the DOT ALPR program but time was limited so the item was tabled to a Special Meeting scheduled for Monday March 11th at 5pm.

8. 6:30pm: Surveillance Equipment Ordinance – OPD – Automated License Plate Reader Anticipated Impact Report and draft Use Policy – review and take possible action.

This item was tabled.

9. 6:50pm: Review of Old Business and take possible action
    a. City Attorney opinion re applicability of SB 1160 (BART jammer bill) to cell-site simulator use
    b. City Attorney opinion re applicability of SB 178 (CalECPA) to cell-site simulator use (PC 1546.2 notice provision)
    c. JTTF MOU review
    d. US Marshals, ATF, FBI – response to higher standards in joint task force operations MOU
    e. City Attorney opinion re PC 832.7 and SB 1421 (Skinner) in context of federal transparency task force ordinance annual report (potential violations)

These items were tabled.

10. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

March 11, 2019 5:00 PM
Oakland City Hall
Hearing Room 2
1 Frank H. Ogawa Plaza, 3rd Floor
Special Meeting Minutes

***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. 5:00pm: Call to Order, determination of quorum

Members present: Hofer, Jaquez, Katz, Oliver, Patterson

2. 5:05pm: Open Forum/Public Comment

There were no Speakers.

3. 5:10pm: Surveillance Equipment Ordinance – DOT – Automated License Plate Reader Anticipated Impact Report and draft Use Policy – review and take possible action.

Michael Ford with DOT was present and answered questions for the PAC. He clarified that the data retention period is only 24 hours, the system only shares "Scofflaw" parkers with OPD (these are cars with multiple unpaid tickets that require a boot) or cars that are known to be stolen. He noted the only outside agency data is shard with is also the scofflaw data which is shared with Berkeley.

The PAC voted unanimously to support the program and forward the Use Policy to the City Council.

4. 5:50pm: Surveillance Equipment Ordinance – OPD – Automated License Plate Reader Anticipated Impact Report and draft Use Policy – review and take possible action.

The PAC continued its deliberations on the OPD ALPR policy and touched on issues including compliance with new state law, performance metrics, system capabilities such as the ability to identify the make and model of a vehicle, and annual audits. The conversation was continued to the next PAC Meeting in April.

5. 6:45pm: 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

Numerous local and state government entities have researched and

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.

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

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) ~~as well~~ 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 ~~manually by~~ authorized personnel turn on their vehicle-based computer at the beginning of a police patrol shift. ~~in a police patrol vehicle~~. Once initiated, the system runs continuously and photographs vehicles ~~during~~ 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 ~~observed and~~ 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 system in vehicles uploads all photographs to the OPD maintained database when authorized personnel turn off the system~~. 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

[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.

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 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 analysists 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. 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, 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. 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. 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 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. ~~Firstly,~~ OPD does not affix ALPR cameras to fixed infrastructure. OPD deploys ALPR camera-affixed vehicles through every area of Oakland[3], 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. ~~Therefore, there is little possibility that vehicles travelling within certain neighborhoods, or by certain streets will more likely have their license plates recorded over an extended period of time~~. Additionally, ~~Lastly~~, 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.

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

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).

5. Mitigations

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).

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. 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[4]; and/or
6. Other Departmental need.

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

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 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

Commented [BS1]: Ongoing 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 ~~Currently spends~~ 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 [BS2]: 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[5]. The AICP report, "News Stories about Law Enforcement ALPR Successes September 2017 - September, 2018"[6] presents scores of cases from different national LEA jurisdictions where ALPR data helped lead to the capture of violent criminals. A July 2014 study[7] 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).

[5] https://www.theiacp.org/projects/automated-license-plate-recognition
[6] https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf
[7] https://www.rand.org/pubs/research_reports/RR467.html

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Gunshot Location Detection System

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:

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.

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) ~~GUNSHOT LOCATION DETECTION SYSTEM~~

Effective Date: ~~XX Apr 19~~
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

Anne E. Kirkpatrick
Chief of Police

Date Signed:

Surveillance Technology Assessment Questionnaire (STAQ) Overview

https://surveillancetech.atlassian.net/wiki/spaces/OAKLAND/pages/295042/Begin+a+New+Surveillance+Technology+Assessment

The primary purpose of this document is to create a framework for collecting the information necessary to make an informed recommendation regarding contemplated surveillance technology equipment and their use. In addition, this document is intended to instill consistency, objectivity, and transparency in the assessment process. It is expected that this framework will be augmented and improved with each evaluation of surveillance technology by the Privacy Advisory Commission (PAC).

Pursuant to the Surveillance Equipment Ordinance, a City entity or department seeking approval of such equipment acquisition or use shall complete this Surveillance Technology Assessment Questionnaire (STAQ), and incorporate the information into the required Surveillance Impact Report (SIR) pertaining to the acquisition or use. All categories may not be applicable to every technology.

STAQ Phase 1: Description, Purpose, and Capabilities

0. Initial Information

1. Name of Respondent:*
    a. First Name*
    b. Last Name*
2. Department/Agency:*
3. Role / Position:*
4. Office Phone Number:*
5. Official Email Address:*
6. Name of Technology:*
7. Regarding this technology, your department is in which stage of the procurement process?*
    a. Proposed Technology: Needs Identification
    b. Proposed Technology: Pre-Solicitation
    c. Proposed Technology: Solicitation / Bidding In-Progress
    d. Proposed Technology: Contract Awarded
    e. Existing Technology: Acquired / Contracted
    f. Existing Technology: Contract up for Renewal
8. Vendor (if known):
9. Manufacturer (if known):
10. Model/Version(s) (if known):
11. What are other names, acronyms, nicknames, or brand names for this technology?

12. Please provide a brief description (one paragraph) of the purpose and proposed use of the technology.* *This 1-3 sentence explanation should include the name of the technology/ program/ application/ equipment (hereinafter referred to as "technology"). It should also include a brief description of the technology and its function.*
13. Explain the reason the technology is being acquired, created or updated and why the SIR is required.* *This 1-3 sentence explanation should include the reasons that caused the project/technology to be identified as "surveillance technology" such as the project/technology collection of personal information, or that the project/technology meets the criteria for surveillance.*
14. Which of the following criteria apply to this technology?
    a. The technology disparately impacts disadvantaged groups.
    b. There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
    c. The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
    d. The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.
15. Please attach a brief diagram of the system showing its major components that collect, process, and store, and share information and how information would be transmitted between those components.* *File uploads may not work on some mobile devices.*

1. Description

1. What is the function of the technology as described by the vendor, manufacturer, or developer?* *Consult vendor materials or other reputable sources. Be specific about the type of surveillance functions (e.g., collection, processing, dissemination) and the type of data collected (e.g., biometric).*
2. What technology capabilities do you intend to use?*
    a. Data Collection
    b. Data Processing
    c. Data Storage
    d. Data Sharing
    e. Other:
3. Describe the data **collection** capabilities you intend to use.*
4. Describe the data **processing** capabilities you intend to use. *
5. Describe the data **storage** capabilities you intend to use. *
6. Describe the data **sharing** capabilities you intend to use.*
7. What other technology capabilities are possible that you don't intend to use? If unknown, please indicate as such.
    a. Data Collection
    b. Data Processing
    c. Data Storage
    d. Data Sharing
    e. Unknown
    f. Other:

8. Describe the other data **collection** capabilities possible (that you don't intend to use). *
9. Describe the other data **processing** capabilities possible (that you don't intend to use). *
10. Describe the other data **storage** capabilities possible (that you don't intend to use). *
11. Describe the other data **sharing** capabilities possible (that you don't intend to use). *
12. What safeguards will be implemented to ensure that unauthorized capabilities or uses will not be implemented?*
13. Who will be involved with the deployment and use of the technology?*
14. Will the technology be operated or used by another entity on behalf of the City?*
    a. Yes
    b. No
    c. Unknown
    d. Not Applicable
15. Provide details about access and applicable protocols by the other entities. Please link memorandums of agreement, contracts, etc. that are applicable.*
16. How and when will the project / technology be deployed or used? *
17. Who will determine when the project / technology is deployed and used?*
18. How often will the technology be in operation?*
19. Were non-surveillance alternatives considered? *
    a. Yes
    b. No
20. If no alternatives were considered, how might success be achieved by non-surveillance measures?*
21. Describe the non-surveillance alternatives considered and the reasons why the non-surveillance alternatives were not pursued.*

2. Purpose

1. Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed.
2. Describe how the use of the technology relates to the department's mission.*
3. What is the specific problem this equipment or use will resolve?*
4. Explain the department's argument for procuring the technology.
5. Describe the benefits of the technology. *
6. Provide any data or research demonstrating anticipated benefits. *
7. How will success be measured? Who will be better off? How will this be determined?* *Indicators of success should be SMART: Specific, Measurable, Attainable, Relevant, and Time-based. Example: "Success seen as X% reduction in shootings per month."*
8. What other communities have achieved success using this technology? If none, describe why this technology could achieve success.*
9. Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology. *List the Agency/Municipality, Name.; Primary Contact; Description of Current Use.*

3. Location

1. Where will the technology be deployed within the community? *
    a. All Oakland neighborhoods.
    b. Other:
2. For information processing systems, indicate which locations within the community will be included in the used information.
3. What is the process or criteria used to select the location(s)?*
4. Please provide any data or statistical evidence showing that the problem addressed by this technology exists at these specific locations.*
5. What are the racial demographics of those living in the area of use? *
6. Is the technology installed permanently, or temporarily? Is it installed on a structure or a mobile platform like a vehicle or person?*
    a. Permanent Installation on Immobile Structure
    b. Temporary Installation on Immobile Structure
    c. Permanent installation on Mobile Platform
    d. Temporary Installation on Mobile Platform
7. Is a physical object, collecting data or images, visible to the public?*
    a. Yes
    b. No
8. If applicable, what are the markings (visual / audible) to indicate that it is in use? * *Enter "NA" if not applicable.*
9. If applicable, what signage is used to determine department ownership and contact information?* *Enter "NA" if not applicable.*
10. Where will the information be stored?*
    a. Locally on the collecting device
    b. On a department computer, file server or other storage medium
    c. Remotely on a third-party server or cloud-based storage provider
    d. Not applicable as information will not be stored.
11. For remote or cloud storage, please list the service provider and contact information for the administrator of the remote storage.*

4. Data Sources

1. What specific legal authorities and/or agreements permit and define the collection or use of information by the technology?*
2. What information about individuals or groups can the technology collect and/or use? *
    a. Biographic or Identifying Data (Name, DOB, License Plate Number, Address, Race, Phone Number, etc.)
    b. Sensory (Audio, Visual, Olfactory, Thermal, Biometric, etc.)
    c. Electronic Signatures (Radio frequencies, cellphone signals, network activity)
    d. Location (GPS data, other geolocational data)
    e. Not Applicable
    f. Other:
3. List the biographic or identifying information collected or used by the technology.*

4. List the sensory information collected or used by the technology.*
5. List the electronic signature information collected or used by the technology.*
6. List the location information collected or used by the technology.*
7. What information about individuals or groups can the technology store or share? *
    a. Biographic or Identifying Data (Name, DOB, License Plate Number, Address, Race, Phone Number, etc.)
    b. Sensory (Audio, Visual, Olfactory, Thermal, Biometric, etc.)
    c. Electronic Signatures (Radio frequencies, cellphone signals, network activity)
    d. Location (GPS data, other geolocational data)
    e. Not Applicable
    f. Other:
8. List the biographic or identifying information stored or shared by the technology. *
9. List the sensory information stored or shared by the technology.*
10. List the electronic signature information stored or shared by the technology.*
11. List the location information stored or shared by the technology.*
12. Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.*
13. Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.*
14. How long will information be retained? * *Retention timelines may vary depending on data type.*
15. Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?*
16. How will the owner allow for departmental and other entities to audit for compliance with legal deletion requirements?*
17. What interaction will third parties (other governments, companies, NGOs, academics) have with the data?*
    a. The system will use data collected by a third party.
    b. The system's data will be shared with a third party.
    c. The system's data will be stored by a third party.
    d. There is no interaction with third-parties.
    e. Other:
18. Why will the system USE data collected by a third party? Will this be on an ongoing basis?*
19. Why will the system's data be SHARED with a third party? Will this be on an ongoing basis?*
20. Why will the system's data be STORED by a third party? Will this be on an ongoing basis?*

5. Data Security

1. Who is authorized to access the technology and data collected?*
2. How many users would be authorized?*
3. What criteria must users meet to be authorized?*
4. What are acceptable reasons for access to the system and/or data collected/generated?*

5. How does the system authenticate users, i.e. which security protocols are implemented (ex: multi-factor authentication, whitelisted IPs, firewall, https)?*
6. How will data be securely stored (ex: encrypted-at-rest on DVDs in a locked office)?*
7. How will data be securely transmitted/shared (ex: sent via secure FTP; hand-carried by trusted personnel)?*
8. What other safeguards are in place for protecting data from unauthorized access (encryption, access control mechanisms, physical locks, etc.)?*
9. What logging and auditing measures are in place to protect the technology and its data? *
10. What type of security audits are conducted?*
    a. The system automatically monitors / flags suspicious activity or data compromise.
    b. Department personnel conduct security audits of the system and its data.
    c. A third-party conducts a security audit of the system and its data.
    d. None of the above.
    e. Other:
11. Who has access to the audit data?*
12. Describe how the technology maintains a record of any disclosures outside of the department.*

Department should complete the next phase AFTER completing their OPAC Engagement (See Appendix 1.)

STAQ Phase 2: Impact and Mitigation Analysis

1. Impact

1. Please list any known or reported harms resulting from the use of this technology in this jurisdiction or others.* *Describe: Jurisdiction - Description of Harm - Source.*
2. Can the technology collect, process, or store information related to the following categories:
    a. Race
    b. Citizenship
    c. Status
    d. Gender
    e. Age
    f. Socio-Economic Level
    g. Sexual Orientation
3. **Given the specific data elements collected, do the following potential risks to privacy or perceived risks to privacy apply?** Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.
    a. Surveillance: Continuous monitoring and observation of a subject, sometimes without their awareness, including by other individuals, "Peeping Toms," parents, businesses, other governments.*
        i. If yes, provide details about how and why:*
    b. Identification: A subject becomes individually identifiable.*
        i. If yes, provide details about how and why:*
    c. Intrusion: Invasions or incursions into one's life, routines, or physical space, often making the subject feel uncomfortable or uneasy.*
        i. If yes, provide details about how and why:*
    d. Interrogation: Subjects are pressured to divulge information.*
        i. If yes, provide details about how and why:*
    e. Aggregation: Information or data about a subject is combined with different sources, telling a different story than the technology alone.*
        i. If yes, provide details about how and why:*
    f. Increased Accessibility: Information that once took some effort to find now takes less effort to find. Example: Physical records that could before only be viewed by physically searching for files are placed into a computer searchable database.*
        i. If yes, provide details about how and why:*
    g. Disclosure: Information or data about a subject is revealed to others.*
        i. If yes, provide details about how and why:*
    h. Secondary Use: Data is used for purposes unrelated to the purposes for which it was initially collected.*
        i. If yes, provide details about how and why:*
4. **Will use of the technology increase the likelihood that any person or group, (including people of color, non-citizens, low-income residents, people living**

with disabilities, or any group historically vulnerable to disproportionate civil-liberties violations) will suffer the following potential problems?

a. Exclusion: Subjects are excluded from systems, services, or spaces. Exclusion also describes when subjects are excluded from knowing what a system does (e.g. it collects or shares personal data without their knowledge or consent).*
    i. If yes, provide details about how and why: *
b. Appropriation: One's identity or personality is used for the purposes and goals other than the intended purpose.*
    i. If yes, provide details about how and why: *
c. Decisional Interference: The subject's ability to make decisions without interference from an outside actor is harmed.*
    i. If yes, provide details about how and why:*
d. Exposure: A subject is exposed to indecent material.*
    i. If yes, provide details about how and why:*
e. Breach of Confidentiality: A release of information about a subject betrays their trust in the technology user or department.*
    i. If yes, provide details about how and why:*
f. Loss of autonomy: Self-imposed restrictions on freedom of movement, expression or assembly (avoiding protest participation, for example).*
    i. If yes, provide details about how and why:*
g. Loss of liberty: Disproportionate exposure to arrest or detainment. Incomplete, inaccurate, improper use of information can lead to arrest.*
    i. If yes, provide details about how and why:*
h. Physical harm: The information could lead to actual physical harm to a person.*
    i. If yes, provide details about how and why:*
i. Stigmatization: Information is linked to an actual identity in such a way as to create a stigma that can cause embarrassment, emotional distress or discrimination.*
    i. If yes, provide details about how and why:*
j. Power Imbalance: Acquisition of personal information creates an inappropriate power imbalance, takes unfair advantage of or abuses a power imbalance between acquirer and the individual.*
    i. If yes, provide details about how and why:*
k. Identity Theft: The security of one's data comes into question. A subject's identity might be stolen; or false data about the subject may be created.*
    i. If yes, provide details about how and why:*
l. Blackmail: A blackmailer threatens to harm the subject or release information about the subject to coerce the subject to give into the blackmailer's demands.*
    i. If yes, provide details about how and why:*
m. Other harms?
    i. Provide details about how and why:

5. **Does the technology collect, use, or retain information about individuals in the following stages of criminal justice system?**
    a. Individuals not suspected of wrongdoing:*
        i. If yes, provide details about how and why:*
    b. Individuals suspected but not charged with an offense:*

        i. If yes, provide details about how and why:*
    c. Individuals charged with but not convicted of any offense:*
        i. If yes, provide details about how and why: *
    d. Individuals convicted of previous offenses but not currently incarcerated:*
        i. If yes, provide details about how and why: *
    e. Individuals convicted of previous offenses and currently incarcerated:*
        i. If yes, provide details about how and why: *
6. What racial equity opportunity area(s) may be affected by the application of the technology?
    a. Education
    b. Community Development
    c. Health
    d. Environment
    e. Criminal Justice
    f. Jobs
    g. Housing
    h. Other:
7. **Could the technology be used to collect, use, or retain information regarding groups, public gatherings, crowds, or their use of associated spaces (houses of worship, polling places, etc.) and impact the following civil liberties?**
    a. Rallies, protests, or other mass public gatherings:*
        i. If yes, provide details about how and why: *
    b. Religious practices:*
        i. If yes, provide details about how and why: *
    c. Union and organized labor activities:*
        i. If yes, provide details about how and why: *
    d. Voting, campaigning, or political advocacy activities:*
        i. If yes, provide details about how and why: *

2. Mitigations

1. What does your department define as the most important racially equitable community outcomes related to the implementation of this technology?*
2. **(Based on previous answers)** What safeguards are in place to limit the collection, processing, storage, or sharing of the following...
    a. Race - Safeguards:*
    b. Citizenship Status - Safeguards:*
    c. Gender - Safeguards:*
    d. Age - Safeguards:*
    e. Socio-Economic Level - Safeguards: *
    f. Sexual Orientation - Safeguards: *
3. What strategies may address the impacts (including unintended consequences) on racial equity? *

4. **(Based on previous answers)** What strategies may address immediate privacy risks identified above...
    a. Strategies to address Surveillance:* *Continuous monitoring and observation of a subject, sometimes without their awareness, including by other individuals, "Peeping Toms," parents, businesses, other governments.*
    b. Strategies to address Identification:* *A subject becomes individually identifiable.*
    c. Strategies to address Intrusion:* *Invasions or incursions into one's life, routines, or physical space, often making the subject feel uncomfortable or uneasy.*
    d. Strategies to address Interrogation:* *Subjects are pressured to divulge information.*
    e. Strategies to address Aggregation:* *Information or data about a subject is combined with different sources, telling a different story than the technology alone.*
    f. Strategies to address Increased Accessibility:* *Information that once took some effort to find now takes less effort to find. Example: Physical records that could before only be viewed by physically searching for files are placed into a computer searchable database.*
    g. Strategies to address Disclosure:* *Information or data about a subject is revealed to others.*
    h. Strategies to address Secondary Use:* *Data is used for purposes unrelated to the purposes for which it was initially collected.*
    i. Strategies to address Exclusion:* *Subjects are excluded from systems, services, or spaces. Exclusion also describes when subjects are excluded from knowing what a system does (e.g. it collects or shares personal data without their knowledge or consent).*
    j. Strategies to address Appropriation:* *One's identity or personality is used for the purposes and goals other than the intended purpose.*
    k. Strategies to address Decisional Interference:* *The subject's ability to make decisions without interference from an outside actor is harmed.*
    l. Strategies to address Exposure:* *A subject is exposed to indecent material.*
    m. Strategies to address Breach of Confidentiality:* *A release of information about a subject betrays their trust in the technology user or department.*
    n. Strategies to address Loss of Autonomy:* *Self-imposed restrictions on freedom of movement, expression or assembly (avoiding protest participation, for example).*
    o. Strategies to address Loss of Liberty:* *Disproportionate exposure to arrest or detainment. Incomplete, inaccurate, improper use of information can lead to arrest.*
    p. Strategies to address Physical Harm:* *The information could lead to actual physical harm to a person.*

q. Strategies to address Stigmatization:* *Information is linked to an actual identity in such a way as to create a stigma that can cause embarrassment, emotional distress or discrimination.*

r. Strategies to address Power Imbalance:* *Acquisition of personal information creates an inappropriate power imbalance, takes unfair advantage of or abuses a power imbalance between acquirer and the individual.*

s. Strategies to address Identity Theft:* *The security of one's data comes into question. A subject's identity might be stolen; or false data about the subject may be created.*

t. Strategies to address Blackmail:* *A blackmailer threatens to harm the subject or release information about the subject to coerce the subject to give into the blackmailer's demands.*

Program Strategies:

5. What measures are in place to minimize inadvertent or improper collection of data?*
6. What measures will be used to destroy improperly collected data?*
7. Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.*
8. Are there any restrictions on non-City data use?*
    a. Yes - If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.
    b. No
9. How does the department review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Oakland and outside agencies?*
10. Please describe the process for reviewing and updating data sharing agreements.

Policy Strategies:

11. List the legal standards or conditions, if any, that must be met before the technology is used.* *For example, the purposes of a criminal investigation are supported by reasonable suspicion.*

12. Describe the processes that are required prior to each use, or access to/ the technology, such as a notification, or check-in, check-out of equipment.*

13. Describe existing policies to be followed by personnel operating the technology, and who has access to ensure compliance with use and management policies. * *Include links to all policies referenced.*

14. Describe the training required of all personnel operating the technology, and who has access to ensure compliance with use and management policies.* *Include links to training documents. If none are available, outline of what the training covers and indicate who provides the training.*

15. Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.* *For example, police department responses may include references to the Oakland Police Manual.*

Partnership Strategies:

16. How will you partner with stakeholders to mitigate the negative impacts? *

STAQ Phase 3: Equity and Fiscal Cost Analysis

1. Equity Analysis

1. What does data and conversations with stakeholders tell you about existing racial inequities that influence people's lives and should be taken into consideration when applying/implementing/using the technology? *
2. What are the root causes or factors creating these racial inequities?* *Examples: bias in process; lack of access or barriers; lack of racially inclusive engagement.*
3. How will the technology, or use of the technology increase or decrease racial equity? *
4. What benefits to the impacted community/demographic may result?*
5. What are potential unintended consequences (both negative and positive potential impact)?*
6. Are the impacts aligned with your department's community outcomes that were defined in Phase 2?*
    a. Yes
    b. No
7. If impacts are not aligned with desired community outcomes for surveillance technology, how will you re-align your work?*
8. How will you partner with stakeholders for long-term positive change? *

2. Fiscal Cost Analysis

1. Are you providing actual current costs or estimating future potential costs?*
    a. Actual current costs
    b. Future potential costs
2. What are the initial costs, including acquisition, infrastructure upgrades, licensing, software, training, and hiring of personnel?*
3. What are the ongoing operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security?*
4. What are potential cost savings through use of the technology?*
5. What are the current or potential funding sources for the proposed acquisition or use?* *Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities.*
6. What other tools capable of furthering the identified purpose may the community wish to spend these funds on (e.g., community-based policing, improved lighting)?*
7. To achieve success, what other tools would be considered for future procurement in addition to this technology?*

References

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology. *Please provide Title, Publication, Link.*

Please list any experts of the technology under consideration, or of the technical completion of the service or function for which the technology is responsible.
Please provide Name, Position/Role, Affiliation, Contact Information.

Thank you for completing the STAQ!

Appendix 1. OPAC/Public Engagement.

OPAC Presentation

Date of presentation:

Summary of comments:

Complete meeting minutes and comments are attached as an appendix to the SIR.

Any letters of feedback by OPAC members are attached as an appendix to the SIR.

Create a public outreach plan. Residents, community leaders, and the public were informed of the public meeting and feedback options via:

- ☐ Email
- ☐ Mailings
- ☐ Fliers
- ☐ Phone calls
- ☐ Social media
- ☐ Other

If other, explain:

Appendix 2. Community Engagement.

How have you involved stakeholders since the implementation/application of the technology began?

☐ Public Meeting(s)

☐ OPAC Presentation

☐ Other external communications

Please provide details:

☐ Stakeholders have not been involved since the implementation/application

What is unresolved? What resources/partnerships do you still need to in order to make changes?

The following community leaders were identified and invited to the public meeting(s):

☐ American Civil Liberties Union (ACLU)

☐ Electronic Frontier Foundation (EFF)

☐ National Association for the Advancement of Colored People (NAACP)

☐ Asian Law Caucus

☐ Council on American-Islamic Relations (CAIR)

☐ Others:

Public Comment Engagement (for each meeting)

Date of meeting:

Location of meeting:

Summary of discussion:

Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

Collect public feedback via mail and email

Number of feedback submissions received:

Summary of feedback:

Open comment period:

Complete compilation of feedback is attached an as an appendix to the SIR