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 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 February 7 meeting minutes

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

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.

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

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

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

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)

10. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

February 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**: Saied R. Karamooz, **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, Katz, Patterson, Jaquez, Karamooz.

2. 5:05pm: Review and approval of January 3 meeting minutes

The minutes were approved unanimously.

3. 5:10pm: Open Forum

There were no Open Forum Speakers.

4. 5:15pm: UC Berkeley's Samuelson Law, Technology & Public Policy Clinic – introduction and discussion of scope of work, including drafting of Privacy Principles.

Member Patterson introduced the group who will be launching an effort to develop a set of privacy principals for the City of Oakland to include in its creation of an overarching privacy policy. The principals will touch on data collection, use, storage, and third party access. The goal is to develop principals that are modeled after other jurisdictions but unique to Oakland. They will be interviewing key stakeholders over the month and bringing a draft back to the PAC in April.

5. 5:20pm: Surveillance Equipment Ordinance – OPD – Exigent Use of Surveillance Technology report, and take possible action.

Bruce Stoffmacher presented the report and it was approved unanimously. He also noted that due to the sudden consistent use of the Sherriff's Department's UAV (drone), staff will be bringing a formal policy to the PAC in the spring.

6. 5:30pm: Surveillance Equipment Ordinance – OPD – Automated License Plate Reader Anticipated Impact Report – review and take possible action.

The PAC reviewed the updated Impact Report and asked several questions regarding camera angles, data retention, and specifics on purpose and mitigations. The suggestion was made to bring the Impact Statement back along with the proposed Use Policy so they could be reviewed together. They will come back in March.

7. 6:00pm: Federal Task Force Transparency Ordinance – OPD – presentation of inaugural annual reports (FBI/JTTF, ATF, DEA task forces), and take possible action.

Six public speakers gave input on this item expressing both optimism that the PAC will be receiving these annual reports but also disappointment about the lack of information the first drafts contain. The fact that some information was not shared without the City submitting a Freedom of Information Act (FOIA) Request was of concern. Also, citing 832.7 as a reason to not share information was also questioned.

The PAC unanimously sent the draft reports back asking staff to get more information (from the federal agencies and internally) > The PAC also asked for a legal opinion about 832.7 and whether that was a valid reason to not disclose information.

8. 6:30pm: Surveillance Equipment Ordinance – OPD – Body Worn Camera Anticipated Impact Report – review and take possible action.

Similar to Item 6, the Impact Statement and Use Policy will be brought back together in March.

9. 7:00pm: Adjournment

The meeting adjourned at 7:05.

City of Oakland Privacy Principles
Preliminary Draft: March 4, 2019

Oakland is a diverse city with a history of active civic participation on issues of privacy and surveillance. As we evolve, it is imperative that we learn from both the positive and negative aspects of our past to build our future. Progress at the expense of personal privacy and safety is unacceptable. We recognize the need to protect Oaklanders' privacy as municipal services incorporate emerging technologies.

Privacy is both a fundamental human right and instrumental to Oaklanders' safety, health, security, and access to essential services. We seek to safeguard the privacy of every Oakland resident in order to promote fairness and protect civil liberties across all of Oakland's diverse communities.

Therefore, when we seek personal information from Oakland residents to provide essential services and protect our communities, we pledge to handle this information in a manner that builds trust and preserves Oaklanders' privacy and safety. The following Privacy Principles guide our actions.

DESIGN AND USE EQUITABLE PRIVACY PRACTICES

Community safety and access to essential services should not come at the expense of any Oaklander's right to privacy. We recognize that our collection and use of personal information has disadvantaged Oakland communities at different periods throughout Oakland's history. We aim to avert future inequities by collecting information in ways that do not discriminate against any Oaklander or Oakland community. When possible, we will offer clearly communicated alternatives to the collection of personal information at the time of collection.

LIMIT COLLECTION AND RETENTION OF PERSONAL INFORMATION

We believe that we should collect and store personal information only when and for as long as is justified to protect Oaklanders' safety, health, security, and access to essential services. We will continue our practice of reaching out to Oaklanders for their views on the information we collect and how we use it. We also will look for new opportunities for outreach.

BE TRANSPARENT AND OPEN

Oaklanders' right to privacy is furthered by the ability to access and understand explanations of why and how we collect, use, manage, and share personal information. To that end, we aim to communicate these explanations to Oakland communities in plain, accessible language. We also aim to communicate this information at a time when it is relevant and useful.

MANAGE PERSONAL INFORMATION WITH DILIGENCE

The personal information of Oaklanders should be treated with respect. We handle all personal information in our custody with care, regardless of how or by whom it was collected. To maintain the security of our systems, we review and regularly update software and applications that interact with Oaklanders' personal information. Further, we recognize that deletion, encryption, minimization, and anonymization can prevent misuse of personal information. We aim to make effective use of these tools and practices. Additionally, we combine personal information gathered from different departments only when we must.

SAFEGUARD INDIVIDUAL PRIVACY IN PUBLIC RECORD DISCLOSURES

Open government and respect for privacy go hand-in-hand. Providing relevant information to interested parties about our services and governance is essential to democratic participation and civic engagement. However, we will protect Oaklanders' privacy and security interests when we comply with public records requests.

EXTEND PRIVACY PROTECTIONS TO OUR RELATIONSHIPS WITH THIRD PARTIES

Our responsibility to protect Oaklanders' privacy extends to our work with vendors and partners. Accordingly, we share personal information with third parties only when necessary to provide municipal services, and only when doing so is consistent with these Principles. We will disclose the identity of parties with which we share personal information.

BE ACCOUNTABLE TO OAKLANDERS

Trust in our stewardship of personal information requires both that we collect and manage personal information appropriately, and that we create opportunities for public engagement. We publicly review and discuss departmental requests to acquire and use technology that can be used for surveillance purposes. We encourage Oaklanders to share their concerns and views about any system that collects and uses their personal information, or has the potential to do so. We also encourage their views on our compliance with these Principles.

OPD - Federal Bureau of Investigation (FBI)
Joint Terrorism Taskforce (JTTF) 2018 Annual Report

Staffing

1. **Number of full and part time OPD officers assigned to JTTF:** One officer.
2. **Number of hours worked as JTTF officer**: Regular 40 hours per week. However, the current task force officer is often assigned to other OPD operations based on OPD needs and priorities and whether or not there is any active counter-terrorism investigation.
3. **Funding source for OPD JTTF officer salary**: Regular OPD general personnel funding.

Other Resources Provided

1. **Communication equipment:** City of Oakland Cellular Telephone
2. **Surveillance equipment:** None
3. **Clerical/administrative staff hours:** None
4. **Funding sources for all the above:** Regular OPD general equipment funding.

Cases

1. **Number of cases OPD JTTF officer was assigned to:** none
2. **Number of "duty to warn" cases:** none
3. **General types of cases:** counter-terrorism
4. **Number of times the FBI asked OPD to perform/OPD declined to perform:** None – the FBI knows that OPD task force officers must comply with all Oakland laws and policies. Furthermore, the FBI commonly works with different jurisdictions and understands that taskforces must collaborate with the particular polices and laws of those jurisdictions.
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of Assessments opened:** none
2. **Number of Voluntary Interviews opened:** The FBI cannot disclose this information; a Freedom of Information Act (FOIA) request would have to be made and the information would be redacted before release.
3. **Number of Assessments closed without becoming preliminary or full investigations:** Same answer as above.
4. **Number of Voluntary Interviews closed without becoming preliminary or full investigations:** Same answer as above.
5. **Number of times use of undercover officers were approved** Same answer as above.
6. **Number of instances where OPD JTTF officer managed informants:** Same answer as above.
7. **Number of cases involving informants that OPD JTTF officer worked on:** Same answer as above.
8. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:**

   a. **Number of such requests that were denied:** Same answer as above.
   b. **Reason for denial:** Same answer as above.
9. **Whether OPD JTTF officer was involved in any cases where USPER (U.S. person status) information was collected:** Same answer as above.
10. **Number of cases:** Same answer as above.

Training and Compliance

1. **Description of training given to OPD JTTF officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the JTTF follows all OPD policies and has received several police trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the JTTF MOU.
2. **Date of last training update, and last training audit:** October 2018
3. **Frequency with which OPD JTTF officer briefs OPD supervisor on cases:** Weekly and daily if and when a critical incident occurs.

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** Release of any of this information would violate California law (832.7), as there is only one OPD officer per task force.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD polices. OPD leadership consult with the Office of the City Attorney to ensure that all polices conform with State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney and the Privacy Advisory Commission to ensure that personnel continue to follow federal, state, and local laws and policies.

SARs and NCRIC

1. **Whether OPD JTTF officer submits SARs to NCRIC:** zero submitted
2. **Whether OPD officer receives SAR information:** zero received

Command Structure for OPD JTTF Officer

1. **Reports to whom at FBI?** Counterterrorism Assistant Agent in Charge
2. **Reports to whom at OPD?** Sergeant Omar Daza-Quiroz in OPD Intelligence Unit

OPD – United States Marshals Service (USMS)
2018 Privacy Advisory Commission Annual Report

Staffing

1. **Number of full and part time OPD officers assigned to ATF Taskforce:** One officer.
2. **Number of hours worked as ATF Taskforce Officer**: Regular 40 hours per week. However, the OPD officer sometimes is ask to assist with OPD operations. The work assignment of this officer is based on OPD needs and priorities and whether or not there active investigations.
3. **Funding source for ATF Taskforce Officer salary**: City of Oakland and USMS ($17,200 in overtime, reimbursement), and USMS vehicle.

Other Resources Provided

1. **Communication equipment:** OPD and USMS radios.
2. **Surveillance equipment:** USMS-funded vehicle
3. **Clerical/administrative staff hours:** none
4. **Funding sources for all the above:** City of Oakland General Purpose Fund and USMS funds.

Cases

1. **Number of cases ATF Taskforce Officer was assigned to:** 50.
2. **Number of "duty to warn" cases:** none
3. **General types of cases:** Local, state, and federal criminal arrest warrants.
4. **Number of times ATF asked OPD to perform/OPD declined to perform:** None
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of Assessments opened:** 65; The USMS Fugitive Task Force located in Oakland, arrested 310 local, state, and federal fugitives in 2018, of those, 39 were for homicide. In addition, the task force seized 66 firearms, 4,500 rounds of ammunition, $200K in cash, and 94 kilograms of various illegal drugs.
2. **Number of Voluntary Interviews opened:** n/a
3. **Number of Assessments closed without becoming preliminary or full investigations:** n/a
4. **Number of Voluntary Interviews closed without becoming preliminary or full investigations:** n/a
5. **Number of times use of undercover officers were approved:** None.
6. **Number of instances where OPD Taskforce officer managed informants:** None.
7. **Number of cases involving informants that ATF Taskforce Officer worked on:** None.
8. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD**
   a. **Number of such requests that were denied:** None.
   b. **Reason for denial:** None.

9. **Whether ATF Taskforce Officer was involved in any cases where USPER (U.S. person status) information was collected:** None.

Training and Compliance

1. **Description of training given to ATF Taskforce Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the USMS Fugitive Task Force follows all OPD policies and procedures, and has received several police trainings, including, but not limited to, continual professional training, procedural justice training, and annual firearms training. The officer has also reviewed all provisions of the USMS Task Force MOU, and operating procedures. If there is a conflict between OPD and USMS policies, the OPD officer is instructed to bring the issue to the attention of the USMS Task Force Commander. If the issue cannot be resolved, the officer will follow OPD policy.
2. **Date of last training update, and last training audit:** August 2018.
3. **Frequency with which ATF Taskforce Officer briefs OPD supervisor on cases:** Weekly.

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officers follow OPD polices. OPD leadership consult with the Office of the City Attorney to ensure that all polices conform with State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney and the Privacy Advisory Commission to ensure that personnel continue to follow federal, state, and local laws and policies.

SARs and NCRIC

1. **Whether OPD Taskforce Officer submits SARs to NCRIC:** None.
2. **Whether OPD officer receives SAR information:** None.

Command Structure for OPD Taskforce Officer

1. **Reports to whom at ATF?** Supervising Deputy U.S. Marshal Mike McCloud**.**
2. **Reports to whom at OPD?** Sergeant Muniz and Lieutenant James Beere.

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 ALRP technology.

10. Track Record of Other Entities

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[3]. The AICP report, "News Stories about Law Enforcement ALPR Successes September 2017 - September, 2018"[4] presents scores of cases from different national LEA jurisdictions where ALPR data helped lead to the capture of violent criminals. A July 2014 study[5] 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.

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

DRAFT

PROPOSED USE POLICY FOR VEHICLE-MOUNTED AUTOMATED LICENSE PLATE RECOGNITION (ALPR) FOR PARKING MANAGEMENT AND ENFORCEMENT

Michael P. Ford, Ph.D.
Parking and Mobility Division
Department of Transportation
City of Oakland
March 1, 2019

1. Purpose

Vehicle-mounted Automated License Plate Recognition (ALPR) technology shall be used to automate the processing of vehicle license plate information by transforming images into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information.

City of Oakland Department of Transportation (DOT) staff proposes to use ALPR for parking management and enforcement purposes.

2. Authorized Use

Authorized uses of ALPR technology include:

- ALPR-assisted citation issuance (i.e., a "hit");
- "Hotlist" identification, including scofflaw and stolen vehicles (so a "hit" also includes vehicles found to be on such lists, which may result in the issue of a citation and or other legal consequences such as booting or towing);[1]
- "Virtual chalk," automating the time-stamping of vehicles in time-limited parking spaces and areas (i.e., a "read" as opposed to a "hit");
- "Digital permits," including annual, weekly, and other limited-duration permits in parking privilege permit areas, e.g., Residential Permit Parking (RPP) areas and City-owned or managed parking facilities (i.e., valid permits result in "reads," which permits identified by the system as expired may result in a citation and thus a "hit");
- Parking payment verification, including "pay-by-phone" and "pay-by-plate" systems (again, with the possibility of both "reads" and "hits");
- Parking demand management, including parking occupancy and turn-over counts and analysis (requiring only meta data to determine counts and length of stay);
- Support for "smart parking" applications, including mobile apps providing parking availability and wayfinding information.

[1] Vehicles with five or more outstanding citations at least 30 days old.

All other uses not referenced above shall be prohibited.

3. Data Collection

DOT is responsible for ensuring proper collection and retention of ALPR data, in accordance with this policy and applicable laws. DOT staff drive Parking Enforcement vehicles with vehicle-mounted ALPR that capture still images and metadata indiscriminately as the vehicle moves through the right-of-way. Data collected include still images (e.g., of license plates, street signs, wheel position) and meta data (e.g., date, time and geolocation).

Images of vehicle license plates are processed using optical character recognition[2], time and geo-stamped, and analyzed in real time with the aim of registering potential violations and matching license plates against "hotlists" (as described above). Data is stored on servers secured and administered by the City's third-party Parking Citation system vendor, Conduent.

4. Data Access

Authorized staff may be from the City's Department of Transportation (DOT), Finance Management Bureau (FMB), Oakland Police Department (OPD) or other departments that contribute to the City's parking operations. Procurement and administration of ALPR contracts and systems is the responsibility of the City's Revenue and Tax Administrator in the Revenue Division of the Finance Management Bureau.

Metadata and still images may be downloaded and released to a third party as required by law. DOT is responsible for reviewing and retaining all requests for ALPR data or images in accordance with the City's Records Retention Policy and approving only those requests that have an official City purpose to obtain the information.

5. Data Protection

City staff depends on its vendor, Conduent, to source and administer its ALPR solution. As such, the City is relying on the safeguards to protect ALPR information from unauthorized access through the use of appropriate control mechanisms as provided by Conduent, e.g., user access to and use of the system is controlled and recorded for audit purposes.

The ALPR system shall be operated only by DOT personnel who have been trained in its operation, including Parking Control Technicians, Parking Enforcement Supervisors and Managers, Program Analysts and Transportation Planners.

Copies of metadata or still images released to an Investigating Officer for law enforcement activities shall be handled by the Investigating Officer pursuant to the Police Department's General Orders and the California Evidence Code.

[2] Optical character recognition (also optical character reader, OCR) is electronic conversion of images of text.

6. Data Retention

All ALPR data and images downloaded to City servers that are associated with citations (i.e., "hits") shall be retained for a minimum of 90 days pursuant to California Government Code 34090.7 and maximum of 5 years[3] in accordance with the City's Records Management Policy[4]. **I**n addition, DOT has incorporated the following into Conduent's scope of services:

- Archive or Purge citation data on an agreed upon schedule or as directed by City Staff.
- Archived data should remain accessible to online inquiry and retrieval as needed.
- Provide method for access for archived data, as well as disaster and recovery plans.
- Provide electronic images of citations issued on demand.
- Transfer data in format determined by City Staff as needed.
- Retain all payment documentation for 7 years.

The reason for these requirements is that they meet the City's minimum needs for administering the parking citation administrative process.

The same requirements do not apply to images and meta data from "reads". Only anonymous meta data will be retains for parking management purposes. All images and identifying information from "reads" will be automatically purged from the system after 24 hours.

7. Public Access

Except where prohibited or limited by law, the public may access ALPR data through public records requests. Again, the available information would depend on whether or not data was associated with a simple "read" (no related citation issued) or a "hit" (related citation issued).

8. Third-Party Data-Sharing

The City depends on Conduent and other third-party vendors for a comprehensive parking citation system, e.g., the Conduent system will build a "hot list" of vehicles subject to scofflaw and share this information with Paylock, a vendor contracted with the City since 2009 to provide a "smart parking boot" solution.

Parking occupancy information originating from the ALPR technology may be shared with and used by third-parties for smart parking applications. In such cases, license plate and other identifiable forms of data would be purged, resulting in only anonymous "counts" or "turn-over" indicators with time and geo-spatial information.

[3] Fiscal year +5 or calendar year +5 depending on type of record.

[4] "Establishing a City-Wide Records Management Program", Ordinance No. 11370 C.M.S.

9. Training

Training for operating ALPR will be provided by the Conduent and will be limited to authorized City staff. Staff will direct Conduent to incorporate this use policy and related privacy policies and procedures into its training materials.

10. Auditing and Oversight

City staff depends on Conduent to provide a “fully auditable” ALPR solution. For example, with the Conduent system staff expect transactions to be recorded in audit logs that capture the user ID of persons performing transactions, including the date, time and description of the functions performed. General oversight of the system falls to the City’s contract manager, currently the Tax and Revenue Administrator. DOT oversight and responsibility for the ALPR solution will fall to the Parking and Mobility Division Manager. The legally enforceable sanctions for violations of the policy include relevant administrative instructions as well as provisions in the Surveillance and Community Safety Ordinance .

DOT will make available to the public, in an Annual Surveillance Report pursuant to Chapter 9.64 of the Oakland Municipal Code, a description of how the technology was used, including the type and quantity of data gathered or analyzed by the technology; whether and how often data acquired through the technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosure(s); and other information required per Section 9.64.010 of that Ordinance.

11. Maintenance

The City’s third-party vendor, Conduent, will be required to maintain the integrity of the Parking Citation system in general and the ALPR solution in particular. Details of the mechanisms and procedures are included in the City’s contract.

Questions or comments concerning this draft Use Policy should be directed to Michael Ford, Manager, Parking and Mobility Division, via email at mford@oaklandca.gov or phone at (510) 238-7670.

DRAFT

Anticipated Impact Report for
Vehicle-Mounted Automated License Plate Recognition (ALPR)
for Parking Management and Enforcement

Michael P. Ford, Ph.D.
Parking and Mobility Division
Department of Transportation
City of Oakland
March 1, 2019

1. Information Describing Vehicle-Mounted Automated License Plate Recognition (ALPR) and How It Works

Vehicle-mounted Automated License Plate Recognition (ALPR**)** technology automates the processing of vehicle license plate and compliance information. Specifically, ALPR:

- uses specially-designed cameras mounted on parking enforcement vehicles to capture digital images from surrounding vehicles as they drive through the streets;
- transforms the images into alphanumeric characters with optical character recognition (OCR) software;
- stores the images, plate information, and related metadata in a restricted-access database;
- compares the transformed license plate characters to databases of license plates of interest to operators;
- archives photo evidence and metadata in support of citations issued ("hits") according to evidence retention standards consistent with City and State law; and
- archives anonymous information about parking usages (e.g., number of vehicles present on a given street at a given time and date) to support parking management decision-making ("reads").

[To do: add example images captured by ALPR, both parked and driving, as well as images of the user interface]

2. Proposed Purpose

City of Oakland Department of Transportation (DOT) proposes to use ALPR for parking management and enforcement purposes. Parking management includes occupancy and vehicle turnover information, and parking enforcement includes identification of possible violations and evidence in support of citations issued. ALPR would be integrated with a comprehensive Parking Citation solution that includes backend server processes, intersystem communication and various user interfaces ranging from authorized staff to public self-serve applications (e.g., a browser-based citation review and payment application that allows parkers to review photo evidence that may or may not have been gathered by the ALPR system).

Specific DOT uses of ALPR technology would include:

- "Virtual chalk," automating the time-stamping of vehicles in time-limited parking spaces and areas;
- "Digital permits," including annual, weekly, and other limited-duration permits in parking privilege permit areas, e.g., Residential Permit Parking (RPP) areas; City-owned or enforced parking facilities;
- Parking payment verification, including "pay-by-phone" and "pay-by-plate," on-street and off-street;
- "Hotlist" identification, including scofflaw and stolen vehicles;[1]
- Parking demand management, including parking occupancy and turn-over counts and analysis; and
- Supporting "smart parking" applications with occupancy information, including mobile apps providing parking availability and wayfinding information.

When ALPR systems are deployed for these purposes, they would be mounted on City-owned Parking Enforcement vehicles operated by Parking Control Technicians trained in proper ALPR operation. Currently, DOT is proposing to operate five ALPR systems with additional vehicles equipped in the future.

3. Locations Where ALPR May Be Deployed

ALPR equipped Parking Enforcement vehicles will be deployed throughout the City, while focusing on commercial districts and neighborhoods with Resident Permit Parking (RPP) areas.

4. Potential Impact on Civil Liberties & Privacy

DOT recognizes that all people have an inalienable right to privacy and are committed to protecting and safeguarding this right, and that ALPR could raise concerns regarding real and/or perceived threats to civil liberties and privacy.

ALPR collects information from license plates of vehicles parked in public places and DOT is not proposing to track movement of individuals. However, DOT understands that the public may be concerned that the collection and analysis of this information over time could potentially be used to generate a detailed profile of an individual's movement or abused for other inappropriate purposes.

Specifically, the Department recognizes following actual or potential public concerns:

- **Identity capture.** The public may be concerned that ALPR will capture personally identifiable information (PII) without notice or consent. Although ALPR does not independently generate information that identifies vehicle occupants, license plate information can be used to determine the registered owner. In addition, vehicle

[1] Vehicles with five or more outstanding citations at least 30 days old.

occupants or immediate surroundings (including addresses) may be pictured. As a result, it is possible that individuals with access to this data could do additional research to identify the individual.

- **Misidentification.** The public may be concerned that, if ALPR data is widely accessible and inaccurate, individuals may be misidentified as the person driving a vehicle that is violation parking rules or is a scofflaw or stolen vehicle. This could lead to improper government actions against such individuals.
- **Activity monitoring.** The public may be concerned that ALPR data will enable individuals' behaviors to be revealed to and/or monitored by DOT or other government agencies, their partners or affiliates, companies interested in targeted marketing, and/or the public. Such concerns may include basic information about when individuals are in certain locations, as well as concerns about what government or individuals may infer from this data (i.e. marital fidelity, religious observance, or political activity). Although ALPR data is gathered from public places, this could conflict with an individual's expectation of locational privacy.

5. Mitigations

DOT will take certain steps to mitigate such privacy concerns:

- DOT will tailor access and retention policies to the two categories of information collected:
    - 1) **Reads,** which are images of license plates on vehicles that are not violating parking requirements and are not stolen or scofflaw vehicles; and
    - 2) **Hits,** which are images of license plates on vehicles that are violating parking requirements or are stolen or scofflaw vehicles.
- DOT will use ALPR to support compliance with parking regulations and parking management initiatives, and will not share ALPR data with the Police Department, DMV, Law Enforcement Agencies, other cities jurisdictions, except when such data is used as evidence in support of parking violations ("hits");
- DOT will use ALPR technology according to the proposed ALPR for Parking Management and Enforcement Use Policy as well as all applicable laws, policies and administrative instructions;
- DOT has no plans or intentions of using or deploying the ALPR technology in a manner that is discriminatory, viewpoint-based, or biased via algorithm;
- DOT will conduct annual audits of ALPR data to ensure a reasonable standard of data accuracy and to verify that system operators and administrators are following use policies;
- DOT will keep the public informed about planned and actual ALPR usage, as well as changes that would significantly affect privacy, civil rights, or civil liberties.

To specifically mitigate the potential or feared impacts enumerated in Section 4 of this Anticipated Impact Report, DOT or vendors acting on its behalf will also take the following actions:

- **Identity capture and/or activity monitoring.**
    - ALPRs will not collect any additional information compared to information that is or could be captured manually by DOT Parking Control Technicians;
    - DOT will aim ALPR cameras downward towards the street, to the extent possible, to avoid capturing the faces of vehicle occupants or identifiable details or immediate surroundings;
    - Where PII, such as faces and house numbers, is captured in still images that are retained by DOT or those acting on its behalf, that data will be obfuscated or cropped through technical means such that it is no longer identifiable or reasonably re-identifiable. PII collected by ALPRs that cannot be technically obfuscated will be used solely for the purpose(s) specified in the City's citation notice.
- **Misidentification.**
    - DOT will restrict ALPR data access to registered users, who will be properly trained and will access the ALPR database through a password-protected system;
    - DOT will conduct annual audits of ALPR data to ensure a reasonable standard of data accuracy and to verify that operators and administrators are following use policies;
    - DOT will offer a mechanism for individuals who believe that their vehicle has been mistakenly identified to contest the information.
- **Activity monitoring.**
    - DOT will not retain ALPR data beyond specified time periods.
    - DOT will only use trained and registered uses-users to access ALPR data.
    - ALPR use will be limited to parking management and enforcement purposes.
    - Still images and metadata may potentially be shared with the following:
        - the public, to enable online search and payment of parking citations-by citation number, not by license number when applicable;
        - third-parties involved in City parking management and enforcement, including Conduent (parking citation issuance and processing solution), Paylock (ALPR scofflaw boot solution), Parkmobile (meter pay-by-phone), IPS (single-head and multi-space smart meters), and Scheidt & Bachmann (off-street parking and access control system); and
        - Outside of these planned distributions, DOT will take steps to ensure that systems and data will not be disseminated outside of DOT unless dissemination is required by law, or fulfills an authorized purpose and complies with the DOT's ALPR use policy.
    - Per DOT's ALPR Use Policy, DOT will make an Annual Surveillance Report describing how the technology was used.

6. Data Types and Sources

ALPR technologies are designed to capture still images of vehicles and vehicle details including:

- License plate information, including state and number;
- Wheel positions; and
- Vehicle make, model, color, and type.[2]

ALPR technologies are also designed to capture metadata related to the images mentioned above, including:

- Time and date of image capture;
- GPS coordinates; and
- Camera identification such as officer and vehicle/unit number.

Optical character recognition (OCR) technology converts images of license plates into readable formats that allow various applications including information matching, lookup, aggregating and storage.

7. Data Security

The City relies on third-party vendors for its parking management systems. Conduent has supplied the City's parking citation issuing and processing solution for the past five years and was recently awarded a new five-year contract. In response to security requirements in the City's competitive request for quotations, Conduent made the following declaration:

"Conduent takes the security of our systems and customer data very seriously. We go to great lengths to make sure that all the proper security measures from an application, operating system, hardware, and network perspective are in place and updated regularly. Starting with our network architecture, Conduent uses a series of industry-standard firewalls and intrusion detection systems to ensure that no unauthorized access to our systems is obtained. Our team of security experts is constantly monitoring for any new security alerts and patches that need to be applied to our infrastructure (e.g., OS, hardware, and network). We also perform regular internal security audits to make sure that all system security measures are kept up to date and no new vulnerabilities exist. From an application perspective, access to our systems requires a valid user ID and password that is set to expire at regular intervals. Each user is given access to specific functions based on job role and each user's access and activity is logged for auditing purposes."

Staff confirms that these general security measures will extend to its use of Conduent's ALPR solution. DOT commits to developing standard operating procedures that respect and build on these measures and related safeguards.

[2] Such as sedan, SUV, hatchback, pickup, minivan, van, or box truck.

8. Fiscal Cost

Initial Purchase Cost

DOT secured City Council approval through the Mid-Cycle Budget process to procure ALPR equipment for five (5) parking enforcement vehicles at a one-time cost for equipment and setup of $338,600.

Personnel Costs

Existing DOT staff, including Parking Enforcement supervisors and Parking Control Technicians, will be trained by the City's vendor to use the ALPR system with the aim of incorporating the technology into its routine enforcement activities. Other DOT staff already dedicated to parking management initiatives will use occupancy data from the system in support of demand-responsive parking and other transportation-related initiatives.

Ongoing Costs

The annual, recurring costs of the five vehicle-mounted APLR systems is expected to be $28,800 payable to the vendor.

Potential Sources of Funding

With ALPR-equipped vehicles, increases in Parking Control Technician productivity are conservatively estimated to result in one additional citation per hour. Together, the five ALPR-equipped vehicles are expected to generate an additional $500,000 in citation revenue annually.

Potential Replacement/Insurance Costs

In the event an ALPR equipped vehicle is permanently out of service (i.e. due to a total loss vehicle accident) there will be an expected cost to replace.

9. Third Party Dependence

The City depends on third-party vendors to provide parking management systems including Conduent (parking citation issuance and processing solution), Paylock (ALPR scofflaw boot solution), Parkmobile (meter pay-by-phone), IPS (single-head and multi-space smart meters), and Scheidt & Bachmann (off-street parking and access control system).

The proposed ALPR solution will be sourced and supported by Conduent. In April, 2018 the City contracted with Conduent to supply a Parking Citation Management Solution, Parking Enforcement Equipment and Special Service Project. That solution is intended to integrate "key City of Oakland and third party stakeholder systems to deliver a comprehensive automated parking citation processing, including a public portal for online services, accurate processing of lockbox payments, timely production of all correspondences and collection of unpaid citation and to ensure parking enforcement equipment/handheld devices and automated license plate recognition systems are fully functional and in compliance with all specifications of the City's Request For Qualifications #13375 and Contractor's RFQ Response." The Genetec-ALPR solution is offered as an option in the new contract.

10. Alternatives

The alternatives to using the proposed ALPR solution include:

- Continuing to capture license plate images as part of the citation issuing process with handhelds (this option will remain available under the new Conduent contract whether the APLR option is executed or not);
- Continuing to time-stamp vehicles in time-limited parking spaces and areas by staff typing plate information into handhelds (this option will remain under the new contact);
- Issuing permits for Residential Permit Parking (RPP) areas by using bumper stickers and hanging placards, the procurement, processing, and use of which would be relatively costly and inconvenient and less environmentally friendly;
- Verifying meter payments using "pay-by-phone" and "pay-by-plate," which would require staff to type plate information into their handhelds;
- Limiting "Hotlist" vehicle identification, including scofflaw and stolen vehicles, to those vehicles that are processed manually through handhelds;
- Continuing to conduct parking occupancy and turn-over counts and analysis in support of parking management programs intermittently and less reliably by costly consultants or, when available, student interns;
- "Smart parking" applications, including mobile apps providing parking availability and wayfinding information, will be less reliable and therefore less likely to be adopted.

11. Track Record

The City of Oakland Department of Transportation is a new department, so it does not have a track record to report concerning its use of ALPR. However, since 2009, the Finance Management Bureau has managed and Police Service Technicians (PSTs) in the Oakland Police Department have staffed a Paylock-contracted project using ALPR to enforce scofflaw vehicles.

In addition, several cities in California have been using ALPR for years. For example, the cities of Berkeley and Sacramento have been using ALPR since 2013 and 2003, respectively.[3] Although these cities most often use ALPR for law enforcement purposes, [DOT is not aware of any privacy issues or concerns arising from these programs.]

While this impact analysis and proposed use policy for ALPR have been developed by DOT alone, DOT staff recognizes the need to work across departments to maximize the benefits of ALPR investments to parking and related operations while preserving the civil liberties and privacy of the community. Questions or comments concerning this draft Impact Assessment should be directed to Michael Ford, Manager, Parking and Mobility Division, via email at mford@oaklandca.gov or phone at (510) 238-7670.

[3] See https://www.eff.org/pages/california-automated-license-plate-reader-policies for a list of California cities using ALPR. [FNs for Berkeley and Sacramento agreements]

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 AL~~R~~PR 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

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: XX Mar 19
Coordinator: Information Technology Unit

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

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

A. Description of the Technology

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

A – 1. How ALPR Works

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

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

A – 2. The ALPR System

There are two components to the ALPR system:

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

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

B. General Guidelines

B – 1. Authorized Users

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

B – 2. Restrictions on Use

1. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

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

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

4. While ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

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

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

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.

8. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.

C. ALPR Data

C – 1. Data Collection and Retention

1. <u>Transfer of Data</u>

   Data will be transferred from vehicles to the designated storage in

accordance with department procedures.

2. Data Retention

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

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

C – 2. Data Security

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

1. All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose (Civil Code § 1798.90.52).

2. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

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

C – 3. Releasing or Sharing ALPR Data

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

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

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

2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy

Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

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

D. ALPR Administration

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

D – 1. ALPR Administrator

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

D – 2. ALPR Coordinator

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

D – 3. Monitoring and Reporting

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

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

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

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

D – 4. Training

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

Training requirements for employees authorized in ALPR Users Section include completion of training by the ALPR Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

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

Training updates are required annually.

By Order of

Anne E. Kirkpatrick
Chief of Police Date Signed: