CITY OF OAKLAND

Privacy Advisory Commission

February 4, 2021 5:00 PM
Teleconference
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Heather Patterson*

Each person wishing to speak on items must raise their hand as per the instructions below during the teleconference. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

Pursuant to the Governor's Executive Order N-29020, all members of the Privacy Advisory Commission as well as City staff will join the meeting via phone/video conference and no teleconference locations are required.

TO OBSERVE:
Please click the link below to join the webinar:
https://us02web.zoom.us/j/85817209915
Or iPhone one-tap:
US: +16699009128, 85817209915# or +13462487799, 85817209915#
Or Telephone:
Dial (for higher quality, dial a number based on your current location):
US: +1 669 900 9128 or +1 346 248 7799 or +1 253 215 8782 or +1 646 558 8656 or +1 301 715 8592 or +1 312 626 6799
Webinar ID: 858 1720 9915
International numbers available: https://us02web.zoom.us/u/kDUn0z2rP

TO COMMENT:
1) To comment by Zoom video conference, you will be prompted to use the "Raise Your Hand" button to request to speak when Public Comment is being taken on the eligible Agenda item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

2) To comment by phone, you will be prompted to "Raise Your Hand" by pressing "* 9" to request to speak when Public Comment is being taken on the eligible Agenda Item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.
ADDITIONAL INSTRUCTIONS:
1) Instructions on how to join a meeting by video conference is available at: https://support.zoom.us/hc/en-us/articles/201362193%20-%20Joining-a-Meeting#
2) Instructions on how to join a meeting by phone are available at: https://support.zoom.us/hc/en-us/articles/201362663%20Joining-a-meeting-by-phone

3) Instructions on how to “Raise Your Hand” is available at: https://support.zoom.us/hc/en-us/articles/205566129-Raising-your-hand-In-a-webinar

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Review and approval of the draft January meeting minutes

4. Surveillance Equipment Ordinance - OPD – Automated License Plate Reader impact report and proposed use policy – review and take possible action.

CITY OF OAKLAND

Privacy Advisory Commission

January 7, 2021 5:00 PM
Zoom Teleconference
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Heather Patterson*

1. Call to Order, determination of quorum

Members present: Suleiman, Hofer, Katz, De La Cruz, Oliver, Gage.

2. Open Forum/Public Comment

Assata Olugbala spoke about the PAC item on the agenda regarding a Fair Payment Ordinance suggesting it is designed to assist undocumented persons only and doesn't help other persons. She also complained about the resources directed at Lake Merritt activities in the fall.

3. Review and approval of the draft October meeting minutes

The minutes were adopted unanimously.

4. Fair Payment Ordinance – Hofer, Patterson, Gage, Tomlinson – introductory review of proposed ordinance requiring that businesses accept cash as one form of payment. No action will be taken on this item at this meeting.

Chairperson Hofer opened by explaining that he and other members worked on the draft a year ago and was intending to set up meetings with the chamber of commerce and some others but the pandemic put this on hold. This is the beginning of the conversation and a chance for PAC Members to discuss initial concerns. He noted that many businesses are refusing to accept cash in part due to the pandemic and in part due to security concerns. However, the impact on those who cannot get bank accounts, or are charged fees when using preloaded debt cards are at a disadvantage. Also, the data collection and tracking being done by credit card companies raises many privacy concerns for individuals.

He noted that other jurisdictions have done this, in varying forms, and the Oakland proposal seeks to go further, beyond just retail, to preserve people's ability to have cash transactions.

He asked that Joe DeVries summarize some thoughts on enforcement and implementation concerns. Joe reflected back on the City's ban on Styrofoam which was a challenge in enforcing. The City was trying to educate small businesses and not punish them but the staffing needs made even that difficult. He also noted the illegal dumping ordinance relies on capturing evidence of a vehicle being involved in the dumping. The City then goes after the vehicle owner but if they are nonresponsive, they can avoid paying and keep dumping. The City doesn't have the power to attach to the vehicle's registration and sending people to collections is not very effective either.

Chairperson Hofer asked about administrative fees being built in to a program ahead of time and Joe drew a comparison to the Excess Litter fee which is charged to convenience stores and fast food restaurants to defray the cost of picking it up in Oakland. He noted that all fees are designed to pay for services but fines are not used to cover fixed costs.

Lou Katz noted credit card transactions track at least one's zip code. He also spoke about transportation systems; BART is moving away from cash which will be a risk for people without bank accounts as the won't be able to take transportation without a credit card. He wants language specifically around transportation as well as pharmacies.

There were XX public comment: J.P. Masser noted that he helped with the Berkeley and San Francisco ordinances and has not heard of any serious issues coming up since adoption. He supports a more expansive measure and noted it is an equity issue across all races for lower income people. He also noted that the ordinance is self-enforcing; if a store doesn't take cash, it will get posted on social media for example and it will be easy for the City to be alerted to the problem.

Assata Olugbala also spoke about the conversation around enforcement and the cost involved. She noted the current budget deficit is huge and the cuts that will occur will make it hard to dedicate any staff resources to it. She is skeptical that social media will be a likely way to call attention to violators.

Member Oliver raised concern about the many fees charged in neighborhood stores for using debit cards/credit cards which is an added tax on people that is frustrating. Although this is a state/federal issue, it is a good example of the hidden costs to people. Member De La Cruz voiced his support for the ordinance based on his past work with AC Transit on this issue.

The Chair noted that this will be a slowly developing item and he will continue to work with the ad hoc committee that started work on the item.

5. Surveillance Equipment Ordinance – Katz, Hofer – how to ensure transmission of Privacy Advisory Commission recommendations to City Council – discuss and take possible action.

The Chair cited a few recent examples where the recommendation from the PAC did not make it to the Council when the item was introduced. He is looking for a mechanism to make sure this does not happen in the future. He asked for some clarification from staff about how things are brought forward.

Joe DeVries explained that when a policy is submitted, it is done so by the department, not the CAO but he reviews the reports to ensure they include the recommendations from the PAC. He believes there were a couple of unique circumstances that created the omissions recently: For example, with the Drone policy it was several months between the PAC action and Council Meeting. He offered to have a section in any report to Council that is for the Chief Privacy Officer to insert some detail as a check and balance. Bruce Stoffmacher agreed that there were a few unique omissions recently but would support the idea of a CPO section in the reports. He also supported Council Member Bas's recommendation that the PAC motion be included in the report. Chairperson Hofer noted that if the PAC provides a written motion in advance it would help as well. Member Suleiman also suggested that the written motion be included in the PAC Minutes in full length instead of shorthand as well.

6. Surveillance Equipment Ordinance – Hofer – Work Flow and Priority List updates.

The Chair shared the original priority list to see what changes need to be made. There was some conversation about the Body Worn Camera discussion and the process it will need to follow in regard to the Police Commission and NSA Court Monitor. There were some items discussed that could be removed and the list will be forwarded to the Chair prior to the February meeting if the department is seeking changes.

The group discussed the website and if the annual reports that are due (or received) are posted accordingly. Joe Devries noted he has an active request in for more admin support to address and update the website but with the deficit, there will not be any new staffing support for the foreseeable future.

7. Surveillance Equipment Ordinance - OPD – Automated License Plate Reader impact report and proposed use policy – review and take possible action.

The Chair noted that the new policy draft is slightly different and asked if staff had anything to highlight. DC Holmgren opened up with a welcome message of continued collaboration. There was a question about expanding the technology and Brice Stoffmacher noted that the department may want to upgrade the technology but they are not at that point right now.

There was conversation about what Hot Lists exist and it was explained that there is a State Department of Justice Hot List only. A local agency may have its own as well (and OPD monitors its own). If they have a vehicle that should be entered into the state system, they will add it. But if it is an internal list, not entered into the state system, the ALPR won't alert an officer that drives by a vehicle usually. However, there is a way to have a vehicle flagged in the system for a limited period of time at the local level without it being sent into the state system.

There were two public speaker on the item: JP Masser noted his discouragement looking at language that is vague such as "legitimate law enforcement use," the point of a policy is to list what is acceptable, not just allow all uses. Also, he believes the reporting section needs strengthening including the analysis of topics such as how many stolen vehicles are recovered. The policy states that OPD only must say how often the system is use; he believes far more detail is needed.

Michael Katz-Lacabe submitted his comments in writing and those are copied here:

C-1.2 Maximum Retention is two years, which is an excessive period of time not based on a demonstrated need. I recommend a substantially shorter retention period on the order of 30-60 days to reduce the potential privacy implications for the storage and use of the data.

C-1.2 states that ALPR data may be retained for "Other Departmental Need." This is far too broad a category for which the data may be retained. This should be eliminated or revised to be much more restrictive.

C-2 This section on data security says nothing about whether the stored ALPR data is encrypted. In addition, while the use of a username and password to access ALPR server data is the bare minimum for what should be expected, the use of two-factor authentication would prevent access to the data in the event that a user's credentials were compromised.

C-3. It's unclear whether any sharing of ALPR data with other agencies would generate an auditable paper trail. How could an audit of ALPR data sharing determine whether the ALPR data had been shared with a rogue agency or with an immigration enforcement agency?

D-3.1 The requirement to report "The number of times the ALPR technology was used." Is unclear at best. I recommend that the information that should be reported to include:

- *How many license plate reads*
- *How many unique license plate reads*
- *How many hits*
- *How many misreads, including the make and model of the ALPR*
- *The data should be disaggregated for mobile (police vehicle), stationary (when that become applicable) and other mobile (trailers or cameras used for tracking dumping)*
- *How many stolen vehicles were recovered/felony suspects arrested*

General Policy Comments:

In addition, the policy states that ALPR data may be shared "for official law enforcement purposes or as otherwise permitted by law" but as otherwise permitted by law means anything goes because there are essentially no laws preventing sharing of ALPR data besides those restricting sharing for immigration purposes.

How would the security of the ALPR data be protected as it is shared with another agency. Would the sharing occur via email? Via paper, Via CopLogic? What would be considered acceptable?

The policy does not appear to include a requirement to manually verify the ALPR read before initiating a stop. Failure to verify the ALPR read has lead to situations in which police have performed high-risk stops of innocent motorists/vehicles.

The policy does not include a requirement for regular audits to ensure that the ALPR data is only accessed by authorized personnel and for authorized reasons.

The policy does not address how hot-lists are generated or where they are sourced from. What are the legitimate and authorized reasons for which a license plate can be added to a hot list?

Member Katz noted his concern with a two-year retention period and recommended a much shorter period. He also noted that the public comments above captured many of his concerns. Member De La Cruz noted a similar concern with retention and that the above comments reflected his concerns as well.

Member Suleiman had a few questions about Hot Lists and databases—how does the department address license plates that remain on the list long after recovery which she imagines is common with rental car companies. She also asked about demographic data that could be collected using ALPR. DC Holmgren noted there is a lot of human error the department has to be very diligent about but is not sure if a manual 90-day audit, for example, is possible. As for demographic data, the department's CAD system just does not have the capability to do this as other departments do—there is no drop-down menu where an officer can identify that ALPR was used in the reporting. This type of ability is about a year out.

Chair Hofer noted areas where the policy has some conflicts with state law/court decisions and some errors that will require an ad hoc committee to focus on. He is concerned about the two-year retention conversation. He also sent the 2016 ALPR Policy that OPD put forward before a Surveillance Ordinance existed but when State Law (SB34) required that all departments adopt one. The Oakland Policy included an annual report and Chairperson Hofer asked if any reports were provided, if any audits were done, and if records of third party data sharing were kept as delineated in the Policy. He asked if these items were handled. DC Holmgren said he believed they were based on his conversations with staff. The department is assembling the data right now. The department has a 2019 annual report and is researching if a 2017 and 2018 report was created. Chairperson Hofer noted that the data that would be included in these reports would be helpful in developing the current policy. Officer Pullen, who works on the system noted that the current system is broken and internal audits cannot be performed and the department is working on correcting this.

There was continued discussion, especially around the retention po;licy and the item was continued to the next meeting with a request for the past annual reports to inform the process and that an ad hoc group meet to work on details between meetings.

The meeting adjourned at 7:08.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Automated License Plate Reader

A. Description: *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 activated when the user logs into the software from their vehicle-based computer and starts the system.~~urned 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; OPD's ALPR system updates daily with three California Department of Justice (CA DOJ) hotlists: felony wants, stolen plates, stolen vehicles – there is no OPD ALPR connection to any federal 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.

[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.

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

B. **Purpose:** *How OPD intends to Use ALPR Technology*

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.

ALPR technology helps OPD personnel to leverage their public 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~~ determine where ~~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 vehicle aspects (e.g. 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 license plate and whether the license plate has been switched from a different vehicle. Such information may help personnel to find new leads in a felony crime investigation.

OPD has not historically quantified ALPR usage for vehicle stops, nor for later criminal investigations[2] in a way that easily allows for impact analysis. However, OPD is developing more automated processes for tracking ALPR usage in connection with investigations – OPD and the City's IT Department are currently engaged in a multi-year new CAD/RMS implementation which will greatly improve this type of data tracking.

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. The following list highlights specific cases from the year 2020 where ALPR played a pivotal role in supporting CID investigations:

- Missing Person + Homicide Case – A female was reported missing. During the CID investigation, a positive hit was recorded by an ALPR system (based on the vehicle license plate registered to the missing person). Officers responded, and her deceased remains were found in the truck of the vehicle. There is an ongoing homicide investigation.
- Human Trafficking Case – A juvenile was a victim of human trafficking. The CID investigator utilized ALPR to identify the suspect. The victim was safely relocated. A Ramey warrant[3] was authorized for the suspect's arrest.
- Human Trafficking Case – A DOE was kidnapped and the victim was able to provide investigators with a license plate. Investigators inputted the license number into the OPD ALPR system so officers could identify a suspect if there was an ALPR hit.
- Human Trafficking Case – undercover OPD officers were working a sting operation when they were approached by a subject who attempted to kidnap them. The suspect was arrested and taken into custody, but his accomplice fled the scene. Body-worn camera (BWC) footage and officer observation captured the suspect vehicle. A Ramey warrant is now pending for the outstanding suspect.
- Sexual Assault – A person was sexually assaulted. ALPR was used to locate and arrest the suspect. This case has been charged by the DA's

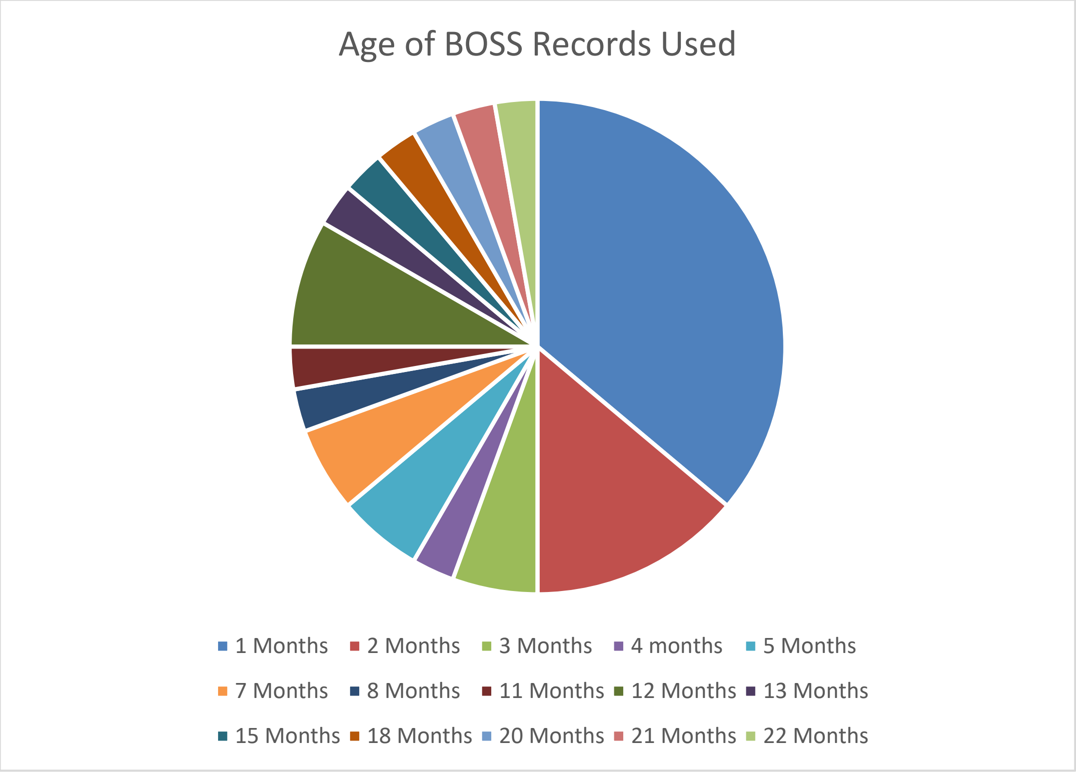
[2] Current policies mandate documenting reasons for vehicle stops and reported race and gender of persons stopped. OPD is reviewing how to ensure that investigators note when ALPR was instrumental in criminal investigations for documenting ALPR impact.

[3] A Ramey Warrant is an arrest warrant that is obtained by a police agency directly from a judge and bypassing the district attorney (DA) (who otherwise issues arrest warrants). In the interest of faster processing due to the nature of the crime and/or DA availability, a police agency may skip the district attorney and go directly to a judge. The police agency must submit a declaration, along with a report, to the judge setting out their reasons for requesting that the judge issue the warrant; the judge must believe that there is probable cause, and sufficient evidence that the suspect has committed a crime.

Office.

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.

The ALPR data used to investigate these cases varies widely. A recent analysis of ALPR queries shows that most revealed data that was less than one month old (13 cases), and the number of cases using older data diminishes. However, there are still valuable cases using data even 18-24 months old. The chart below illustrates the recent age of this query data.



C. ~~L~~ocations 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, while engaged in the course of their duties.

D. Privacy Impact: How is the OPD ALPR Use Policy Adequate in Protecting Civil Rights and Liberties and whether ALPR was used or deployed, intentionally or inadvertently, in a manner that is

discriminatory, viewpoint-based, or biased via algorithm

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. People are generally creatures of habit and often drive in their vehicles the same way to work, to visit friends and associates, to houses of worship, and neighborhood grocery stores. Research shows that “metadata”, 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 University lawyer and computer scientist Jonathan Mayer was able to accurately identify 80 percent of the volunteers in his study, using only open source databases such as Yelp, Facebook, and Google[4].

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~~However, OPD can only develop use the system to make such determinations by ~~such by~~ manually querying the system based upon a right to know (see Mitigation section 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 (A) above and the Mitigation (E) 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. OPD does not affix ALPR cameras to fixed infrastructure. OPD deploys ALPR camera-affixed vehicles through every area of Oakland[5], 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

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

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

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 in connecting to CA DOJ felony wants, stolen plates, stolen vehicles hotlists).

E. Mitigations: specific, affirmative technical and procedural measures that will be implemented to safeguard the public

Oakland residents and visitors have 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 of r~~r~~eal-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, etc.) may be captured in an ALPR image capture as well. However, OPD's BOSS ALPR database can only query license plate numbers.

ALPR can only be used for authorized purposes consisting only of queries related to criminal investigations and other authorized law enforcement functions, as explained in ~~to investigate criminal activity, as explained in~~ DGO I-12.B-2 "Restriction on Use: 1. "Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53); authorized purposes consist only of queries related to criminal investigations and other authorized law enforcement functions~~.~~" Additionally, OPD is required to provide an annual report to the PAC (per OMC 9.64) documenting ALPR usage during the prior calendar year. The annual report will contain audit data of system queries (e.g. document aspects of use activity - time, date, and what is searched).

DGO I.12.B-2 also provides a number of internal safeguards, including:

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

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

3. No ALPR operator may access department, state or federal data unless

otherwise authorized to do so pursuant to Section D1 below.

4. 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.

F. **Data Types and Sources*:*** *A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom.*

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 (although newer systems allows for queries based on license plate characters; newer systems do allow for queries~~y~~ based on vehicle type and color); therefore, ~~authorized personnel can only query license plate numbers~~. T~~ — t~~here is no way to query the system based on vehicle details (such as bumper stickers) or individuals associated with a vehicle.

All ALPR data downloaded to the server shall be purged from the server at the point of 365~~730~~ [SB1]days in alignment with Government Code section 34090. Data may be retained outside the database for the following purposes:

a. A criminal investigation;

b. An administrative investigation;

c. Research;

d. Civil litigation;

e. Training; and/or

f. Other Departmental need.

California law does not mandate a specific retention period for ALPR data. California Civil Code Title 1.81 .23 governs "Collection of License Plate Information."

Although the Civil Code requires ALPR operators to adopt a "usage and privacy policy" that specifies the "length of time ALPR information will be retained", it does not mandate a specific retention period. However, when the legislature has not prescribed a retention period for a particular type of document, the two-year "catch-all" retention period in California Government Code section 34090 applies.

Section 34090.6 specifically addresses "routine video monitoring" and the destruction of video "recordings," and stipulates that the head of a department of a city may destroy recordings of routine video monitoring after one year. However, there is no legislative history or case law interpreting or suggesting that this is the appropriate retention period for ALPR data. OPD and the Office of the City Attorney ultimately believe that a 730 day data retention period would be most aligned with CA Government regulations, but that a 365-day data retention period still aligns with state law. Any data retention short of 365 days would open the City to liability risks; staff therefore believes that a 365 day ALPR data retention period aligns with internal investigatory need and State law while balancing public privacy concerns.

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.

OPD ALPR's system is connected to the City's virtual private network (VPN) gateway, and is encrypted through the transport. The encrypted data ends at the VPN gateway and the ALPR data goes into the internal SQL database where records can be search using the OPD internal BOSS3 server. Both the BOSS3 server and ALPR SQL database are internal services that can only be accessible within the OPDnet network.

The current OPD BOSS ALPR system is not-cloud based; ALPR-camera equipped vehicle computers can download (not upload) State DOJ databases as described above. However, OPD will look to upgrade this outdated system should the City Council approve DGO I-12.

Only authorized OPD personnel have ~~Limited OPD personnel have acc~~access to the OPD ~~the~~ ALPR ~~BOSS~~ system. The ALPR coordinator is responsible for providing training ~~including the verification of potentially malicious email or other forms of computer hacking~~on the ALPR system use to authorized personnel.~~ OPD also conducts regular ALPR system audits to ensure the accuracy of ALPR data~~.

G. **Fiscal Cost:** *The fiscal costs for the surveillance technology, including* *initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;*

OPD spent $293,500 in 2014 to purchase the ALPR system from 3M. Neology later purchased the ALPR product line from 3M. OPD 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.

The following information is a financial estimate to upgrade OPD's entire ALPR system:

- New Hardware and support for 35 vehicles: $363,000
- New BOSS4 software (On premise on year license): $15,000
- New BOSS4 software (Hosted storage 1 year license): $43,000

H. **Third Party Dependence:** *Whether use or maintenance of ALPR technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis*

OPD relies upon third party technology vendors to install and provide maintenance for ALPR systems (currently EVO as explained in Section H above). Vendors contracted with the City for vehicle ALPR installation and maintenance of the systems will not handle or store the ALPR data. Data gathered from each vehicle system is uploaded from the vehicle to the server for secure storage.

Maintenance of the server may require vendor supplying OPD with the server software to handle data stored in it; this access will be controlled by the City's IT Department.

I. **Alternatives Considered:** *A summary of all alternative methods considered in-lieu of ALPR, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate*

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 on 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.

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

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

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

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

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: XX
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 System are for the official use of this department. Because such data contains investigatory and/or 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 where the photograph was taken, 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 where the photography was taken ~~of the license plate~~ – in a ~~forward-facing graphical user interface~~ database that is accessible by law enforcement agencies for investigative query purposes.

A – 2. The ALPR System

There are two components to the ALPR system:

1. Automated License Plate Readers: These devices include cameras which can be attached to vehicles or fixed objects and a computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hotlists; data is transmitted for comparison (the hotlists are downloaded to the vehicle at the start of the

patrol shift and then compared from that list)~~, 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: A~~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. Sworn personnel, Police Service Technicians or other OPD authorized ~~, OPD parking~~ personnel may ~~are authorized to~~ use the technology. Other authorized users may be designated by the Chief of Police or designee.

B – 2. Restrictions on Use

1. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53); authorized purposes consist only of queries related to criminal investigations, administrative investigations, and other authorized law enforcement functions, at the approval of a commander at rank of Deputy Chief or Deputy Director.

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

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

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

C. ALPR Data

C – 1. Data Collection and Retention

1. Transfer of Data

   Data will be transferred from vehicles to the designated storage in accordance as defined and designed by the ALPR technology system provider data transfer protocol.

2. Data Retention

All ALPR data downloaded to the server shall be purged in the server at the point of ~~730~~ 365 days in the server system. Data may be retained outside the database for the following purposes:

a. A criminal investigation;
b. An administrative investigation;
c. Research;
d. Civil litigation;
e. Training; and/or
f. Other Departmental need – with written authority from the Deputy Chief or Deputy Director.

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

2. Members approved to access ALPR data under these guidelines are permitted to access the data for ~~legitimate~~ law enforcement purposes only.

3. ALPR system audits shall be conducted on a regular basis by the Bureau of Services to ensure proper system functionality; designated personnel will notify the City's Privacy Advisory Commission (PAC) in the event that the ALPR system cannot fully produce system audits due to technical issues with the system, and collaborate with the PAC to develop a plan to ensure audit functionality.

C – 3. Releasing or Sharing ALPR Server Data

ALPR server 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~~:

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.

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

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, 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 proper functionality of the system.
The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report in accordance with the requirements of OMC 9.64 (Oakland Surveillance Technology Ordinance).

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 shall include the following:

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

By Order of

Susan E. Manheimer
Chief of Police

Date Signed: