CITY OF OAKLAND

Privacy Advisory Commission

January 7, 2021 5:00 PM
Zoom 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 fill out a speaker's card. 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 October meeting minutes

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.

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

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

7. 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

October 1, 2020 5:00 PM
Online Zoom Meeting
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**: Vacant*

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. Call to Order, determination of quorum

Members Present: Suleiman, Brown, Hofer, Katz, De La Cruz, Tomlinson, and Oliver.

2. Open Forum/Public Comment

Asada Olugbala spoke about the proposal to end the City's involvement with the Joint Terrorism Task Force that the PAC is supporting which is coming before the City Council soon. She expressed concern that this could impact the City and Federal Government's efforts to combat domestic terrorism by right-wing white supremacist groups that target communities of color.

3. Review and approval of the draft September meeting minutes

The September minutes were passed unanimously.

4. Surveillance Equipment Ordinance – OPD – Exigent Circumstances Use Report (UAV) – review and take possible action.

Lt. Daza-Quiroz presented the UAV Use Report from two instances in which OPD was provided UAV support from the Alameda County Sherriff. In both instances the UAV was used to photograph crime scenes (and aid in collecting evidence) and in one instance it was used to locate a missing K9 (dog) that went missing during the operation. The Lieutenant read to the PAC an email he sent department-wide

after these uses that directed all staff to contact him prior to any future use of a UAV to ensure the planned use is allowable.

Member Suleiman noted her concern about department staff needing training on all Use Policies based on this instance which clearly was not exigent. She also spoke about her concern that the evidence was collected by the Alameda County Sherriff and therefore outside OPD's control. Chair Hofer stated that the collection of evidence does not qualify as exigent.

There was one Public Speaker: Asada Olugbala also aired concern that the evidence collected is outside the City's control and that the AC Sherriff retains that data for up to three years. She asked how this can be prevented in the future.

Chair Hofer moved that the PAC accept the report but to include the email the Lieutenant sent to staff and a letter from the Co-Chairs about the need for training staff on existing policies.

DC Holmgren noted that the use of the drone to track down the K9 was actually exigent and Chairperson agreed and modified the motion to note that difference. The motion passed unanimously.

5. Surveillance Equipment Ordinance – OPD – Live Stream Use Reports (2) – review and take possible action.

Captain Wingate delivered the reports to the PAC and the reports included information about why the department felt it was necessary to deploy the cameras during large scale gatherings following the George Floyd killing and subsequent protest and civil unrest. The reports contained a greater amount of detail than prior reports which members appreciated.

Member Suleiman asked about adding more information about outcomes—explaining after-the-fact how the equipment was helpful. Captain Wingate agreed to incorporate that type of detail into subsequent reports. Chairperson Hofer asked if it would be easier for OPD to provide immediate notification when the equipment is deployed as opposed to a report afterwards and Captain Wingate confirmed that would be an easier process. Joe DeVries noted the EOC is updating its procedures and perhaps that notification can be built into that process. Captain Wingate also offered a tour of the EOC for PAC members.

There was one public speaker: Asada Olugbala raised concerns about what other jurisdictions do when they come into Oakland to provide Mutual Aid. She worries that they do not follow the same procedures that OPD is held to.

A motion was made to accept the reports and it passed unanimously.

6. Surveillance Equipment Ordinance – OPD – Crime Lab Biometric Technology Impact Report and proposed Use Policy -review and take possible action.

Dr. Sandra Sachs presented the Use Policy on behalf of the department and was supported by staff member Laura Silva. The PAC had several questions that mostly focused on data storage and security. Member Tomlinson asked what vehicle is used to transfer data and Laura Silva explained that a CD is

burned and then handed off with a close tracking of the chain of custody. For electronic transfers it is done through the CODIS server which is walled off from other networks/internet in the building.

Member Suleiman asked about "documented consent" in the Use policy and Laura explained that all evidence must be lawfully collected and there are different levels of consent that must be adhered to. Member Katz asked if we know who can access our data in CODIS and Laura confirmed there is a careful audit trail. The lab staff noted they chose not to use a cloud system to backup data to maintain security and all CD back-up copies are kept under lock and key.

Chairperson Hofer asked Dr. Sachs about any backlog of evidence kits and she reported that there currently is no backlog and expressed pride in her team for their diligence in addressing the one that had existed.

There was one public speaker: Asada Olugbala noted that the City Council directed staff to bring a policy forward by September 2020 to the PAC and Chairperson Hofer stated he felt the department had abided by that direction.

Chairperson Hofer made motion to approve the redlined policy as presented and it was adopted unanimously.

7. Surveillance Equipment Ordinance Amendments – Hofer/Gage/De La Cruz – review and take possible action.

There was some discussion on Annual Reporting requirements, prioritizing policies, and consensus was reached on when a department needs to return to Council. After some conversation, a motion was made to approve the modified ordinance and it passed unanimously.

THE FAIR PAYMENT PRACTICES ORDINANCE

Whereas, the City of Oakland strives to be a welcoming, inclusive place for all City residents; and

Whereas, the City of Oakland strives to empower all its residents to participate in Oakland's economic life. A key aspect of participation in economic life is the ability as a consumer to purchase goods and services; and

Whereas, for many Oakland residents (for example, those who are denied access to credit, or who are unable to obtain bank accounts), the ability to engage in consumer transactions depends on the ability to pay for goods and many services in cash. This is especially true of the very poor; and

Whereas, millions of Americans do not hold bank accounts, or otherwise fall outside the non-cash financial system. Some stand apart by choice, because they are concerned about privacy and do not want their every financial transaction recorded by banks and credit card companies; physical cash remains the most accessible anonymous medium of exchange in this country. Others may not be well situated to participate in the formal banking system or may be excluded from that system against their will. In short, denying the ability to use cash as a payment method means excluding too many people; and

Whereas, according to the Federal Deposit Insurance Corporation (FDIC), in 2017, 17% of all African-American households and 14% of all Latino households in the U.S. had no bank account at all, and while 84% of white people are considered "fully banked", only 52% of African-American households and 63% of Latino households achieve the same status.[1] Not accepting cash payment is tantamount to systematically excluding segments of the population that are largely low-income people of color. Cashless business models may also have significant detrimental impacts on young people who do not meet age requirements for credit cards, for the elderly (many of whom have not transitioned to credit and digital payment modes at the same rate as younger generations), and for other vulnerable groups (such as the homeless and immigrant populations); and

Whereas, a so-called "privacy tax" is imposed upon lower income residents that cannot afford more secure products. The U.S. funded "Lifeline Assistance" program funded the purchase of certain Android phones that came pre-installed with Chinese malware that could not be uninstalled, and which were given at low or no cost to qualifying individuals thereby placing their privacy interests and communications at risk[2]. Lower income residents entitled to government benefits are already forced to surrender their right to

---

[1] https://www.federalreserve.gov/publications/2018-economic-well-being-of-us-households-in-2017-banking-credit.htm

[2] https://www.forbes.com/sites/thomasbrewster/2020/01/09/us-funds-free-android-phones-for-the-poor---but-with-permanent-chinese-malware/#170ba279abab

privacy in order to qualify, forced to agree to searches of their person, home, drug testing, and disclosure of information not normally required during the regular course of business[3]; and

Whereas, the use of a credit or debit card as payment allows the seller to learn our first and last name, and when combined with a zip code required by many merchants, a revealing portrait of our lives becomes possible. When data appending services are used, sellers may be able to acquire our email and postal addresses, and phone number. This information allows sellers to access the largely unrelated data broker industry, which could reveal additional demographic information including but not limited to, our employment history, marital and homeownership status, hobbies, medical conditions, sexual preferences, and locational history[4]; and

Whereas, the City of Oakland has been a Sanctuary City since 1986, and did enact a Sanctuary Contracting Ordinance in May 2019, to ensure that taxpayer funds are not subsidizing ICE's deportation machine. ICE Enforcement Removal Operations issued a Request for Information on August 3, 2017, and subsequently entered into a contract with data broker behemoth Thomson-Reuters to obtain commercial subscription data services capable of providing continuous real-time information pertaining to 500,000 identities per month from sources such as State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; Vehicle Registration Information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN) data; and employer records. Undocumented residents that are forced to use credit or debit cards to conduct everyday transactions are therefore placed at additional risk of detection and deportation by ICE; and

Whereas, the July 2019 data breach of Capital One, which affected over 100 million Americans and 6 million Canadians, greatly impacting the privacy interests of all involved, did not even register in the top 10 largest data breaches; and

Whereas, the five largest known data breaches occurred at American owned businesses and impacted billions of people around the world[5]; and

[3] https://www.fastcompany.com/90317495/another-tax-on-the-poor-surrendering-privacy-for-survival
[4] https://www.aclufl.org/en/news/why-dont-we-have-more-privacy-when-we-use-credit-card
[5] https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html

Whereas, the states of New Jersey[6] and Massachusetts[7], and the cities of San Francisco[8], Philadelphia[9], and Berkeley[10] have each enacted prohibitions on cashless stores. On January 23, 2020, the City Council of New York passed a similar ordinance - Mayor DeBlasio has stated he supports the intent[11].

Whereas, the City Council finds that it is the intent of this ordinance to ensure that all Oakland residents, including those who lack access to other forms of payment, are able to participate in Oakland's economic life by paying cash for goods or services; now, therefore

Commented [PHM1]: Helpful to include information about prevalence of the practice in Oakland? Is this currently a problem? If not currently a problem, could use Berkeley ordinance language: "As of today, there are few stores in Oakland that do not accept cash, and so now is a good opportunity to guarantee that these discriminatory practices are not permitted in our City."

THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

Section 1. Title

This ordinance shall be known as the Fair Payment Practices Ordinance.

Section 2. Definitions.

1) "Brick-and-Mortar Business" shall mean any place of business operating at a fixed, permanent physical premises. Brick-and-Mortar Business does not include any business not operating at a physical premises within Oakland (one example being a business operating in Oakland exclusively via the Internet without any physical premises in Oakland), or any business operating from a vehicle or other mobile space (one example being a food truck), or any business operating from a temporary physical premises (one example being a pop-up restaurant).
2) "Cash" shall mean United States currency, in the form of both paper Federal Reserve Notes and metal coins.
3) "Professional Services" shall mean any service that requires extended analysis, the exercise of discretion and independent judgment in their performance, and/or the application of an advanced, specialized type of knowledge, expertise, or training customarily acquired either by a prolonged course of study or equivalent experience in the field. Examples of Professional Services include, but are not limited to, services provided by accountants, architects, attorneys, engineers, financial advisers, insurance agents, interior designers, management and other consultants, medical and allied health care professionals such as doctors, dentists, and nurses; and software developers. Licensure by the state or city

[6] https://www.politico.com/states/new-jersey/story/2019/03/18/murphy-signs-bill-banning-most-cashless-stores-in-new-jersey-919093
[7] https://malegislature.gov/laws/generallaws/partiii/titleiv/chapter255d/section10a
[8] https://sfgov.legistar.com/View.ashx?M=F&ID=7255924&GUID=2EE5FAC2-597B-4806-81FB-A3F1F398C0A9
[9] http://phlcouncil.com/wp-content/uploads/2018/10/Cashless-Retail-Prohibition-Bill-Greenlee.pdf
[10] https://www.dailycal.org/2019/12/10/berkeley-city-council-ordinance-requires-businesses-to-accept-cash-as-payment/
[11] https://www.nytimes.com/2020/01/23/nyregion/nyc-cashless-ban.html

does not in itself mean an individual provides Professional Services; for example, a cosmetologist, shoe repair, tailor of clothes, and dry cleaning shall fall under the Brick-and-Mortar Business category.

Section 3. Requirement To Accept Cash.

(a) Except as set forth in Section 4, any Brick-and-Mortar Business offering goods or services, or any person, or entity offering Professional Services, shall not require a buyer to pay using credit or to prohibit Cash as payment in order to purchase the goods or services. A Brick-and-Mortar Business, or any person, or entity offering Professional Services, shall accept Cash when offered by the buyer as payment, so long as that buyer is physically present and not conducting the transaction by telephone, mail, or the Internet.

(b) A Brick-and-Mortar Business or person or entity offering Professional Services shall not:

i. Post signs on the premises that cash payment is not accepted; or
ii. Charge a higher price to customers who pay cash than they would pay using any other form of payment.

Section 4. Exceptions.

a) Suspected Counterfeit Currency. A Brick-and-Mortar Business, or person or entity offering Professional Services may refuse to accept Cash that the person or business reasonably suspects to be counterfeit.

b) Single Transactions Above $5,000. Where a single transaction involves the purchase of one or more goods and/or services, the total price of which (including tax) exceeds $5,000, a Brick-and-Mortar Business, or person or entity offering Professional Services must accept Cash as payment for any amount up to $5,000, but may refuse to accept Cash as payment for the remainder of the amount due. By way of example but not limitation, if a customer purchases an item the total price of which (including tax) is $7,500, the buyer would be entitled to pay up to $5,000 in cash, but the seller would be permitted to require the customer to pay the remaining $2,500 due using some form of payment other than Cash.

c) Renter of Motor Vehicles. Any company in the business of renting motor vehicles is exempt from Section 3, provided that the company accepts a cashier's check or a certified check when offered by a buyer as payment.

~~c)~~d) Large denominations. A Covered Business may refuse to accept Cash in any denomination larger than a twenty dollar note, but shall otherwise accept any combination of Federal Reserve Notes and metal coins in connection with any transaction.

~~d)~~

Commented [PHM2]: Why $5000? Berkeley ordinance exception is $500.

Commented [PHM3]: Doesn't have to be $20, but a large denominations limit will be less burdensome (and less dangerous) to small businesses.

Formatted: Font: (Default) Arial, 12 pt

Formatted: Font: (Default) Arial, 12 pt

Formatted: Font: (Default) Arial, 12 pt

Formatted: Font: (Default) Arial, 12 pt

Section 5. Enforcement.

(a) Cause of Action. Any violation of this Ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance.

(b) No Worker Liability. The obligation to ensure compliance with this Ordinance shall fall only on the business entity (or where a formal entity is not present, the individual owner(s) of the business which are responsible for a policy or practice which violates this Ordinance) or the individual owner(s) of the business. No employee or independent contractor shall be held liable for any violation of this Ordinance.

(c) Violations. Each transaction or attempted transaction whereby Cash is not accepted as required by Section 3 shall constitute a separate violation of this Ordinance.

(d) Penalties. The City of Oakland shall issue an administrative citation for any violation of this Ordinance. The amount of the penalty shall be determined as specified below:

i. For a first violation of this Ordinance, an infraction punishable by a fine not to exceed $100, and not less than $50.
ii. For a second violation of this ordinance within a 12-month period, an infraction punishable by a fine not to exceed $500, and not less than $200.
iii. For a third violation of this ordinance within a 12-month period, and any additional violation within the same period, a misdemeanor punishable by a fine not to exceed $1,000 and not less than $700.
iv. Subject to the specific criteria of this Ordinance, the City Manager shall follow the due process requirements outlined in Oakland Municipal Code sections 1.12.050 (Notification), 1.12.060 (Assessment), and 1.12.080 (Appeal).

(e) Attorney's Fees and Costs. A court shall award a plaintiff who prevails on a cause of action under subsection (a) reasonable attorney's fees and costs.

Section 6. Severability

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 7. Construction

The provisions of this Ordinance are to be construed broadly to effectuate the purposes of this Ordinance.

Section 8. Effective Date

This Ordinance shall take effect immediately upon adoption.

Work in Progress

Oakland Privacy Advisory Commission Workplan 2020-21

Last update 6-24-20

Feb '20	Mar '20	Apr '20	May '20	Jun '20	Jul '20	Aug '20	Sep '20	Oct '20	Nov '20	Dec '20	Jan '21	Feb '21	Mar '21
	OPD Live Stream Camera Policy				OPD Forensic Logic Policy	OPD Automated License Plate Reader Policy	OPD FLIR Boat Policy	OPD ShotSpotter Annual Report	OPD Cellebrite Policy		OPD Hostage Throw Phone Policy	OPD Robot - Land Policy	OPD Cellsite Simulator Policy (conversion only)
					OPD JTTF Annual Report	OPD Body Worn Camera Policy	OPD Remote Camera Policy	OPD FLIR Helicopter Annual Report	OPD Starchaser Annual Report		OPD Live Stream Camera Annual Report	OPD Robot - Water Policy	
OPD Cell-site Simulator Annual Report		OPD Unmanned Aerial Device Policy				OPD FLIR Helicopter Policy (conversion only)	OPD Crime Lab Biometric Equipment Policy	OPD Pen-Link Policy				OPD Cell-Site Simulator Annual Report	
	PAC Annual Report		PAC Privacy Principles Update		PAC Agenda Management		PAC Privacy Principles Update				PAC Privacy Principles Update		PAC Annual Report
						DOT Automated License Plate Reader Annual Report	DOT Dockless Data Sharing Annual Report						
					City Mgr Sanctuary Contracting Annual Report								
		Chinatown Camera Grant Policy											

Department	Color
OPD	
DOT	
PAC	
OFD	
DPW	
City Manager/CPO	
IT	

OPD Surveillance Technologies with Priority List for Review by Oakland Privacy Advisory Commission (PAC)

Item	Description	Use Policy and Impact Report	Priority for bringing to PAC	Estimated Date to Bring Use Policy / Impact Report to PAC	Annual Report
Automated License Plate Recognition (ALPR)	Cameras photograph all seen license plates and use optical recognition software to structure text of license, and populate into license database for tracking	Draft to PAC; needed legal review of data retention schedule	3	Mar-20	n/a
Body Worn Camera (BWC)	Officer BWC manually used to record videos. Officers use docking system to upload to city-maintained server system, w/ plans to upgrade to cloud-storage system.	Draft to PAC; needed legal review of data retention schedule	5	Jun-20	n/a
Cell Site Simulator (Cell Phone Locator)	Machine to mimic cell phone tower signals and determine location of cell phones with predetermined identifiers for specific cell phones or in rescue mode to locate cell phones with unknown identifiers.	Pre-Surveillance Technology ordinance, OPD to revise policy into DGO format	11	Mar-21	Need to bring 2019 annual report to PAC Feb - 2020
Cellphone Data Extraction Equipment	Technology is used to manually download data from seized cell phones.	no	8	Nov-20	n/a
DNA Typing Technology (Crime Lab)	Various technologies used by OPD's crime lab to analyze DNA systems	no	4	Apr-20	n/a
FLIR Camera / Boat	Thermal and video camera in boat	no	7	Sep-20	n/a
FLIR Camera / Helicopter	Thermal and video camera in helicopter.	no	7	Sep-20	n/a
FLIR Camera / Portable Observation Tower	Thermal and video camera in portable manned observation tower.	no		Apr-20	n/a

Commented [SB1]: Confirm this is FLIR tech

Item	Description	Use Policy and Impact Report	Priority for bringing to PAC	Estimated Date to Bring Use Policy / Impact Report to PAC	Annual Report
GPS Tracker	Technology is used to track vehicles in relation to an investigation.	OPD brought policy and report to PAC; PAC recommended both to Council.	n/a	n/a	OPD to bring 2019 Annual Report to PAC by Aug-2020
Gunshot Locater Technology	OPD uses gunshot locater technology (ShotSpotter) to determine time and place as well as other data concerning gunshots.	PAC recommended the Use Policy and Impact Report; approved by City Council	n/a	n/a	Need to bring 2019 annual report to PAC by Oct 2020
Hostage Negotiation Throw Phone	The phone that OPD uses to throw into structures with hostage takers include communication capabilities.	no	9	Jan-21	n/a
Live-Stream Transmitter	Transmitter attached to a video camera to live-stream (not record) to the EOC.	Yes	n/a	n/a	Bring 2020 report in Jan 2021
Remote Mobile (Utility Pole) Camera	Video camera mounted to utility pole that can be moved to different locations, reviewed remotely.	As part of pre-combined policy with live-stream transmitter introduce to PAC in 2019	2	Feb-20	n/a
Remote Audio Telecommunications Monitoring (Pen-Link)	Technology is used to monitor private phone calls.	no	6	Jul-20	n/a
Robot (Land)	The OPD (land) robot for critical incident use includes remote access video capability, to the operator.	no	10	Feb-21	n/a
Robot (Water)	The OPD aquatic robot includes remote access video capability to the operator via cabled connection.	no	10	Feb-21	n/a

Item	Description	Use Policy and Impact Report	Priority for bringing to PAC	Estimated Date to Bring Use Policy / Impact Report to PAC	Annual Report
Thermal Imaging /VIDEO ATTIC Camera	Thermal and Infrared camera on mobile pole	PAC to review if falls under Surveillance Ordinance	n/a	TBD	n/a
Unmanned Aerial Devices (UAV) *	Remote operated aerial device to which video cameras can be mounted	Introduced Jan-20 to PAC	1	Jan-20	Bring 2019 Annual Report to PAC
*** = recently added to list**					

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

The platform software allows authorized personnel to query the system to see if a certain license plate (and associated vehicle) have been photographed. The system will show the geographic location within Oakland for license

[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.

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

There are also documented cases where other LEA contact OPD to make specific queries regarding serious crimes which have occurred in their

[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.

jurisdictions. OPD personnel believe that ALPR has provided critical information for many other felony cases but cannot currently document them.

C. 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.

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, OPD can only develop 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.

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

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 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).

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 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, 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 to investigate criminal activity, as explained in DGO I-12.B-2 "Restriction on Use." 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;

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

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; 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.

All ALPR data downloaded to the server shall be purged in the server at the point of 730 days in the server system, 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.

G. **Data Security***: Steps taken to ensure that adequate security measures are used to safeguard ALPR data collected or generated from unauthorized access or disclosure*

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.

Limited OPD personnel have access to 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. OPD also conducts regular ALPR system audits to ensure the accuracy of ALPR data.

H. **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

I. **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 company EVO as explained above in Section H.

J. **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 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.

K. 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 Mar 20
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 Automated License Plate Reader (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 contains investigatory and/or confidential information, it is not open to public review.

A. Description of the Technology

OPD uses 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 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. ALPRs: These devices include cameras which can be attached to vehicles or fixed objects, 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 ALPRs.

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, and OPD parking personnel 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 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 D – 1 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 days (two years) 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.

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.

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 that contains the 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 requested ALPR data.
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 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: