CITY OF OAKLAND

Privacy Advisory Commission

February 2, 2017 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor

Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Yaman Salahi, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Clint M. Johnson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **Mayoral Representative**: Deirdre Mulligan.*

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

1. 5:00pm: Call to Order, determination of quorum.

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

3. 5:10pm: Presentation on Automated License Plate Readers by Oakland Police Department.

4. 5:20pm: Presentation on Automated License Plate Readers by Cyrus Farivar, Senior Business Editor at Ars Technica.

5. 5:30pm: Presentation on Automated License Plate Readers by Mike Katz-Lacabe, Director of Research at Center for Human Rights and Privacy.

6. 5:40pm: Review and discuss current Oakland Police Department Automated License Plate Reader policy. No action on this item will be taken at this meeting.

7. 6:15pm: Open Forum

8. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

January 5, 2017 5:00 PM
Oakland City Hall
City Council Chambers
1 Frank H. Ogawa Plaza, 3rd Floor
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Yaman Salahi, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Clint M. Johnson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **Mayoral Representative**: Deirdre Mulligan.*

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

1. 5:00pm: Call to Order, determination of quorum

All members were present.

2. 5:05pm: Review and approval of December 1 meeting minutes

The December minutes were approved unanimously.

3. 5:10pm: Presentation on Surveillance Equipment Ordinance by Nuala O'Connor, President and CEO of Center for Democracy and Technology; Question and Answer session.

Ms. O'Connor provided her background in Privacy, first in the private sector and then in key positions within the federal government, in particular, as the Department of Homeland Security's first Chief Privacy Officer. She expressed support for the City's efforts in developing the ordinance and made some specific recommendations for how the City could move forward successfully: First, she recommended that the City adopt Standardized Impact Assessments so they are consistent and easy for the public to understand. Second, she recommended the creation of enhanced internal institutional structures, noting that by creating privacy advocates within the City's structure, they will help evaluate proposals before they ever reach the City Council level. This will help avoid poorly thought out proposals. Third, she recommended that there be further analysis of disparate impacts of the use of surveillance technologies included in annual reports to help identify possible trends in the use of the equipment that could target certain communities.

Chairperson Hofer asked about the current Surveillance Technology Questionnaire that the Commission developed and she recommended simplicity as that is what has been successful in the models that already exist. He also asked about identifying Privacy Officers within each City Department to which she noted that this is a trend at the state and local level but is actually required at the federal level for each department.

Member Oliver noted that Oakland is a city of over 400,000 people and there is a lot of data being gathered. He is concerned that while the government gathers data for different reasons than private businesses, there is the potential to monetize the data government collects for private interests. Ms. O'Connor noted there is a problem with a blurring of the lines in these situations which is why there needs to be a high wall created to prevent that blurring. She went on to add that this is why it's important for government to anonymize or delete the data it collects as quickly as possible.

Member Mulligan asked how the Commission can help agencies to do this work to which Ms. O'Conner noted that constant advocacy for masking people's Personally Identifiable Information (PII) is vital. She referenced the DMV having problems in this arena.

4. 5:20pm: Presentation on Surveillance Equipment Ordinance by Professor Catherine Crump, Co-Director Berkeley Center for Law & Technology; Question and Answer session.

Professor Crump discussed her background working with the ACLU to hold police department's accountable for their use of surveillance technology and her work at UC Berkeley. She applauded the City's effort and noted that the current draft of the ordinance will achieve the vast majority of the goals that it intends to. She noted that the City of Oakland is not unique vis-vis its recent controversy over the Domain Awareness Center (DAC). Seattle faced a similar problem when it purchased a drone without the City Council being aware of it. San Diego quietly rolled out the use of facial recognition software which was also unknown by the elected leadership. She went on to note that ordinances are very helpful in setting a standard and requiring an assessment of the equipment and how it's used.

Chairperson Hofer, asked about problems that are created when there is no public process citing a recent article about the DAC controversy. Professor Crump noted that it's not enough for City Council's to just be told about what is being purchased because that does not signal enough of a need for scrutiny around the topic. This is especially true when grant money is involved, often when money is being offered to cash-strapped cities, there is less scrutiny. This is why the ordinance gets it right by requiring a process before money is accepted.

Member Mulligan asked about the use of federal funds and how that impacts the use of technology. Professor Crump pointed out that the federal grants don't require that local governments conduct impact assessment son the technology that they purchase with the federal grant dollars but do require themselves to conduct such assessments.

Member Karamooz asked about the federal government requiring access to data that is collected locally. Professor crump noted this is most common with prescription drug use databases and an example of why it is a good policy for local governments to not hold on to data—that way it is not available for collection.

5. 5:30pm: Discuss and take possible action on a Surveillance Equipment Ordinance.

There were nine public speakers on this item:

Christina Singha from the Asian Law Caucus spoke in support of the ordinance noting that we live in an age where there is a huge amount of digital data about all of us. She has seen many clients express fear with the new administration and their overtures; people are afraid to speak up at work, participate in rallies, etc.

Tessa D'Arcangalew is an organizer with the ACLU and stated her excitement that Oakland is taking a leadership role on this issue.

Brian Geiser also supports the ordinance and also asked about section 8-1 of the DAC and FLIR Policies noting that we are due for some annual, reports soon on those pieces of equipment.

Camille Ochoa with the Electronic Frontier Foundation suggests that Standard operating Procedures be developed within the ordinance for City departments that require them to wait for permission to move forward with any grant application.

Mike Katz-Lacabe lives in San Leandro and described how his city was using LPR technology for 3 years before the City Council was aware of it and they took his picture hundreds of times tracking where he went. He also noted that stingray technology was being used in Oakland for many years before leaders were aware.

Susan Harmon applauded the efforts and also suggested the City make it nationally known once it is passed.

Sameen Usman with the Council on American-Islamic Relations noted that many people are concerned about the use of technology—people are being tracked as to where they pray, eat, congregate, and it has strained the relationship the community has with its government. He cited New York City as an example of where this is very profound.

Tracey Rosenberg with the Media Alliance spoke about how far Oakland had come since the DAC debate and applauded the progress. She noted a lot can go wrong with the use of surveillance technology and the cost/benefit ratio can be severely out of balance.

Allan Brill spoke about his past work on the DAC Committee and praised the Commission for its current work. He also talked about his work in his own neighborhood on crime prevention issues and the need to build trust in the community as a better prevention tool than surveilling people and destroying trust.

The Commission unanimously voted to recommend the ordinance to the City Council.

Joe DeVries explained that now that the Commission has formally acted, he will draft and submit the Council Staff report and have the various departments review the ordinance and that it would then be scheduled for the Public Safety Committee in several weeks.

6. 6:15pm: Presentation by Greg Minor on Illegal Dumping Cameras Project. Discuss and take possible action.

Greg Minor presented the Surveillance Technology questionnaire and received several questions about the functionality of the cameras and the program:

Can the cameras can be moved from one spot to another –yes that is the plan. Is there remote access to the footage? Yes. What is the data storage length? As yet to be determined—if no dumping occurs then the goal is to delete it within 72 hours, if dumping is captured it would be kept as evidence. Have other jurisdictions used these successfully? Unknown-the City has not conducted extensive research on other jurisdiction's effectiveness. Is this an enforcement tactic because OPD cannot respond? The penalties for dumping will mostly be administrative, not criminal because criminal cases are too burdensome.

Member Karamooz noted that he does not see how the program will be successful in reducing illegal dumping which is a much bigger problem. He noted the cost of disposing material at the dump and public education are likely far more impactful. Greg Minor noted that there are several efforts underway in Oakland to reduce dumping and the cameras are just one small component.

Chairperson Hofer noted that State Senate Bill 34 which is in regard to License Plate Readers will apply to this program and will need to be considered.

There was one public speaker: Brian Geiser noted that it is very difficult for renters (who don't have bulky pick-up) to dispose of bigger items and that many don't have the means to transport things to the dump or to pay the dump fees.

7. 6:45pm: Open Forum

There were no open forum speakers.

8. 7:00pm: Adjournment

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Document Overview

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

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

SIR Section	STAQ Section
a. Description	1. Technology Solution Overview
b. Purpose	1. Technology Solution Overview
c. Location	4. Location(s) of Deployment and Data Storage
d. Impact	5. Protecting Civil Rights and Liberties
e. Data Sources	2. Surveillance Technology Detail
f. Data Security	3. Authorized Users
g. Fiscal Cost	6. Initial and On-going Costs of Technology
h. Third Party Dependence	2. Surveillance Technology Detail
i. Alternatives	1. Technology Solution Overview
j. Track Record	1. Technology Solution Overview

Questionnaire

Question		Response	Supporting Documentation
1	**Why: Technology Solution Overview**		
1.1	What is the function of the technology as described by the manufacturer?	Captures license plates and the location of the license plates. The technology converts the data into a readable format and compares it to a database supplied daily from the California Department of Justice as well as other information provided by the Oakland Police Department.	Manufacturer's supplied manual
1.2	What is the specific problem this equipment or use will resolve?	To help reduce crime.	

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Question		Response	Supporting Documentation
1.3	How will success be demonstrated?	Successful automated license plate hits and manual database queries against the LPR database that produce a match leading to the recovery of wanted vehicles and persons.	
1.4	What is the success rate for this equipment or use?	Unknown	
1.5	What non-surveillance alternatives were considered?	There were no alternatives considered. One alternative might be having OPD staff members drive around or walk around and take photos of license plates and then later checking the license plates against the same databases used for the ALPR.	
1.6	Why were the non-surveillance alternatives not pursued?	None were considered. However, manually checking license plates (described above) would be incredibly inefficient and much, much more costly.	
2	**What: Surveillance Technology Detail**		
2.1	What equipment capabilities do you intend to use?	Plate capturing camera capable of recording 60fps. GPS location. OCR (optical character recognition) hardware/software unit.	
2.2	What other equipment capabilities are possible?	Install additional cameras onto the vehicle. Current configuration is 2 cameras.	
2.3	What safeguards will be implemented to ensure that unauthorized capabilities or uses will not be implemented?	Policy and restricted use only to authorized users that have access to the backend database for license plate lookup. Client software also needs to be installed onto a desktop. Only a limited amount of vehicles have LPR capturing hardware installed.	
2.4	What information can the technology capture?	Picture of the vehicles license plate and vehicle.	
2.5	What information can the technology store?	Pictures, GPS location data, camera and user identifying data.	
2.6	How long will information be retained?	Six months, per policy.	Policy 403
2.7	Will the data gathered and stored by handled by a third party on an on-going basis	The database is stored and managed in-house. Several third party vendors receive LPR data for third party crime analysis.	
2.8	How will you ensure that data is not retained for longer than allowed?	By policy and running of a database script to purge data that resides longer than the policy allows for.	Policy 403

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Question		Response	Supporting Documentation
3	**Who: Authorized Users**		
3.1	Who is authorized to access the technology?	Per policy: designated sergeants, officers, police service technicians, and parking enforcement personnel and other authorized users.	Policy 403
3.2	How are users authenticated?	Users are manually added to the LPR user list.	
3.3	How is access to the technology audited?	Per policy: ALPR system audits shall be conducted on a regular basis by the Bureau of Services.	Policy 403
3.4	What is the mechanism for monitoring compliance with access policies?	Regular audits by Bureau of Services.	Policy 403
4	**Where: Location(s) of deployment and data storage**		
4.1	Where will the technology be deployed within the community?	At any location – some based on need. The technology is mounted on OPD patrol vehicles.	
4.2	What is the basis for selecting these locations?	A location may be selected due to a community or department concern.	
4.3	What are the crime statistics for each proposed deployment location?	The LPR is deployed on vehicles driven by officers throughout the City 365 days a year, seven days a week. As crime trends and analysis dictate additional resources, LPR equipped vehicles can be redirected to selected area's or "hot spots" throughout the City.	
4.4	Where will the information be stored (on-site, remote, cloud)?	The information is stored on a local database server.	
4.5	What are the safeguards, monitors, and audits to ensure security of information at storage (at rest) and when accessed (transmission)?		
5	**How: Protecting Civil Rights and Liberties**		
5.1	Could the technology or use collect information related to race, citizenship status, gender, age, socioeconomic level, reproductive choices, or	This is incredibly unlikely. While it is possible for an ALPR device to capture an individual's photo, the camera is actually pointed toward license plates.	

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Question		Response	Supporting Documentation
	sexual orientation? If so, what safeguards are in place to limit such collection?		
5.2	Will the technology be deployed in communities with minority residents, non-citizens, low-income residents, or any group historically vulnerable to disproportionate civil liberties violations?	Yes. Oakland is a very diverse city that has many minority residents as well as non-citizen residents, low-income residents, and other residents that are historically vulnerable to disproportionate civil liberties violations.	
5.3	Could the technology be used on groups, public gatherings, or crowds and thus have an effect on First Amendment activities such as protests? If so, what safeguards are in place to limit this?	This would be difficult. Most protests take place on foot in the City of Oakland. Most gatherings also involve persons on foot. It is rare that vehicles are associated with crowds, groups, public gatherings, and protests. There is no therefore no applicable safeguard.	
5.4	Does the technology collect and retain information about individuals not suspected of wrongdoing? If so, how could such information impact their right to privacy?	Yes, the technology collects and retains information about vehicles that are operated and/or owned by many individuals who are not suspected of wrongdoing. There is no impact to privacy, as there is no actionable data if the individual is not suspected of wrongdoing.	
6	**How Much: Initial and On-going Costs of Technology**		
6.1	What are the initial costs, including acquisition, infrastructure upgrades, licensing, software, training, and hiring of personnel?		
6.2	What are the ongoing costs, including measures to secure data and data storage?		
6.3	What is the funding source for the proposed acquisition or use?		

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Question		Response	Supporting Documentation
6.4	Are there other tools capable of furthering the identified purpose that the community may wish to spend these funds on (e.g., community-based policing, improved lighting)?	Yes, there are other tools the community may wish to spend funding on. However, the return on investment for any other tool would be substantially smaller than for ALPR.	

Automated License Plate Readers (ALPRs)

430.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

430.2 POLICY

The policy of the Oakland Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

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

430.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Oakland Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Bureau of Services Deputy Chief. The Deputy Chief will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

430.3.1 ALPR ADMINISTRATOR

The Bureau of Services Deputy Chief shall be the administrator of ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to Civil Code §§ 1798.90.51 through 1798.90.53:

(a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.

(b) Training requirements for authorized users.

(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

(d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.

(e) The title of the current designee overseeing the ALPR operation.

(f) Working with the Custodian of Records on the retention and destruction of ALPR data.

(g) Ensuring this policy and related procedures are conspicuously posted on the department's website.

430.4 ALPR USERS

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

430.5 PURPOSES FOR ACCESSING AND USING ALPR INFORMATION

Use of an ALPR is restricted to the purposes outlined below. The title of the official custodian of the ALPR system, responsible for implementing this section, is the ALPR Coordinator.

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).

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

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

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

(d) An ALPR shall only be used for official law enforcement business.

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

(f) If practicable, agency personnel should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

(g) 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.

430.6 DATA COLLECTION AND RETENTION

The Bureau of Services Deputy Chief is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server shall be stored for six months. Thereafter, ALPR data shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a

criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data shall be downloaded from the server onto portable media and booked into evidence.

430.7 SYSTEM MONITORING AND SECURITY

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

(a) 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).

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

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

For security or data breaches, see the Records Release and Maintenance Policy.

430.8 AGENCY MONITORING AND CONTROLS

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

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

(a) The number of times the ALPR technology was used.
(b) A list of agencies other than the Oakland Police Department that were authorized to use the equipment.
(c) A list of agencies other than the Oakland Police Department that received information from use of the equipment.
(d) Information concerning any violation of this policy.
(e) Total costs for maintenance, licensing and training, if any.
(f) 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.

430.9 RELEASING OR SHARING ALPR DATA

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

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Bureau of Services Deputy Chief or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55) and per any interagency agreements.

430.10 TRAINING

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

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

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

Training updates are required annually.