



Privacy Advisory Commission
January 5, 2017 5:00 PM
Oakland City Hall
City Council Chambers
1 Frank H. Ogawa Plaza, 3rd 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 December 1 meeting minutes
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.
4. 5:20pm: Presentation on Surveillance Equipment Ordinance by Professor Catherine Crump, Co-Director Berkeley Center for Law & Technology; Question and Answer session.
5. 5:30pm: Discuss and take possible action on a Surveillance Equipment Ordinance.
6. 6:15pm: Presentation by Greg Minor on Illegal Dumping Cameras Project. Discuss and take possible action.
7. 6:45pm: Open Forum
8. 7:00pm: Adjournment



Privacy Advisory Commission
Special Meeting
December 1, 2016 5:15 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st 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.*

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

All members were present.

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

The November Minutes were approved unanimously.

3. 5:10pm: Discuss and take possible action on a Streetline/Parking Management Strategy Report.

Michael Ford, the City's Parking Manager made a request that the Commission support a modified resolution, based on the new information provided (Including the Surveillance Technology Questionnaire) that will go before the City Council. The new resolution clarifies short term uses of cameras, and requires staff to return to the Privacy Commission annually to report on the Streetline Parking Program.

The Streetline Team was also available to answer the Commission's questions.

Commissioners asked several questions about the program as summarized below:

Why would License Plate Reader Technology help the Streetline system? At this point it is not the intent to use LPR info but it could provide for a more accurate car count on each block as LPR is another data set that can be used. Similar to the temporary cameras that will be placed on streets; there is no desire to capture personal data—Streetline can use the total car count but has no use for the individual car's identity..

Will the implementation of the Parking App cause it to be more difficult to park for people who do not have the App? No, the City's parking meters will not change in any way for non-app users.

Is Streetline required to remove the equipment after three years if the City decides not to keep using the system? Yes.

What is the benefit to Streetline to provide \$1 Million in services to the City for free? Streetline hopes to expand to many cities and sell its data and application to car navigation and mapping companies so it will be built into cars in the future.

Do you need a smart phone to get the parking availability information? No, it is available on the website and the City could post it on its website as well.

Can the resolution before the City Council be modified to include limits on the collection of personally identifiable information (PII)? Yes, and it can require that changes in Streetline's Privacy Policy require an alert to the City and a review by the Privacy Advisory Commission.

What PII can Streetline currently get from users of the app? Can they get people's individual contact information? No, only if people proactively provide that info while giving feedback to the company about its products.

Who covers the cost of removing the sensors from the ground? Typically, the sensors remain until the City repaves the street and they get ground up during that process. Once the networking equipment is removed for the city, the sensors are essentially useless.

In a natural disaster could the LPR data be used to locate a car associated with a missing person? No, even if the City shared LPR data with Streetline, Streetline would only be receiving the car count for a particular block so no personal data would be available.

There was one Public Speaker on the item: Brian Geyser noted that the modified resolution work was admirable but he still has concerns about the report not having enough information and believes the Commission should express its concerns about the program. He also raised a concern about the 1500 sensors that would be installed throughout the City.

Modifications were made to the Resolution that included: signage indicating the use of the temporary cameras that would be installed, striking references to the use of LPR data/technology, and requiring notification and a return to the commission for any substantial changes to Streetline's Privacy Policies or User Agreements that change the collection of PII data from individual users.

The full text of the modified resolution is below:

RESOLUTION AUTHORIZING THE CITY ADMINISTRATOR OR DESIGNEE TO NEGOTIATE, FINALIZE AND EXECUTE A NON-EXCLUSIVE AGREEMENT WITH STREETLINE INC. FOR A SMART PARKING SYSTEM AT NO DIRECT COST TO THE CITY FOR A TERM OF THREE YEARS

WHEREAS, the Downtown Oakland Parking Management Report recommends that the City improve the management of City-owned parking supply by, among other things, improving parking monitoring and enforcement with integrated "smart" meters, off-street parking Access and Revenue Control Systems; evaluating emerging parking occupancy sensor

technologies (in-ground and/or on-meter) and consider deploying them if and when current reliability, accuracy and cost problems are overcome; and developing real-time wayfinding systems; and

WHEREAS, Streetline Inc. has developed a smart parking system that promises to deliver consumer facing parking applications and parking management information; and

WHEREAS, parking management systems are rapidly evolving: smart meters, vehicle detection systems, machine learning, smart phone applications, wireless networks and other components are converging to create increasingly sophisticated “smart parking” systems; and

WHEREAS, business models and public-private partnerships are evolving to support those systems; and

WHEREAS, Streetline Inc. is proposing to invest in the installation and operation of a smart parking system in Oakland in the amount of approximately one million dollars in infrastructure and nearly half a million in operating costs over a three-year period to bring its smart parking solution to as many as fifteen hundred city block faces, with no direct cost to the City; and

WHEREAS, Staff is requesting authorization to negotiate and enter into a non-exclusive agreement with Streetline that would commit the City to certain responsibilities like the following proposed by Streetline:

- Securing all required permissions and permits granting installation permission to Streetline at no cost to Streetline
- Arranging for street closures and applicable sign postings
- Arranging for continuous power for gateway(s) through an acceptable source (120 or 240v, 50 or 60 Hz) at a location (or locations) in accordance with Network Plan
- Cooperating with Streetline in establishing metrics and providing necessary benchmark data for Streetline’s Executive Summary report
- Using best efforts to notify Streetline 10 business days prior to scheduled road paving or slurring activity of areas with sensors
- Promptly notifying Streetline of any power interruption to gateways or removal of repeaters or gateways by Customer’s maintenance crews
- Establishing a plan for active marketing, advertising and promotion of the Smart Parking system and the Parker App with the goal of achieving 10,000 local downloads of the Parker App
- To the extent available, providing machine readable policy information to Streetline
- To the extent available, providing real-time and historical payment information for parking; and

WHEREAS, Oakland Public Works and Information Technology staff have reviewed the Streetline proposal and assessed the technical merits and possible obstacles of the installation and operation of the system; and

WHEREAS, City staff agree that the design of the Streetline system has merit and that the technical obstacles to installing and operating the system are manageable; and

WHEREAS, in exchange and consideration for its installation and operation of the smart parking system, Streetline is proposing that it have the right to use the data that its system generates for its own commercial uses; and

WHEREAS, those uses and other aspects of Streetline’s proposal have been reviewed by the City’s Privacy Advisory Commission, which resulted in substantial changes to that proposal; and

WHEREAS, the implementation of this pilot project will be closely aligned with and support the MTC-funded Parking and Mobility Management Initiative; and

WHEREAS, Streetline Inc. has shared its proposal with Oakland community groups including Business Improvement Districts; and

WHEREAS, the City Council finds that the services provided pursuant to the agreement authorized hereunder are of a professional, scientific, or technical nature and are temporary in nature; and

WHEREAS, the City Council finds that this contract shall not result in the loss of employment or salary by any person having permanent status in the competitive service; now, therefore, be it

RESOLVED: That the Council hereby authorizes the City Administrator or Designee to negotiate, finalize and execute an agreement with Streetline Inc. for a term of three years the installation, operation, maintenance and, if necessary, removal of its smart parking system at no direct cost to the City; and be it

FURTHER RESOLVED: That said agreement may include permissions granted to Streetline, such as the temporary encumbrance and obstruction of the right-of-way, and obligate the City in ways that require no cash outlays to Streetline, such as providing data and supporting Streetline's marketing efforts; and be it

FURTHER RESOLVED: That any such data provided by the City to Streetline be free of any identifying information; and be it

FURTHER RESOLVED: That any use of cameras by Streetline be accompanied by signage that explains their use and purpose to the public and that each installation be removed after a maximum of two weeks; and be it

FURTHER RESOLVED: That staff return to the Privacy Advisory Commission once a year for the three-year duration of the pilot program to present results and incorporate those results and the Commission's comments into an informational report for Council; and be it

FURTHER RESOLVED: That said agreement between the City of Oakland and Streetline shall require Streetline to notify the City of Oakland and the Privacy Advisory Commission of material changes to its end year user license agreements or privacy policies which change the scope of data gathered from individual users or the use of that data; and be it

FURTHER RESOLVED: That the City Attorney shall review and approve the proposed contract as to form and legality, and copies of the agreement(s) shall be filed with the Office of the City Clerk without returning to Council.

4. 5:30pm: Discuss and take possible action on a Surveillance Equipment Ordinance.

Chairperson Hofer introduced modified language that addresses the City staff concern about the timing of applying for grants for surveillance technology while still allowing for public input.

Vice Chair Johnson introduced modified language for the second finding in the Ordinance as he felt the current language was too negative. The Commission supported the insertion of the new finding however also voted to retain the original language as well.

The Commission discussed conducting a public hearing on the draft ordinance to solicit more input and decided to schedule the hearing as part of the January Meeting, during which some key experts will be scheduled to present and the public will be asked to provide further information before submitting the ordinance to the City Council.

5. 6:45pm: Open Forum

There were three public speakers under Open Forum:

Ken Pratt thinks the commission should take more time to discuss the Streetline Parking Program before supporting it.

Brian Geyser spoke favorably about how the public comments are received at Commission meetings.

J.P. Masser raised concern about waiting until January to approve the ordinance to send to the City Council. He suggested in these changing times there is a renewed sense of urgency.

6. 7:00pm: Adjournment

The meeting adjourned at 7:05pm.

OAKLAND CITY COUNCIL

ORDINANCE NO. _____ C.M.S.

INTRODUCED BY COUNCILMEMBER [IF APPLICABLE]

THE SURVEILLANCE AND COMMUNITY SAFETY ORDINANCE

Whereas, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology; and

Whereas, the City Council finds that, while surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

Whereas, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes, while acknowledging the significance of protecting the privacy of citizens; and

Whereas, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

Whereas, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

Whereas, the City Council finds that any and all decisions regarding if and how surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight; and

Whereas, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed; and

Whereas, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to; now, therefore

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

Section 1. Title

This ordinance shall be known as the Surveillance & Community Safety Ordinance.

Section 2. City Council Approval Requirement

- 1) A City entity shall notify the Chair of the Privacy Advisory Commission prior to the entity:
 - a) Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
 - b) Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

Upon notification by the entity, the Chair shall place the item on the agenda at the next meeting for discussion and possible action. At this meeting, the entity shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action the entity intends to take. The Privacy Advisory Commission may vote its approval to proceed, object to the proposal, recommend that the entity modify its proposal, or take no action. Failure by the Privacy Advisory Commission to act shall not prohibit the entity from proceeding. Opposition to the action by the Privacy Advisory Commission shall not prohibit the entity from proceeding. The City entity is still bound by subsection (2) regardless of the action taken by the Privacy Advisory Commission under this subsection.

- 2) A City entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public hearing prior to any of the following:
 - a) Accepting state or federal funds or in-kind or other donations for surveillance technology;
 - b) Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
 - c) Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner or in a location not previously approved by the City Council; or
 - d) Entering into an agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

- 3) A City entity must obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (2)(a)-(d).

Section 3. Information Required

1) The City entity seeking approval under Section 2 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.

- a) Prior to seeking City Council approval under Section 2, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting.
- b) The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose modifications to the City entity and/or City Council in writing.
- c) Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the City entity to proceed to the City Council for approval of the item.

2) After receiving the recommendation of the Privacy Advisory Commission, the City Council shall provide the public notice that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.

3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Section 4. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 2, subsection (1) or Section 5 of this ordinance after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 5. Compliance for Existing Surveillance Technology

Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy for each surveillance technology, in compliance with Section 3 (1) (a-c).

- a) Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, each City entity shall present to the Privacy Advisory Commission a list of surveillance technology already possessed or used by the City entity.
- b) The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
- c) Within sixty (60) days of the Privacy Advisory Commission's action in b), each City entity shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter every month until the list is exhausted.
- d) Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following City Council Approval

1) A City entity which obtained approval for the use of surveillance technology must submit a written Surveillance Report for each such surveillance technology to the City Council within twelve (12) months of City Council approval and annually thereafter on or before November 1.

- a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the Privacy Advisory Commission for its review.
- b) The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the Surveillance Use Policy that will resolve the concerns.

2) Based upon information provided in the Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall determine whether the requirements of Section 4 are still satisfied. If the requirements of Section 4 are not satisfied, the City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.

3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:

- a) A summary of all requests for City Council approval pursuant to Section 2 or Section 5 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval; and
- b) All Surveillance Reports submitted.

Section 7. Definitions

The following definitions apply to this Ordinance:

- 1) “Surveillance Report” means a written report concerning a specific surveillance technology that includes all the following:
- a) A description of how the surveillance technology was used, including the quantity of data gathered or analyzed by the technology;
 - b) Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
 - c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
 - d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau;
 - e) A summary of community complaints or concerns about the surveillance technology, and an analysis of any discriminatory uses of the technology and effects on the public’s civil rights and civil liberties, including but not limited to those guaranteed by the California and Federal Constitutions;
 - f) The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;
 - g) Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - h) Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - i) Statistics and information about public records act requests, including response rates;

- j) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
 - k) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
- 2) “City entity” means any department, bureau, division, or unit of the City of Oakland.
- 3) “Surveillance technology” means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.
- a) “Surveillance technology” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 7(3): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (f) municipal agency databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
- 4) “Surveillance Impact Report” means a publicly-released written report including at a minimum the following:
- a) **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - b) **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
 - c) **Location:** The location(s) it may be deployed and crime statistics for any location(s);
 - d) **Impact:** An assessment identifying any potential impact on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm. In addition, identify specific, affirmative

measures that will be implemented to safeguard the public from each such impacts;

- e) **Data Sources:** A list of all sources of data to be collected, analyzed, or processed by the surveillance technology, including “open source” data;
- f) **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
- 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;
- h) **Third-Party Dependence:** Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
- i) **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
- j) **Track Record:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

5) “Surveillance Use Policy” means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:

- a) **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
- b) **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;
- c) **Data Collection:** The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including “open source” data;
- d) **Data Access:** The individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- e) **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
- f) **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

- g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
- h) **Third-Party Data Sharing:** If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials;
- j) **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
- k) **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Section 8. Enforcement

1) Any violation of Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR Surveillance Use Policy adopted October 6, 2015), Resolution No. xxxxx (Cell Site Simulator Use Policy adopted xxxxxx, 2017), this Ordinance, or of a Surveillance Use Policy promulgated under 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. An action instituted under this paragraph shall be brought against the respective City agency, the City of Oakland, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third-party with possession, custody, or control of data subject to this Ordinance.

2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars (\$1,000) or one hundred dollars (\$100) per day for each day of violation, whichever is greater) and punitive damages.

3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) or (2).

- 4) In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding one thousand dollars (\$1,000) per violation.

Section 9. Secrecy of Surveillance Technology

It shall be unlawful for the City of Oakland or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Ordinance shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Ordinance.

Section 10. Whistleblower Protections

- 1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or civil or criminal liability, because:
 - a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
 - b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.
- 2) It shall be grounds for disciplinary action for a municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Ordinance.
- 3) Any employee or applicant who is injured by a violation of Section 10 may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

Section 11. 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 12. Construction

The provisions of this Ordinance, including the terms defined in Section 7, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 13. Effective Date

This Ordinance shall take effect on [DATE].

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL WASHINGTON, GALLO, GUILLÉN, KALB, KAPLAN, REID AND
PRESIDENT GIBSON MCELHANEY

NOES –

ABSENT –

ABSTENTION –

ATTEST:

LATONDA SIMMONS
City Clerk and Clerk of the Council of the
City of Oakland, California

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?		
1.2	What is the specific problem this equipment or use will resolve?		
1.3	How will success be demonstrated?		
1.4	What is the success rate		

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

Question		Response	Supporting Documentation
	for this equipment or use?		
1.5	What non-surveillance alternatives were considered?		
1.6	Why were the non-surveillance alternatives not pursued?		
2	What: Surveillance Technology Detail		
2.1	What equipment capabilities do you intend to use?		
2.2	What other equipment capabilities are possible?		
2.3	What safeguards will be implemented to ensure that unauthorized capabilities or uses will not be implemented?		
2.4	What information can the technology capture?		
2.5	What information can the technology store?		
2.6	How long will information be retained?		
2.7	Will the data gathered and stored be handled by a third party on an on-going basis		
2.8	How will you ensure that data is not retained for longer than allowed?		
3	Who: Authorized Users		
3.1	Who is authorized to access the technology?		
3.2	How are users authenticated?		
3.3	How is access to the technology audited?		
3.4	What is the mechanism for monitoring compliance with access		

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

Question		Response	Supporting Documentation
	policies?		
4	Where: Location(s) of deployment and data storage		
4.1	Where will the technology be deployed within the community?		
4.2	What is the basis for selecting these locations?		
4.3	What are the crime statistics for each proposed deployment location?		
4.4	Where will the information be stored (on-site, remote, cloud)?		
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 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?		
5.3	Could the technology be used on groups, public		

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

Question		Response	Supporting Documentation
	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?		
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?		
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?		
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)?		

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 ?	One camera captures video and the license plate reader camera (LPR) takes an image of the license plate of cars passing through the designated location.	
1.2	What is the specific problem this	Documenting illegal dumping violators for criminal or administrative enforcement actions. The cameras will be located in areas where	

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

Question		Response	Supporting Documentation
	equipment or use will resolve?	there typically are few/zero people around to observe/document the illegal dumping, so the cameras will allow the City to hold illegal dumpers accountable by providing much needed evidence the City would not otherwise have. In particular, the LPR helps identify the car owner, allowing the City to identify who is responsible.	
1. 3	How will success be demonstrated ?	Capturing illegal dumpers in the act and identifying the license plates of vehicles involved.	
1. 4	What is the success rate for this equipment or use?	Once tuned, the plate read success is 85-95 percent. Things like license plate rings can give a false read. Similarly, plate covers or material placed over license plates can cause misreads. To ensure accuracy of license plate identification by LPR, all images are human verified post incident.	
1. 5	What non-surveillance alternatives were considered?	<p>The City has been and currently is pursuing a number of non-surveillance alternatives to address illegal dumping in Oakland.</p> <ul style="list-style-type: none"> • The City's Adopt a Spot program supports individuals, neighborhood groups, civic organizations, and businesses in ongoing cleaning and greening of parks, creeks, shorelines, storm drains, streets, trails, medians and other public spaces. Volunteers have adopted hundreds of sites around Oakland. Public Works provides tool loans, debris collection services, and technical assistance. • Similarly, Oakland Public Works coordinates two city-wide volunteer events each year, Creek to Bay Day and Earth Day, involving thousands of participants. • Single family-homes and multi-family housing receive a free annual bulky waste pick up via Waste Management. • The City provides quarterly amnesty days where bulky-waste can be dropped off for free at Davis Transfer 	http://www2.oaklandnet.com/government/o/PWA/o/FE/s/ID/OAK024735 https://oakland.legistar.com/LegislationDetail.aspx?ID=2892081&GUID=3B7F356E-D067-43C3-B433-00965FBA5BE7&Options=&Search=

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

Question		Response	Supporting Documentation
		<p>Station.</p> <ul style="list-style-type: none"> At an annual cost of \$5.5 million, Oakland Public Works Keep Oakland Clean and Beautiful (KOCB) Division removes illegal dumping debris from the public right of way. Illegal dumping service requests have increased 100% in past five years, from 14,083 piles of illegally dumped material in FY 2010-2011 to 29,370 piles of illegally dumped material. The City's current enforcement efforts rely on reports by citizens; while some reports include pictures/videos, many do not which limits the city's ability to hold illegal dumpers accountable (via administrative or criminal proceedings) When OPD has tried illegal dumping stakeouts they have been unsuccessful in observing illegal dumping and this time could have been spent by law enforcement responding to other calls/assignments 	
1.6	Why were the non-surveillance alternatives not pursued?	Non-surveillance alternatives are being pursued concurrently. See above.	
2	What: Surveillance Technology Detail		
2.1	What equipment capabilities do you intend to use?	<ul style="list-style-type: none"> One camera to video record activity at illegal dumping hotspots and one LPR to document license plates of vehicles passing by. If an illegal dumping incident is recorded, that video clip and license plate information will be saved and used as part of an administrative or criminal case against the suspected illegal dumper. 	
2.2	What other equipment capabilities are possible?	<ul style="list-style-type: none"> It is possible to set specific "triggers" that notify when someone is illegally dumping, eg lingering for prolonged period at illegal dumping hotspot. This 	

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

Question		Response	Supporting Documentation
		trigger is difficult to determine at this point.	
2. 3	What safeguards will be implemented to ensure that unauthorized capabilities or uses will not be implemented?	Network security and local login database prevents unauthorized access to the system. Further, the OnSSI Base server the LRP Zamir software records what user accessed the system and when, what cameras were accessed and when, and it keeps what video was exported or manipulated. It will also document system configuration changes.	
2. 4	What information can the technology capture?	Video within certain range of camera and license plates of vehicle passing by LPR.	
2. 5	What information can the technology store?	The video and license plate information can be stored.	
2. 6	How long will information be retained?	During initial system testing phase we have 7 days of video and 90 days of plate images. However, on final turn over of the system 30 days of recording video and 90 days of plates may be stored.	
2. 7	Will the data gathered and stored by handled by a third party on an on-going basis	Data gathering/storage will be handled by City Administrator's Office, though, contractor AMS.net will have access for support services.	
2. 8	How will you ensure that data is not retained for longer than allowed?	The thresholds in the system ensure video grooming of data at determined point. Once the time has been reached the system self-grooms the video and the LPR software will delete the plate hits.	
3	Who: Authorized Users		
3. 1	Who is authorized to	Nuisance Abatement Division and contractor, AMS.net.	

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

Question		Response	Supporting Documentation
	access the technology?		
3.2	How are users authenticated?	Local Database of the OnSSI and Zamir software.	
3.3	How is access to the technology audited?	Software auditing is turned on in the OnSSI software. Logging is on in the Zamir LPR software.	
3.4	What is the mechanism for monitoring compliance with access policies?	Policy can be established in concert with privacy commission.	
4	Where: Location(s) of deployment and data storage		
4.1	Where will the technology be deployed within the community?	Cameras and LPRs will be utilized at illegal dumping hotspots, e.g. freeway underpasses, industrial areas, etc. Initial pilot phase will consist of four sites; more sites to be added depending on success of program and funding availability.	
4.2	What is the basis for selecting these locations?	Combination of following factors: <ul style="list-style-type: none"> • High amount of illegal dumping at location. • Ability to target illegal dumpers at location given camera positioning. • Power source availability. • Sufficient server connectivity so data can be sent back to City. 	
4.3	What are the crime statistics for each proposed deployment location?	Very high with respect to illegal dumping (which is a violation of both OMC and penal code).	
4.4	Where will the information be stored (on-	The information is stored on the OnSSI recorder at 150 LJW building on the 8 th floor server room.	

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

Question		Response	Supporting Documentation
	site, remote, cloud)?		
4. 5	What are the safeguards, monitors, and audits to ensure security of information at storage (at rest) and when accessed (transmission) ?	On the OnSSI Base server and in the LRP Zamir software, auditing has been enabled. It records what user accessed the system and when. It tells what cameras were accessed and when. It keeps what video was exported or manipulated. It will also document system configuration changes.	
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 sexual orientation? If so, what safeguards are in place to limit such collection?	No, though the video captured may depict the appearance of individuals recorded.	
5. 2	Will the technology be deployed in communities with minority residents, non-citizens, low-income	The technology will be used in illegal dumping hotspots, which can overlap with low-income areas.	Map of illegal dumping hotspot areas can be found here: https://oakland.legistar.com/LegislationDetail.aspx?ID=2892081&GUID=3B7F356E-D067-43C3-B433-00965FBA5BE7&Options=&Search=

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

Question		Response	Supporting Documentation
	residents, or any group historically vulnerable to disproportionate civil liberties violations?		ch =
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?	No. The cameras will be located in illegal dumping hotspots where there are typically no individuals let alone public gatherings present.	
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?	As mentioned above in 2.6, the technology retains data until determined point.	
6	How Much: Initial and On-going Costs of Technology		
6.1	What are the initial costs, including	<ul style="list-style-type: none"> City Council has allocated \$100,000 no longer needed to operate a mattress 	

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

Question		Response	Supporting Documentation
	acquisition, infrastructure upgrades, licensing, software, training, and hiring of personnel?	<p>reimbursement program towards this illegal dumping camera pilot project. This amount is sufficient for all the software and licensing to install a server at the City to receive information and four sites with high-quality cameras and LPRs.</p> <ul style="list-style-type: none"> • Adding each additional site should be around \$5-10,000 as the cost of cameras decrease. • There is no funding to support hiring of personnel. 	
6.2	What are the ongoing costs, including measures to secure data and data storage?	Currently no ongoing costs in regards to data or the storage of this data. It is local and not cloud based or at a Co-Location facility.	
6.3	What is the funding source for the proposed acquisition or use?	See above.	
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)?	<p>No.</p> <ul style="list-style-type: none"> • As noted above, law enforcement efforts to catch illegal dumpers in the act have proved ineffective and a misuse of scarce law enforcement resources. • Citizen reports are helpful, but typically lack high quality information and information on large-scale commercial illegal dumping that plagues Oakland neighborhoods the most. • The City already has installed LED lighting citywide. 	

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