



Privacy Advisory Commission
May 4, 2017 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor
Meeting Agenda

Commission Members: *District 1 Representative: Reem Suleiman, District 2 Representative: 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 April 6 meeting minutes
3. 5:10pm: Open Forum
4. 5:15pm: Staff update on Surveillance Equipment Ordinance proposal to Public Safety Committee
5. 5:20pm: Discussion and possible action on Non-Cooperation with Registry Ordinance
6. 5:40pm: Presentation by Electronic Frontier Foundation – Analysis of Oakland Police Department's use of Automated License Plate Readers (ALPR), and overview of ALPR use by law enforcement
7. 6:00pm: Review and discussion of Oakland Police Department's Automated License Plate Reader policy. No action will be taken on this item at this meeting.
8. 7:00pm: Adjournment



Privacy Advisory Commission
April 6, 2017 5:00 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.*

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

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

Members present: Suleiman, Hofer, Katz, Jacquez, Johnson, Oliver, Karamooz, and Mulligan.

Members absent: Salahi.

2. 5:05pm: Review and approval of March 27 Special Meeting Minutes.

The minutes were approved unanimously with one minor edit.

3. 5:10pm: Open Forum

No Speakers.

4. 5:20pm: Presentation and possible action on Request For Proposal (Crime Analysis Software) – Nicole Freeman, Oakland Police Department, Crime Analysis Manager

Nicole Freeman with OPD's crime analysis unit presented an overview of the program and what OPD is looking for. The RFP is for a Crime Analysis Vendor and the City has been using Forensic Logic for the past 5 years but the City Council directed staff to conduct a competitive RFP for the next contract cycle. Generally there are three products the City needs: Pin Mapping of crimes that occur, Data Mining, and Investigative

Analysis and Data Management. Once the City receives responses to the RFP it should take 4-6 weeks to review and determine the most qualified vendor.

Member Mulligan asked if the Commission could see an electronic copy of the RFP in hopes of making some recommendations that would improve the end product the city gets; she cited experience helping the Berkeley Public Library refine their questions to vendors regarding their radio frequency book tag program and by asking those questions, the Library got better information about the vendors' capabilities. She noted in this RFP she could help develop questions about machine learning algorithms and analysis tools for example.

Member Karamooz raised concerns about the collection, storage, and analysis of large amounts of data, especially social media data. Member Jaquez also aired concerns about mass collection of social media data.

One Public Speaker on the item, JP Masser also raised concern about the data collection and about any efforts to use algorithms to implement predictive policing.

Member Oliver cited a publication highlighting the problems NYC police faced when they attempted to use predictive policing and the disparate impact it had on certain neighborhoods.

Tim Birch stated that OPD has no interest in using predictive policing, finds it problematic and will not deploy it. Member Suleiman noted that the data input for predictive policing is already racialized which simply magnifies the problems with using this strategy in policing.

5. 5:50pm: Presentation and possible action on data sharing/joint operation agreements with outside entities (Oakland Police Department).

Tim Birch presented his proposal to generate a comprehensive report on what OPD is currently doing regarding the issue of data sharing and joint operations. He will have the report touch on the following areas:

- A. *Collection of data from previous interactions with ICE historically and the outcomes of those*
- B. *Review of a new immigration policy that is being reviewed by the City Attorney's Office*
- C. *The Safe Streets MOU with rewritten language based on recent City Council resolutions*
- D. *A review of database access to verify who has access and that the access is appropriate and valuable*

He would like to present this item in June to ensure its completeness. Member Katz asked about also looking into an end date on the MOUs OPD enters into with the feds and Member Karamooz asked that it include info on what OPD can do if a federal agency demands access to the data. Chairperson Hofer also asked if controls could be put into place to ensure the language in the MOUs matches the language in City Council resolutions to avoid any ambiguity.

Three members of the public spoke on this item:

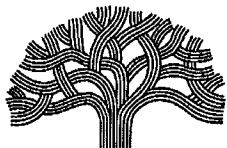
Rashidah Grinage asked if OPD Officers had participated in the Task Force and if so, how are they selected, how are they trained, and what policy applies to their work—OPD or federal when they are doing the work of the task force. Tim Birch indicated OPD Officers must always comply with OPD policy whenever they are working but he would come back with more detailed answers to her questions as well.

Tracy Rosenberg raised concerns about ICE deporting people whose only crime is an administrative violation of immigration law. She cited a case in Chicago where this just occurred. She also asked why an MOU was signed in January and if no officers have been assigned to the task force, why it's even necessary.

JP Masser notes that the Berkeley City Council approves and reviews all MOUs annually. Although this may be over-regulation, some higher level of oversight is needed. He also asked about access to databases that are of less significant crimes and whether the impact of that should be reviewed.

Chairperson Hofer also asked that the report include input regarding the threat of pulling federal funding that the City is facing.

6. 7:00pm: Adjournment



CITY OF OAKLAND

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2017 APR 28 AM 8:39

AGENDA REPORT

TO: Sabrina B. Landreth
City Administrator

FROM: Joe DeVries
Asst. to the City
Administrator

SUBJECT: Surveillance Ordinance

DATE: April 17, 2017

City Administrator Approval

Date:

4/27/17

RECOMMENDATION

Staff Recommends That The City Council Adopt The Surveillance And Community Safety Ordinance Which Prescribes The Rules For The Acquisition And Use Of Surveillance Equipment And Technology, Establishes Oversight, Auditing And Reporting Requirements, And Imposes Penalties For Violations.

EXECUTIVE SUMMARY

Approval of this Ordinance will require all City entities to seek City Council approval before accepting grant funds for, or the purchase or use of any new surveillance technology or equipment. The approval process for acquiring and using such technology will include completing a Surveillance Technology Impact Report, a Surveillance Use Policy, and the City Council making a determination that the benefits of the technology outweigh the costs. The Ordinance will also require that current surveillance technology undergo a similar public review and approval process and that annual oversight of all surveillance uses be conducted by the Privacy Advisory Commission and reported to the City Council.

The Ordinance allows individuals to seek injunctive or declaratory relief to enforce this Ordinance and provides that the City will pay reasonable attorney's costs should the plaintiff prevail. It also declares willful, intentional, or reckless violation of this Ordinance to be a misdemeanor and also provides whistleblower protection for individuals who report violations.

BACKGROUND/LEGISLATIVE HISTORY

On March 4, 2014 the City Council passed Resolution No. 84869 C.M.S. which stated in part, "That a Data Retention and Privacy Policy shall be developed by a Council-approved advisory body prior to the activation of the Port-only Domain Awareness Center, and members of said body will be appointed by each member of the City Council" which led to the creation of an Ad Hoc Privacy and Data Retention Policy Advisory Committee (Advisory Committee).

Item: _____
Public Safety Committee
May 9, 2017

The Advisory Committee met for over a year and developed the Policy which was adopted as Resolution No. 85638 C.M.S on June 2, 2015. Section II. A. of the resolution states that "The City Council shall establish a citywide Permanent Privacy Policy Advisory Committee. The City Council adopted Ordinance No.13349 C.M.S. on December 17, 2015 creating the Privacy Advisory Commission (PAC). Section 2.c of the Ordinance states that the PAC will draft for City Council consideration, model legislation relevant to the above subject matter, including a Surveillance Equipment Usage Ordinance.

The PAC began meeting in July 2016 and began drafting the Surveillance Technology and Community Safety Ordinance in collaboration with City Staff in September 2016. The PAC discussed the Ordinance at six monthly meetings in addition to a public hearing in January 2017. **Attachment A** is the final draft approved unanimously for submission to the City Council by the PAC. **Attachment B** is the ordinance that has been re-organized by the City Attorney's office so that it can be codified in the Oakland Municipal Code and arranged around sections delineating the review and approval process for the PAC and City Council. No substantive changes have been made in this draft other than necessary clarifications for the terms "City" and "City staff." These terms were created/modified to provide guidance to staff in implementing the ordinance.

ANALYSIS AND POLICY ALTERNATIVES

Public Process for New Technology

Approval of this Ordinance will require all City departments to seek City Council approval before accepting grant funds for, or the purchase or use of any new surveillance technology or equipment. Although City Departments already are required to seek Council approval to accept grant money, this approval process is much more robust and Oakland would be the first City in the nation to do so. It includes a requirement that the City department first submit a Surveillance Technology Impact Report to the PAC which allows for a standardized public format to evaluate the intended use of the equipment or technology. The Ordinance also requires that the City department submit a Surveillance Use Policy to the PAC and that the policy be adopted by the City Council before any equipment or technology can begin to be used. This is similar to the process followed recently for the Cell Site Simulator Equipment for which the City Council recently authorized the Police Department to enter into an MOU with Alameda County only after the Department collaborated with the PAC. Since before the creation of the PAC, over the past two years, the City's Ad Hoc Advisory Committee developed Use Policies for the Domain Awareness Center (DAC) and the Forward Looking Infrared Thermal Imaging Camera System (FLIR) in similar fashion and the new Ordinance creates a framework to apply citywide.

During the newly proposed process, the City Council is required to make a determination that the benefits of the technology outweigh its costs. This discussion will allow for greater public discourse on the use of such technologies and will apply across several City Departments. For example, the Parking Management Division of the Department of Transportation underwent a similar process regarding the use of a SMART Parking System in the fall before seeking final City Council approval. During that effort, the PAC met with City Staff and the vendor to make

Item: _____
Public Safety Committee
May 9, 2017

substantive changes to the use policies which allow for greater protection of Oaklanders' Personally Identifiable Information. The Police Department also followed this process as it developed its use policy and memorandum of understanding with Alameda County regarding the Cell Site Simulator Technology before seeking final City Council approval. .

Review of Current Technology

The Ordinance will also require that the City's current surveillance technology and equipment undergo a similar public review and approval process and discussions have already begun at the PAC about Automated License Plate Reading Technology. Staff raised concerns with the PAC about the potential workload increase in looking back in time at existing technology and being required to prepare Questionnaires and Use Policies for longstanding equipment that has generally been widely accepted over the past several years. The PAC modified the Ordinance language to address this concern and will prioritize existing equipment or technology to evaluate in partnership with City staff to ensure the workload in the first year is manageable. Once initial evaluations are performed, the workload should be reduced to 1) receiving annual reports about current uses, 2) developing policies for new uses, and 3) reporting annually to the City Council.

The term "City" means "any department, agency, and/or subdivisions of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code." "City staff" "means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this ordinance." This could be construed to include the Port of Oakland. However, Sections 701 and 706 of the City Charter gives exclusive control and management of the Port to the Board of Port Commissioners, and therefore this Ordinance would not apply to the Port of Oakland.

Enforcement, Protections, and Labor and Employment Issues

The Ordinance language allows individuals to seek injunctive or declaratory relief to enforce this Ordinance and provides that the City will pay reasonable attorney's costs should the plaintiff prevail. It also declares willful, intentional, or reckless violation of this Ordinance to be a misdemeanor and also provides whistleblower protection for individuals who report violations.

Section 8.(2) is very broad in scope. As it reads, "any person" who uses surveillance technology in violation of the Ordinance (which incorporates the DAC and FLIR policies) is subject to liquidated damages, civil penalties, and punitive damages. Conceivably, this could mean a City employee who violates any provision of an applicable policy/this Ordinance, even for an administrative matter such as not filling a report by the required deadline.

If the City wants to accept this type of provision it would be advisable to consider narrowing it. For example, the Santa Clara County Ordinance has a similar provision, but it requires that the jurisdiction must be notified of the harm first and be provided a chance to remedy before a private right of action is available. It also limits liability for instances where the conduct was "arbitrary and capricious." A similar provision may be worth pursuing.

Item: _____
Public Safety Committee
May 9, 2017

To the extent it effects the terms and conditions of employment, the Meyers Milias Brown Act requires the City to meet and confer with the unions over the Ordinance as currently drafted.

Provision Voiding City Contracts

Section 9 prohibits the City from entering into contracts that conflict with the Ordinance and voids conflicting provisions in existing contracts. This language was included to prevent the City from entering into non-disclosure agreements because, by their nature, those agreements could prevent open public discourse about proposed new surveillance technology. However, the retroactive language may not be enforceable depending on the contract in question and as written could apply to contracts beyond "non-disclosure agreements". Therefore staff is offering modified language for Section 9 that would not impact or apply to existing agreements. The modified language is below:

"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."

FISCAL IMPACT

The passage of this Ordinance has no direct fiscal impact. However, it requires all City departments to embark on a lengthier public process before acquiring or using new technology than previously required and to report annually on the use of such technology. It also requires staff to submit to a similar process for existing technology. This will require an unknown amount of additional staff time depending on how often new technology or equipment is sought.

PUBLIC OUTREACH/INTEREST

The PAC discussed the Ordinance over the course of seven months and held a public hearing in January. Both the Ordinance and the public hearing were promoted on the City's website and social media. At the public hearing, several public speakers commented and two prominent privacy experts testified in support of the measure including Professor Catherine Crump, Co-Director Berkeley Center for Law and Technology, and Nuala O'Connor, President and CEO of Center for Democracy and Technology.

COORDINATION

The Ordinance was developed by the PAC with the assistance of the City Administrator's Office, the Oakland Police Department, the Office of the City Attorney, and the Information Technology Department. This report was reviewed by the Oakland Police Department, the Controller's Bureau, and the Office of the City Attorney.

Item: _____
Public Safety Committee
May 9, 2017

SUSTAINABLE OPPORTUNITIES

Economic: The information presented in this report presents no economic impact.

Environmental: There are no environmental opportunities identified in this report.

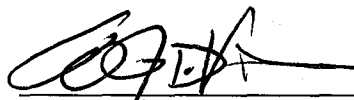
Social Equity: The adoption of a Surveillance and Community Safety Ordinance provides residents with a public process to evaluate how the City monitors its residents. Having such a process indicates that the City is responding appropriately to concerns about civil liberties and privacy during a time of rapidly evolving technology. By establishing safeguards to prevent potential abuse of technology, the City strengthens residents' faith in local government and allows for robust public dialogue and increased trust.

ACTION REQUESTED OF THE CITY COUNCIL

Staff recommends that the City Council adopt the Surveillance and Community Safety Ordinance which prescribes the rules for the acquisition and use of surveillance equipment and technology, establishes oversight, auditing and reporting requirements, and imposes penalties for violations.

For questions regarding this report, please contact Joe DeVries, Assistant to the City Administrator at (510) 238-3083.

Respectfully submitted,



Joe DeVries
Assistant to the City Administrator
City Administrator's Office

Reviewed by:

Amadis Sotelo
Deputy City Attorney

Item: _____
Public Safety Committee
May 9, 2017

2017 APR 20 10:39 AM 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 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 type and 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, analyze, 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;
 - e) **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
 - 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;
 - g) **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;

- 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;
 - i) **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;
 - j) **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,
 - k) **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. 86505 (Cell Site Simulator Use Policy adopted February 7, 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, or Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR Surveillance Use Policy adopted October 6, 2015), Resolution No. 86505 (Cell Site Simulator Use Policy adopted February 7, 2017), 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 \$1,000 or \$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, a Surveillance Use Policy promulgated under this Ordinance, or Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR Surveillance Use Policy adopted October 6, 2015), Resolution No. 86505 (Cell Site Simulator Use Policy adopted February 7, 2017), an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$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) Neither the City nor anyone acting on behalf of the City 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 and conditions of employment, access to information, restrictions on due process rights, 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 City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or Administrative Instruction promulgated under 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 against the City 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].

2017 APR 28 AM 8:39

INTRODUCED BY COUNCILMEMBER _____

DRAFT
CITY ATTORNEY'S OFFICE

OAKLAND CITY COUNCIL
ORDINANCE NO. _____ C.M.S.

**ORDINANCE ADDING CHAPTER 9.64 TO THE OAKLAND
MUNICIPAL CODE ESTABLISHING RULES FOR THE
CITY'S ACQUISITION AND USE OF SURVEILLANCE
EQUIPMENT**

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City of Oakland's ("City") acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of 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, while acknowledging the significance of protecting the privacy of citizens, 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, 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 may include 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 the City's use of 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 the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; 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 City surveillance technology is deployed.

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. This Ordinance shall be known as the Surveillance and Community Safety Ordinance.

SECTION 2. Oakland Municipal Code Chapter 9.64, is hereby added as set forth below (chapter and section numbers are indicated in **bold type**).

Chapter 9.64 REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

9.64.010. DEFINITIONS. The following definitions apply to this Chapter.

1. "Annual 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 type and 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 each individual census tract as

defined City Council District/Police Beat 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 regarding the relevant subject surveillance technology, 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, agency, bureau, and/or subordinate division, ~~or unit of the City of Oakland~~ as provided by Chapter 2.29 of the Oakland Municipal Code.
3. "City staff" means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this Chapter.
4. "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, 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 above in Section 7(3):

1. 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;
 2. Parking Ticket Devices (PTDs);
 3. 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;
 4. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
 5. 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;
 6. ~~City Municipal agency~~ databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
5. "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;
 - E. **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
 - 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;
 - G. **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;

- 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;
 - I. **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;
 - J. **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,
 - K. **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).
6. "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 departments/bureaus/divisions ~~entities~~ 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.

9.64.020 Privacy Advisory Commission (PAC) Notification and Review Requirements

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

- A. A City entity staff shall notify the Chair of the Privacy Advisory Commission prior to ~~the entity~~:
 - 1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
 - 2. Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.
- B. Upon notification by ~~the~~ City staff entity, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, City staff ~~the entity~~ shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action ~~the City staff entity intends to will seek~~ Council approval for pursuant to 9.64.030~~take~~. The Privacy Advisory

Commission may make a recommendation to City Council by voting its approval to proceed, object to the proposal, recommend that the entity City staff modify its the proposal, or take no action.

- C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020.1.B, City staff may proceed and seek Council Approval of the proposed Surveillance Technology initiative pursuant to the requirements of Section 9.64.030.

~~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. PAC Review Required for New Surveillance Technology Before City Council Approval

- A. Prior to seeking City Council approval under Section 9.64.030, ~~the City staff shall entity shall~~ submit a Surveillance Impact Report and proposed a Surveillance Use Policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 9.64.010.
- 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 such modifications to the City staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.
- C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval

- A. Prior to seeking City Council approval for existing City surveillance technology under Section 9.64.030 the City entity staff shall submit the a Surveillance Impact Report and Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 9.64.010.
- B. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, each City staff entity shall present to the Privacy Advisory Commission a list of surveillance technology already possessed and/or used by the City entity.
- C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
- D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020.1.C., each City staff 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 each month until a policy has been submitted for each item on the list the list is exhausted.
- E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable the City staff entity to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

9.64.030. City Council Approval Requirements for New and Existing Surveillance Technology.

- 1. City staff 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.

2. City Council Approval Process

- A. After the PAC Notification and Review requirements in Section 9.64.020 have been met, City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed
After the recommendation of the Privacy Advisory Commission, the City Council shall provide the public notice that will include the Surveillance Impact Report and proposed Surveillance Use Policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing.
- B. The City Council shall only approve any action as provided in this Chapter 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.
- C. For Approval of Existing Surveillance Technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020.3.E, if the City Council has not reviewed and approved such item within sixty (60) days of the City Council submission date it was scheduled for City Council consideration, the City shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records

The City Council, or its appointed designee City staff shall continue to make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, and updated versions thereof, available to the public as long as the City municipal entity continues to utilize uses the surveillance technology in accordance with its request pursuant to Section 9.64.020.A.1-2(1).

9.64.040. 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 of surveillance technology, and annually thereafter on or before November 1, City staff must schedule and submit a written

Annual Surveillance Report for City Council review for each approved surveillance technology item.

- A. Prior to submission of the Annual Surveillance Report to the City Council, the City staff entity shall submit the Annual 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 Annual Surveillance Use Policy that will resolve the concerns.
2. Based upon information provided in City staff's the Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030.2.B and either uphold or set aside the previous determination ~~determine whether the requirements of Section 4 are still satisfied. If the requirements of Section 4 are not satisfied, Should the City Council set aside its previous determination, the City Council shall direct that City's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.~~
3. No later than January 15 of each year, City staff shall schedule an informational report for the a City Council meeting 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~~ 9.64.030 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 Annual Surveillance Reports submitted.

9.64.050. Enforcement

1. Violations of this article are subject to the following remedies:
 - A. 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~~), 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.

- B. 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 \$1,000 or \$100 per day for each day of violation, whichever is greater) and punitive damages.
- C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (A) or (B).
- D. 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 \$1,000 per violation.

9.64.060. 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 collective bargaining agreement and related memorandum of agreement or understanding that pre-date this Ordinance

9.64.070. Whistleblower Protections.

1. Neither the City nor anyone acting on behalf of the City 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 and conditions of employment, access to information, restrictions on due process rights, 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 City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or Administrative Instruction promulgated under 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 against the City in any court of competent jurisdiction.

SECTION 3. Existing Surveillance Use Policies for the Domain Awareness Center, Forward Looking Infrared Thermal Imaging Camera System, and Cell Site Simulator, Must Be Adopted as Ordinances.

City staff shall return to City Council with an ordinance or ordinances adopting and codifying the following surveillance use policies under the Oakland Municipal Code: the Domain Awareness Center (DAC) Policy for Privacy and Data Retention (Resolution No. 85638 C.M.S., passed June 2, 2015); the Forward Looking Infrared Thermal Imaging Camera System (FLIR) Privacy and Data Retention Policy (Resolution No. 85807 C.M.S., passed October 6, 2015); and the Cell Site Simulator Policy (Resolution No. 86585 C.M.S., passed February 7, 2017) .

SECTION 4. Severability. If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof irrespective of the fact

that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

SECTION 5. Effective Date. This ordinance shall become effective immediately on final adoption if it receives six or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

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

NOES -

ABSENT -

ABSTENTION -

ATTEST: _____

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

Date of Attestation: _____

NOTICE AND DIGEST

ORDINANCE ADDING CHAPTER 9.64 TO THE OAKLAND MUNICIPAL CODE, A SURVEILLANCE AND COMMUNITY SAFETY ORDINANCE WHICH PRESCRIBES RULES FOR THE ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT AND TECHNOLOGY, ESTABLISHES OVERSIGHT, AUDITING AND REPORTING REQUIREMENT, AND IMPOSES PENALTY VIOLATIONS

This ordinance sets rules for how the City of Oakland acquires and uses surveillance technology. It requires the City to establish policies governing the use of surveillance technology. It also provides a review process for new and existing surveillance technology whereby the Privacy Advisory Commission will evaluate and provide a public forum for discussion on proposed and existing City surveillance technology in regards to privacy rights, public safety, and fiscal considerations. The Ordinance also specifies that City Council approval is required for the City to use new and existing surveillance technology. Further, it establishes an ongoing review process for City Council, on an annual basis to evaluate whether already approved surveillance technology should continue to be used based on the same considerations referenced above.

THE NON-COOPERATION WITH IDENTITY-BASED REGISTRY/INTERMENT ORDINANCE

Whereas, the City Council finds that freedom of religion and protection from persecution based on religion are founding ideals of our nation; and

Whereas, the City Council finds that the City of Oakland has a moral obligation to protect its citizens from persecution based on religious affiliation as well as national origin and ethnicity, which are often used as proxies to target religion; and

Whereas, the City Council finds that immigrants are valuable and essential members of both the California and Oakland community; and

Whereas, the City Council finds that a registry of individuals identified by religion, national origin, or ethnicity, in a list, database, or registry including that information, could be used by the government to persecute those individuals; and

Whereas, President Trump has repeatedly signaled that he intends to require Muslims to register in a database, by reenacting and expanding the 2002-2011 discriminatory Nation Security Entry-Exit Registration System, which required registration of non-citizen men from 25 Muslim-majority countries which lead to 83,000 registrants, 13,000 in the pipeline for deportation, and zero terrorism convictions; and

Whereas, Trump advisors have invoked WWII Japanese-American internment as a precedent for the proposed expansion of the registry; and

Whereas, President Trump has ordered a sweeping expansion of deportations and assigned unprecedented powers to Immigration and Customs Enforcement (ICE) officers targeting and terrorizing immigrant communities; and

Whereas, President Trump has issued two executive orders banning entry from certain Muslim-majority countries; and

Whereas, the City Council finds that the City of Oakland's Sanctuary City status has caused President Trump to threaten to withhold federal funding from the City of Oakland; and

Whereas, the City Council finds that the City of Oakland's Municipal Identification Card program, which exists to achieve certain policy goals of the City of Oakland, may also place participating individuals at risk of persecution, and therefore the program must be structured to ensure that sufficient safeguards are in place to prohibit such persecution while still allowing for the benefits of such program participation to be delivered to the individuals entitled to them; and

Whereas, the City Council finds that both the United States and California Constitution guarantee freedom of religion and equal protection under the law; and

Whereas, the City Council finds that it is the intent of this ordinance to prevent the use of City resources to assist in any way with a discriminatory government or private registry based on religion, national origin, or ethnicity for the purposes of persecuting such individuals, and to prevent the City from disclosing personal information regarding any individual that could be used to create such a registry;

Whereas, the City Council finds that it is not the intent of this ordinance to prohibit the City from creating or maintaining a list, database, or registry that contains ethnicity or national origin information where such information is collected in the aggregate or for complying with anti-discrimination laws or laws regarding the administration of public benefits, or for purposes of ensuring City programs adequately serve the City's diverse communities, or where the city collects this information to ensure equal or equitable access to City programs, services, benefits, and contracts; now, therefore

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

Section 1. Title

This ordinance shall be known as the Non-Cooperation with Identity-Based Registry Ordinance.

Section 2. Assistance With Registry Or Database, Or Internment

- 1) No officer, employee, department, board, commission, or other entity of the City shall use City resources, moneys, facilities, property, equipment, or personnel to create, implement, provide investigation for, enforce, or assist in the creation, implementation, provision of investigation for, or enforcement of, or provide support in any manner for, any government program that (1) creates or compiles a List, Database, or Registry of individuals on the basis of religious affiliation, kinship, belief, or practice; national origin; or ethnicity or (2) requires registration of individuals in a List, Database, Registry, or otherwise, on the basis of religious affiliation, kinship, belief, or practice; national origin; or ethnicity, or (3) requires the detention, relocation or internment of individuals on the basis of religious affiliation, kinship, belief or practice; national origin, or ethnicity.
- 2) Notwithstanding any other law, no officer, employee, department, board, commission, or other entity of the City shall provide or disclose to any government authority or private party Personal Information regarding any individual that is requested for the purpose of (1) created or compiling a List, Database, or Registry of individuals based on religious affiliation, kinship, belief, or practice; national original; or ethnicity, or (2) requiring registration of individuals in a List, Database, Registry, or otherwise, on the basis of religious affiliation, kinship, belief, or practice; national origin; or ethnicity, or (3) requires the detention, relocation or internment of individuals on the basis of religious affiliation, kinship, belief or practice; national origin; or ethnicity. This includes a prohibition on making available Personal Information from any City database for the purposes mentioned in subsection 1) supra, including any City database

maintained by a private vendor under contract with the City or any subcontractor thereof.

- 3) This section shall apply to any individual, regardless of citizenship or immigration status, race, age, or any other factor.
- 4) Nothing in this section prohibits an officer, employee, department, board, commission, or other entity of the City from sending to, or receiving from any local, state, or federal agency, aggregate information about religious affiliation, kinship, belief, or practice; national origin; or ethnicity within a geographic area, institution, category, or group, where such information is not associated with Personal Information, including but not limited to names, addresses, and telephone numbers, and cannot be used to identify individuals on the basis of religious affiliation, kinship, belief, or practice; national origin; or ethnicity.
- 5) Nothing in this section prohibits the City from creating or maintain a List, Database, or Registry that contains ethnicity or national origin information where such information is collected for purposes of complying with anti-discriminating laws or laws regarding the administration of public benefits, or for purposes of ensuring City programs adequately serve the City's diverse communities, or where the City collects this information to ensure equal and equitable access to City programs, services, benefits, and contracts.
- 6) "List", "Database", or "Registry" shall mean any public, private, or joint public-private collection of information stored in any form.
- 7) "Personal Information" shall mean any information that can, on its own or in combination with other information, be used to contact, track, locate, identify, or reasonably infer the identity of a specific individual.
- 8) "Persons and Individual" refers to natural and legal persons.

Section 3. Investigation And Reporting

- (a) The City Administrator, or his or her designee, shall review compliance with Section 2. The City Administrator may initiate and receive complaints regarding violations of Section 2. After conducting an investigation, the City Administrator may issue findings regarding any alleged violation. If the City Administrator finds that a violation occurred, the City Administrator shall, within 30 days of such finding, send a report of such finding to the City Council, the Mayor, and the head of any department involved in the violation or in which the violation occurred. All officers, employees, departments, boards, commissions, and other entities of the City shall cooperate with the City Administrator in any investigation of a violation of Section 2.
- (b) By April 1 of each year, each City department shall submit to the City Council a written, public report regarding the department's compliance with Section 2 over the previous calendar year. At minimum, this report must (1) detail with specificity the steps the department has taken to ensure compliance with Section 2, (2) disclose any issues with compliance, including any violations or potential

violations of this Ordinance, and (3) detail actions taken to cure any deficiencies with compliance.

Section 4. Enforcement

- (a) Cause of Action. The City shall be liable in a civil action for a violation of this Ordinance filed by either (1) an individual whose Personal Information has been disclosed in violation of Section 2, or (2) a non-profit organization exempt from taxation pursuant to Title 26, Section 501 of the United States Code, that has the defense of immigrants' and ethnic minorities' rights as a stated purpose in its articles of incorporation or bylaws.
- (b) Damages and Civil Penalties. If the City is found liable in a cause of action brought by an individual under section (a)(1) above, the City shall be liable for (1) the damages suffered by the plaintiff, if any, as determined by the court, and (2) a civil penalty no greater than \$5,000 per violation, as determined by the court. If the City is found liable in a cause of action brought by an organization under section (a)(2) above, the City shall be liable for a civil penalty no greater than \$5,000 per violation, as determined by the court; provided that an organization may not recover a civil penalty if a court has already awarded a penalty to an individual or another organization arising out of the same violation. In determining the amount of the civil penalty in any action filed pursuant to Section 4, the court shall consider whether the violation was intentional or negligent, and any other prior violations of Section 2 by the City department that committed the violation. For the purpose of this subsection, each disclosure of each individual's Personal Information shall be a separate violation.
- (c) 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.
- (d) Limitations on Actions. Any person or entity bringing an action pursuant to Section 4 must first file a claim with the City pursuant to Government Code 905 or any successor statute within four years of the alleged violation.
- (e) Any disclosure of Personal Information required by a legally enforceable subpoena, judicial warrant, or court order shall not give rise to a cause of action under Section 4.

Section 5. 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 6. Construction

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

Section 7. Effective Date

This Ordinance shall take effect on [DATE].

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.

Oakland Police Department

Policy Manual

Automated License Plate Readers (ALPRs)

- (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.
- (f) If practicable, the officer 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.

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.

Oakland Police Department

Policy Manual

Automated License Plate Readers (ALPRs)

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 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).

430.9 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

Oakland Police Department

Policy Manual

Automated License Plate Readers (ALPRs)

- 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.