



FILED  
OFFICE OF THE CITY CLERK  
OAKLAND

2018 MAR 29 PM 4:50

# AGENDA REPORT

**TO:** Sabrina B. Landreth  
City Administrator

**FROM:** Joe DeVries  
Asst. to the City  
Administrator

**SUBJECT:** Surveillance Ordinance

**DATE:** March 19, 2018

City Administrator Approval

Date:

3/29/18

## RECOMMENDATION

**Staff Recommends That The City Council Adopt An Ordinance Adding Chapter 9.64 To The Oakland Municipal Code Establishing Rules For The City's Acquisition And Use Of Surveillance Equipment.**

## REASON FOR SUPPLEMENTAL

On May 9, 2017, the Public Safety Committee (PSC) voted unanimously to forward the draft ordinance (**Attachment A**) to the City Council pending the scheduling of Meet and Confer sessions with any affected bargaining units of the City. Since that time, staff met with the Oakland Police Officers Association (OPOA) on three separate occasions to hear their concerns about the current draft Ordinance language. Staff also met with Oakland Police Department (OPD) Leadership on four separate occasions on proposed modified language to address those concerns. A modified draft was presented to the Privacy Advisory Commission (PAC) and was approved unanimously at the February meeting. The newly proposed draft was also presented to any affected bargaining units to allow for final input. After receiving that input, staff is proposing modified language (**Attachment B**).

Areas of concern that were identified by OPOA and OPD leadership during the meet and confer process included discipline standards, reporting mechanisms, exigent circumstances, clarification of certain definitions, and data sharing restrictions. Revisions were made to the ordinance to address those concerns as outlined below.

### *Revisions to Ordinance*

#### **9.64.010 DEFINITIONS:**

Revisions were made to the details of the Annual Surveillance Report to offer better clarity to staff as to what the reporting requirements will be each year. A definition was added for Exigent Circumstances, Surveillance, Large Scale Events, and several clarifications were added to the definition of Surveillance Technology.

Item: \_\_\_\_\_  
Public Safety Committee  
April 10, 2018

**9.64.030 section D. Entering into a continuing or written agreement with a non-City entity:**

This section requires City Departments to receive City Council approval before entering into agreements with non-city entities to use technology those other entities may have, but have not been through an approval process at the City. For example, if the City Council had prohibited the use of a facial recognition device that a federal partner uses on a regular basis, the ordinance attempts to protect against City departments side-stepping the ordinance by routinely borrowing the device from the federal partner. However, in the prior draft, OPD was concerned that it would prevent them from more routine, informal information sharing in the immediate course of an investigation. For example, if a convenience store owner had video footage of a shooting that investigators wanted to use to build a case and there had been no prior approval from the City Council, using the footage could be considered a violation. Therefore, the language was modified to specify that entering into *continuing written agreements* requires prior approval.

**9.64.035. Use of Unapproved Technology during Exigent Circumstances and Large Scale Events:**

This section was added (**Attachment B, pages 4 and 10**) to create a process to allow the use of unapproved technology when there are exigent circumstances and there is no time to seek prior approval or during unique circumstances in which a large-scale event of more than 10,000 people, with the potential for national attention that creates an unusual increased risk for an exigent circumstance develops. The best recent example of such an event was last year's Warriors Parade. That event was scheduled within days of the Warriors championship win and it would have been impossible to seek prior approval to access resources that other law enforcement agencies had available to improve public safety at the parade. The section has after-the-fact reporting requirements and built-in limitations to see that the technology is used only for the exigent circumstance or event.

**9.64.050. Enforcement:**

**Section A** of the original draft (**Attachment A, page 10**) allows for a person to seek injunctive relief against the City and against any third party for violations of the ordinance. The reference to third parties was intended to allow for relief to be sought against another governmental entity that may be allowing the City to improperly use one of its devices such as the example cited above regarding an unapproved facial recognition device. However, concerns were identified that in the case of the convenience store owner who has shared video footage of a shooting, they would potentially face legal exposure for trying to help solve a crime in their neighborhood. Therefore, the language was modified to only allow injunctive relief against another governmental agency.

**Section B** of the original draft (**Attachment A, page 10**) allowed for persons who had been subject to a surveillance technology in violation of the ordinance to seek damages in civil court against *any person* who committed such a violation and entitled that person to recover damages. Concerns were raised that this would expose city employees or employees of local partner law enforcement agencies such as the Alameda County District Attorney's investigators for actions they may take as part of their normal job duties. If investigators believe they could individually be sued for providing information about a crime that was gathered by a non-

approved device, it could have a chilling effect on the working relationship between these agencies. Therefore, the language was modified to allow for civil action to be taken directly against the City only and not individuals.

**Section D** of the original draft (**Attachment A, page 11**) stated:

*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.*

This language was raised throughout the development of the ordinance as the most concerning language in the enforcement section from employee organizations. The language identifies only the most severe penalty for a violation and does not provide the type of progressive disciplinary/training structure typically afforded employees who make mistakes on the job whether willfully or unintentionally.

The proposed modified language is (**Attachment B, page 12**):

*Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.*

This allows flexibility to address all levels of violations that could occur: employees could receive training about the ordinance for a minor violation that may be inadvertent, or more substantial consequences including suspension or termination for serious violations.

#### **ACTION REQUESTED OF THE CITY COUNCIL**

Staff recommends that the City Council adopt an Ordinance adding Chapter 9.64 to the Oakland Municipal Code establishing rules for the City's acquisition and use of surveillance equipment.

Sabrina B. Landreth, City Administrator

Subject: Surveillance Ordinance

Date: March 19, 2018

Page 4

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

Attachments (2)

A: Original Draft Ordinance

B: Proposed Revised Draft Ordinance

Attachment A

FILED  
OFFICE OF THE CITY CLERK  
OAKLAND

APPROVED AS TO FORM AND LEGALITY

2018 MAR 29 PM 4:51

INTRODUCED BY COUNCILMEMBER \_\_\_\_\_

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 hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; 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 Police Area in the relevant year;
  - E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
  - 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 unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
  - 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 helps 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" means any department, agency, bureau, and/or subordinate division 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. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.
  5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

6. "Large scale event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.
7. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.
8. "Police area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.
9. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.
10. "Surveillance technology" means any software, 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. Examples of surveillance technology includes, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services to forecast criminal activity or criminality, biometric identification hardware or software.
  - 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:
    1. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread 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 databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.
  7. Medical equipment used to diagnose, treat, or prevent disease or injury.
  8. Police department interview room cameras.
  9. Police department case management systems.
  10. Police department early warning systems.
  11. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.
6. "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, using general descriptive terms, and crime statistics for any location(s);
  - D. **Impact:** An assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether 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).
7. "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 category of 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, 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;
- 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. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
    - 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 City staff, 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 shall inform the Privacy Advisory Commission of

the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify 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.

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

- A. Prior to seeking City Council approval under Section 9.64.030, City staff shall submit a Surveillance Impact Report and 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 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 City staff shall submit 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, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.

- 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., City staff 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 each month until a policy has been submitted for each item on the list.
- E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff 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 must obtain City Council approval 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 or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or
  - D. Entering into a continuing agreement or written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
- 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 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. Approval may only occur at a 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 four City Council meetings from when the item was initially 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

City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section 9.64.020.A.1.

**9.64.035. Use of Unapproved Technology during Exigent Circumstances**

(a) City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy in two types of circumstances without following the provisions of Section 9.64.030: (1) Exigent circumstances, and (2) a large scale event.

(b) If City staff acquires or uses a surveillance technology in these two circumstances pursuant to subdivision (a), the City staff shall:

(1) Use the surveillance technology to solely respond to the exigent circumstances or large scale event.

(2) Cease using the surveillance technology when the exigent circumstances or large scale event ends.

(3) Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

(4) Following the end of the exigent circumstances or large scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

(c) Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

#### **9.64.040. Oversight Following City Council Approval**

1. On March 15<sup>th</sup> of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, City staff must present a written Annual Surveillance Report for Privacy Advisory Commission review for each approved surveillance technology item. If City staff is unable to meet the March 15<sup>th</sup> deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.
  - A. After review by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.
  - 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 corresponding Surveillance Use Policy that will resolve the concerns.
  - 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 Annual Surveillance Report.
  - D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 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.

2. Based upon information provided in City staff's 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. Should the City Council set aside its previous determination, the 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.

#### **9.64.050. Enforcement**

1. Violations of this article are subject to the following remedies:
  - A. Any violation of 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 the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city department, and 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 other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permissible by law.
  - 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 the Superior Court of the State of California against the City of Oakland 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).



- 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. Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.

#### **9.64.060. Secrecy of Surveillance Technology**

It shall be unlawful for the City to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

#### **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 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 this section 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.**

Within 180 days of the effective date of this ordinance, 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:

---

Attachment B

FILED  
OFFICE OF THE CITY CLERK  
OAKLAND

2018 MAR 29 PM 4: 54

APPROVED AS TO FORM AND LEGALITY

AS AMENDED BY THE MAY 9, 2017  
PUBLIC SAFETY COMMITTEE

INTRODUCED BY COUNCILMEMBER \_\_\_\_\_

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; using general descriptive terms so as not to reveal the specific location of such hardware; 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 ~~City Council-District/Police Area Beat~~ in the relevant year;
  - 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;~~ the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
  - 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" means any department, agency, bureau, and/or subordinate division 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. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.
  5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

6. “Large scale event” means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.
7. “Personal communication device” means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.
8. “Police area” refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time
9. “Surveillance” or “surveil” means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.
10. “Surveillance technology” means any software, 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. Examples of surveillance technology includes, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.
  - 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:
    1. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, 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 databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
7. Medical equipment used to diagnose, treat, or prevent disease or injury.
8. Police department interview room cameras.
9. Police department case management systems.
10. Police department early warning systems.
11. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

11. "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, using general descriptive terms, 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 of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether~~ 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).

12. "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 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. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
    - 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 City staff, 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 shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify 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.
2. PAC Review Required for New Surveillance Technology Before City Council Approval
- A. Prior to seeking City Council approval under Section 9.64.030, City staff shall submit a Surveillance Impact Report and 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 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 City staff shall

submit 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, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.
- 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., City staff 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 each month until a policy has been submitted for each item on the list.
- E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff 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 must obtain City Council approval 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 pursuant to the requirements of this ordinance; or
  - D. Entering into an continuing agreement or written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

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 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. Approval may only occur at a 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 four City Council meetings from when the item was initially of the 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

City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section 9.64.020.A.1.

**9.64.035. Use of Unapproved Technology during Exigent Circumstances**

(a) City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy in two types of circumstances without following the provisions of Section 9.64.030: (1) Exigent circumstances, and (2) a large scale event.

(b) If City staff acquires or uses a surveillance technology in these two circumstances pursuant to subdivision (a), the City staff shall:

(1) Use the surveillance technology to solely respond to the exigent circumstances or large scale event.

(2) Cease using the surveillance technology when the exigent circumstances or large scale event ends.

(3) Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

(4) Following the end of the exigent circumstances or large scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

(c) Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

#### **9.64.040. Oversight Following City Council Approval**

1. Within twelve (12) months of City Council approval of surveillance technology, and annually thereafter on or before November 1, On March 15<sup>th</sup> of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, City staff must schedule and submit present a written Annual Surveillance Report for City Council review for each approved surveillance technology item. If City staff is unable to meet the March 15th deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.
  - A. Prior to submission of the Annual Surveillance Report to the City Council, City staff shall submit the Annual Surveillance Report to the Privacy Advisory Commission for its review. After review by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.
  - 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.

- 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 Annual Surveillance Report.
- D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 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.

2. Based upon information provided in City staff's 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. Should the City Council set aside its previous determination, the 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 a City Council meeting that includes, for the prior year:~~

- ~~A. A summary of all requests for City Council approval pursuant to Section 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 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~~ the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city ~~agency~~ department, 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~~ other governmental agency 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~~ the Superior Court of the State of California against any ~~person who committed such violation~~ the City of Oakland 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.~~ Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.

#### **9.64.060. Secrecy of Surveillance Technology**

It shall be unlawful for the City to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.



To the extent permitted by law, the City shall publicly disclose all of its ~~existing and future~~ surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary. ~~In addition, the City shall publicly disclose its existing and future employee labor agreements/memorandums of understanding.~~

**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: \_\_\_\_\_

FILED  
OFFICE OF THE CITY CLERK  
OAKLAND

FILED  
OFFICE OF THE CITY CLERK  
OAKLAND

2018 MAR 29 PM 4:55 2018 MAR 29 PM 4:51

APPROVED AS TO FORM AND LEGALITY

  
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; 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.** 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 hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; 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 Police Area in the relevant year;
  - E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
  - 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 unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
  - 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 helps 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" means any department, agency, bureau, and/or subordinate division 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. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.
  5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

6. "Large-scale event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.
7. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.
8. "Police area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.
9. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.
10. "Surveillance technology" means any software, 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. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.
  - 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:
    1. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread 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 databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.
  7. Medical equipment used to diagnose, treat, or prevent disease or injury.
  8. Police department interview room cameras.
  9. Police department case management systems.
  10. Police department early warning systems.
  11. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.
6. "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, using general descriptive terms, and crime statistics for any location(s);
  - D. **Impact:** An assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether 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).
7. "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 category of 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, 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;
- 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. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
    - 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 City staff, 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 shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify 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.

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

- A. Prior to seeking City Council approval under Section 9.64.030, City staff shall submit a Surveillance Impact Report and 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 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 City staff shall submit 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, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.
- 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., City staff 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 each month until a policy has been submitted for each item on the list.
- E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff 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 must obtain City Council approval 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 or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or
  - D. Entering into a continuing agreement or written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
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 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. Approval may only occur at a 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 four City Council meetings from when the item was initially 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

City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section 9.64.020.A.1.

**9.64.035. Use of Unapproved Technology during Exigent Circumstances or Large-Scale Event**

- 1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy in two types of circumstances without following the provisions of Section 9.64.030: (A) Exigent circumstances, and (B) a Large-scale event.
- 2. If City staff acquires or uses a surveillance technology in the two circumstances pursuant to subdivision (1), the City staff shall:
  - A. Use the surveillance technology to solely respond to the Exigent circumstances or Large-scale event.
  - B. Cease using the surveillance technology when the Exigent circumstances or Large scale event ends.
  - C. Only keep and maintain data related to the Exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

(15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a 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 four City Council meetings from when the item was initially 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

City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section 9.64.020.A.1.

**9.64.035. Use of Unapproved Technology during Exigent Circumstances or Large-Scale Event**

- 1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy in two types of circumstances without following the provisions of Section 9.64.030: (A) Exigent circumstances, and (B) a Large-scale event.
- 2. If City staff acquires or uses a surveillance technology in the two circumstances pursuant to subdivision (1), the City staff shall:
  - A. Use the surveillance technology to solely respond to the Exigent circumstances or Large-scale event.
  - B. Cease using the surveillance technology when the Exigent circumstances or Large scale event ends.
  - C. Only keep and maintain data related to the Exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

- D. Following the end of the Exigent circumstances or Large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.
- 3. Any technology temporarily acquired in Exigent circumstances or during a Large-scale event shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

#### **9.64.040. Oversight Following City Council Approval**

- 1. On March 15<sup>th</sup> of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, City staff must present a written Annual Surveillance Report for Privacy Advisory Commission review for each approved surveillance technology item. If City staff is unable to meet the March 15<sup>th</sup> deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.
  - A. After review by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.
  - 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 corresponding Surveillance Use Policy that will resolve the concerns.
  - 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 Annual Surveillance Report.
  - D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all

requests for City Council approval pursuant to Section 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.

2. Based upon information provided in City staff's 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. Should the City Council set aside its previous determination, the 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.

#### **9.64.050. Enforcement**

1. Violations of this article are subject to the following remedies:
  - A. Any violation of 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 the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective City department, and 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 other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permitted by law.
  - 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 the Superior Court of the State of California against the City of Oakland 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).

- 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. Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.

**9.64.060. Secrecy of Surveillance Technology**

It shall be unlawful for the City to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

**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 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 this section 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.**

Within 180 days of the effective date of this ordinance, 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: \_\_\_\_\_