CITY OF OAKLAND

Privacy Advisory Commission

January 4, 2018 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor
Meeting Agenda

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

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

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

2. 5:05pm: Open Forum

3. 5:10pm: Roundtable discussion on data sharing with Mike Sena, Executive Director of Northern California Regional Intelligence Center (NCRIC). There is no action to be taken on this item.

4. 6:30pm: Discuss and take possible action on Surveillance Equipment Ordinance.

5. 7:00pm: Adjournment

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 abuse 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

Commented [TB1]: OPD doesn't perceive the use of surveillance technology as a threat to the community. The abuse, however, is indeed a threat.

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 ACQUISTION 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 provided such information does not compromise operations;

   ~~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.~~B. ~~Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; f~~For surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

Commented [TB2]: OPD recommends adding this qualification because this may otherwise risk operational integrity. It is also not required under the California Evidence Code.

Commented [TB3]: OPD recommends removing this section, as OPD has no knowledge or control over data that is shared from a database that OPD is feeding into – such as CRIMS.

Commented [TB4]: OPD recommends removing the first part of this section, as There are serious security risks in disclosing a breakdown of what physical objects surveillance technology is installed upon, such as the vehicle that houses the cell site simulator technology.

~~D.~~C. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each ~~City Council District/~~Police ~~Beat~~ Areain the relevant year;

~~E.~~D. 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 ~~any discriminatory uses of the technology and effects on the public's~~ civil rights and civil liberties~~, including but not limited to those guaranteed by the California and Federal Constitutions;~~.

~~F.~~E. 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 prohibited by law, including but not limited to confidential personnel file information.

~~G.~~F. 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.~~G. Information, ~~including crime statistics,~~ that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;

~~I.~~H. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;

~~J.~~I. ~~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.~~J. 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. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of death or serious physical injury to any person requires the use of surveillance technology or the information it provides or the destruction of evidence is imminent.

Commented [TB5]: OPD does not track or record data by Council District. Doing so overly politicizes data and risks Council interference. Police areas are best because then we are not revealing info about a specific investigation.

Commented [TB6]: It is exceptionally difficult to assess whether there is an impact on crime through use of a specific technology.

Commented [TB7]: This seems duplicative with the report for each individual technology. This information can be required and included for each specific technology. Personnel costs don't seem necessary and it is unclear as to what is being sought.

Commented [DJ8]: This is newly inserted to allow for use of unapproved technology in such circumstances—see newly added section 9.64.35

Commented [TB9]: The imminent destruction of evidence may also be an exigency.

~~5. "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.~~

5. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

It is not surveillance if an individual knowingly and voluntarily consents to provide the information, or had a clear and conspicuous opportunity to opt out of being subject to surveillance.

~~6. "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. 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; and personal communication devices. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.~~

6. Surveillance Technology" is divided into two distinct types: Hardware-Based Surveillance Technology and Software-Based Surveillance Technology.

   a. Hardware-Based Surveillance Technology: For the purposes of this statute, a piece of electronic equipment will be considered Hardware-Based Surveillance Technology if it meets either of the following two criteria:

      1) There is a statutory requirement to obtain authorization by a higher authority prior to its use (i.e. a court order or search warrant);

      OR

      2) If the electronic equipment meets all the following criteria:

Commented [DJ10]: This is a new definition

Commented [TB11]: Including these devices – particularly cell phones and especially personally owned cell phones – will require thousands of City staff – including Council members and department heads – to comply with reporting requirements in this ordinance.

Commented [TB12]: OPD recommends including a definition of "surveillance." This was largely taken from the Seattle ordinance.

Commented [TB13]: The existing definition of surveillance technology provided is overly broad.

Commented [DJ14]: This is newly inserted to provide clarity.

Commented [TB15]: OPD recommends removing the examples and using above definitions instead.

Formatted: List Paragraph, Indent: Left: 1", Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

a) It is owned and/or operated by a law enforcement agency or City Department;
b) It is, by design, capable of indiscriminately capturing the movements, images, or biometrics of the public without their knowledge; AND
c) It is, by design, capable of being operated and monitored both remotely and wirelessly.

b. Software-Based Surveillance Technology: For the purposes of this statute, a piece of software will be considered Software-Based Surveillance Technology if it meets ANY of the following criteria:

1) There is a statutory requirement to obtain authorization by a higher authority prior to its use (i.e. a court order or search warrant);
2) It is, by design and as a primary function, capable of facial recognition, gait analysis, or biometric identification.
3) Third party software purchased or acquired by the City, that, by design and as primary functions, gathers, aggregates, and analyzes social media and other open source data in an indiscriminate manner.
4) Data Collected Through Hardware-Based Surveillance Technology, as described in this statute.

Data collected or maintained through Non-Surveillance Technology or through intra-City systems (i.e. Crime Statistics, Payroll/Accounting/Fiscal, PRIME) is NOT surveillance technology.

6. "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, 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;

Commented [SC16]: I think this is necessary because our cell phone photo apps as well as Facebook have facial recognition, but it is not their primary function.

Formatted: Font: (Default) Arial, 12 pt

Commented [TB17]: The word "public" should be removed here. Computers in staff member offices are not public.

6. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
7. The following are examples of existing technology that do not meet the above definition of surveillance technology:
   a. Interview room cameras
   b. Digital recorders
   c. ShotSpotter
8. The following do meet the above definition of surveillance technology but are exempt from annual reporting requirements:
   a. Body worn cameras
   b. Personal communication devices
   c. Security cameras

Commented [TB18]: These are included as additional exemptions because they do not meet the recommended definition of surveillance technology.

Commented [TB19]: Even though these would all have policies in place, annual reporting on each of them is overly burdensome and not terribly useful.

7. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

A. **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
B. **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
~~C. **Location:** The location(s) it may be deployed and crime statistics for any location(s);~~
~~D.~~C. **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.~~D. **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
~~F.~~E. **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.~~F. **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
~~H.~~G. **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

Commented [TB20]: OPD recommends removing this category and replacing it with another that meets the same or similar need. This is impractical and could compromise investigations. Much surveillance technology is mobile. Crime statistics for even static locations are impractical, as it is not a valid measurement for impact of a specific technology use. Providing information about where surveillance technology may be deployed could compromise ongoing or future investigations.

Commented [TB21]: It is unknown how such impact would be assessed or measured. This is essentially covered in Description if surveillance capability is included in the Description section as part of the policy specific to each technology.

Commented [TB22]: It is unknown how such mitigation would be assessed or measured. This is essentially covered in Description if surveillance capability is included in the Description section as part of the policy specific to each technology.

~~I.~~H. **Third Party Dependence:** Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

~~J.~~I. **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,

~~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).~~

8. "Surveillance Use Policy" means a publicly-released and ~~legally~~administratively-enforceable policy for use of the surveillance technology that at a minimum specifies the following, when applicable:

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:** ~~T~~Restrictions on 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

Commented [TB23]: Other entities are under no obligation to share information on their use of technology. Publishing information about technology owned or used by other agencies could compromise the other agencies' use of technology that is not publicly known.

For present technology, city departments will report on its success to date. For future technology, city departments will develop a mechanism for tracking success. Anticipated benefits would be provided in a way that does not compromise use by other agencies. City departments would obtain available surveillance impact reports from other agencies.

Commented [TB24]: "Legally enforceable" is not appropriate for policy. Not every section (A-K) will apply to every technology.

Commented [TB25]: It is incredibly difficult to identify the entire universe of all individuals who can access or use the info.

Commented [TB26]: What about impact of legal requirements for data retention and deviation from them?

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~~ administratively 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.

Commented [TB27]: Technology use – including investigations – would be compromised by the sharing of training materials.

Commented [TB28]: This requirement is too specific, such as "including internal personnel assigned to ensure compliance." "Legally enforceable" is not appropriate for policy.

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; or
   D. Entering into a written agreement or MOU ~~with a governmental agency or non-City entity~~ to acquire, share or ~~otherwise~~ use an item of surveillance technology with a governmental agency or non-City entity~~on a regular ongoing basis. or the information it provides.~~

2. City Council Approval Process

   A. After the PAC Notification and Review requirements in Section 9.64.020 have been met, City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Impact Report and proposed Surveillance Use Policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing.
   B. The City Council shall only approve any action as provided in this Chapter after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser

Commented [DJ29]: Removed formal and added MOU

Commented [DJ30]: This modification is to make it clear to an officer that simply receiving info from a non-city entity such as a convenience store video camera or sharing information with the DA would not require a written agreement ahead of time.

Commented [TB31]: OPD recommends rewording this section to focus on the specific item of technology as the subject of the MOU – such as the success we had with the cell site simulator.

economic cost or impact on civil rights or civil liberties would be as effective.

C. For Approval of Existing Surveillance Technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020.3.E, if the City Council has not reviewed and approved such item within sixty (60) days of the date it was scheduled for City Council consideration, the City may continue ~~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 other Urgent Need

(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 exigent circumstances or other urgent need without following the provisions of Section 9.64.030.

(b) If City staff acquires or uses a surveillance technology in exigent circumstances or other urgent use pursuant to subdivision (a), the City staff shall:

(1) Use the surveillance technology to solely respond to the exigent circumstances or other urgent need.

(2) Cease using the surveillance technology when the exigent circumstances or urgent need ends.

(3) Only keep and maintain data related to the exigent circumstances or other urgent need and dispose of any data that ~~is not related to the exigent circumstances~~ has no evidentiary value.

(4) Following the end of the exigent circumstances or other urgent need, report that acquisition or use to the PAC at its next regularly scheduled meeting for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines unless doing so would compromise an ongoing investigation.

(c) Any technology temporarily acquired in exigent circumstances shall be returned within seven days following its acquisition, or when the exigent

Commented [DJ32]: the concern raised is that if both the PAC and City Council fail to act in a timely manner, officers would suddenly be unable to use existing technology without violating the ordinance. legislative inertia could halt critical investigations/operations.

Commented [t33]: Exigent circumstances needs to be expanded to include other urgent need such as large-scale, short-notice pubic events and other unforeseeable urgent circumstances. Examples include the Warriors parade.

Commented [DJ34]: This clarifies that the technology *and the data it provides* can be used.

Commented [t35]: Evidence may legally required that does not relate to the exigency.

Commented [t36]: Next regularly scheduled PAC and/or Council meetings can take several weeks to get items scheduled – next regularly scheduled is not sufficient to address the bureaucratic process.

circumstances end, ~~whichever is sooner,~~ unless the technology is submitted to the PAC 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 PAC, who may grant an extension.~~

Commented [DJ37]: This proposed new language is to allow for flexibility during exigent circumstances when OPD may rely on technology or information generated by technology that is owned by a partner law enforcement agency such as NCRIC or the DA.

Commented [t38]: This reporting requirement (beyond seven days) is insufficient, as reporting out to a public entity during the course of the investigation would compromise the investigation.

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, City staff must schedule and submit a written Annual Surveillance Report for ~~City Council~~ review for each approved surveillance technology item. Any extension to the November 1 deadline must be approved by the City Administrator's Office.

    A. ~~Prior to submission of the Annual Surveillance Report to the City Council,~~ City staff shall initially submit the Annual Surveillance Report to the Privacy Advisory Commission for its review.

    B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the ~~Annual~~ Surveillance Use Policy that will resolve the concerns.

Commented [TB39]: Most of these recommended edits are just for clarification – it previously appeared from 1. that the report was being submitted to City Council by November 1. It was only by reading A. that it became clear the report went initially to the PAC.

The extension language is to address the competing demands of OPD – such as the 24 protests we had between Thanksgiving week and New Year's 2014.

Commented [TB40]: The word "annual" is removed here because it appeared to refer to policy – not the report. (Policies aren't submitted every year, the report is.)

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 to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city ~~agency~~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 ~~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 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. 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 if applicable, criminal fines and penalties. 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~~.

E. ~~To the extent individuals can be assessed criminal fines and penalties for violating the Oakland Municipal Code, such fines and penalties will apply for violations of this ordinance. Such fines and penalties would not apply for violations to specific surveillance technology use policies~~

Commented [DJ41]: There is a concern that this exposure to liability would stop our partner agencies from working with Oakland out of fear of needing to defend against lawsuits., it is a serious operational concern that warrants conversation.

Commented [DJ42]: Cities cannot be held liable for punitive damages.

Formatted: Strikethrough

Commented [DJ43]: This replaces the language with that in the DAC policy. It provides a range of possible consequences for violations as opposed to a fixed one of a misdemeanor charge.

~~promulgated by this ordinance but rather only violations of the ordinance itself.~~

~~D.~~ Unlawful use of surveillance technology can result in prosecution for violation of state and/or federal law.

Formatted: Font: (Default) Arial, 12 pt

Commented [t44]: This section is unnecessary, as state and federal law already provide necessary criminal penalties for misuse. This section would provide a chilling effect for City employees and partner agencies.

Formatted: Font: (Default) Arial, 12 pt

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.~~

Commented [DJ45]: All labor MOUs are already publicly disclosed.

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: