To: Honorable Mayor and Members of the City Council

From: Police Review Commission

Submitted by: George Lippman, Chairperson, Police Review Commission

Subject: Proposed Ordinance: Surveillance Technology Use and Community Safety

RECOMMENDATION

Adopt first reading of an ordinance governing the approval, acquisition, and use of surveillance technology by the City of Berkeley.

FISCAL IMPACTS OF RECOMMENDATION

Staff and commission time to carry out review and reporting requirements.

CURRENT SITUATION AND ITS EFFECTS

Presently, when surveillance technology is acquired and used by City departments, it is often done so without public discussion of the potential intrusions into civil liberties and privacy rights associated with the use of such technologies. While City departments use surveillance technology to advance their work, consideration is not always given to possible drawbacks, and whether those are outweighed by the benefits in using the particular technology. The proposed ordinance establishes a public process by which benefits are balanced against costs before any new surveillance technology is purchased or used, and applies that process to surveillance equipment currently in use.

BACKGROUND

Process

At its July 12, 2016 meeting, the City Council referred to the City Manager, the Police Review Commission, and the Peace and Justice Commission an item to consider adopting a community control of surveillance measure similar to that enacted by the County of Santa Clara. (Attachment 1.) On September 14, 2016, the Police Review Commission formed a Surveillance and Community Safety Ordinance Subcommittee. Four members of the Commission were appointed to the Subcommittee, along with three members of the public with interest and expertise in the subject.

After several meetings, the Subcommittee learned that the Fire Department used many more technologies subject to the draft ordinance than the Police Department and, on January 11, 2017, the PRC voted to refer the draft to the Disaster and Fire Safety
Commission, and to suspend its own work in the interim. The Disaster and Fire Safety Commission completed its review on March 22, 2017, and the PRC’s Surveillance and Community Safety Subcommittee resumed its work on April 12, 2017, proceeding diligently on a proposal, culminating in its presentation of a recommended draft ordinance to the full Commission on July 26, 2017.

At its July 26, 2017 meeting, the PRC voted unanimously to recommend that the City Council adopt the attached Surveillance Technology Use and Community Safety Ordinance. (Attachment 2.) (M/S/C Yampolsky/Halpern. Ayes: Allamby, Halpern (temp.), Lippman, Price, Prichett, Roberts, Yampolsky; Noes: None; Abstain: None; Absent: DaSilva, Ford, Perezvelez.)

Ordinance provisions
Under the ordinance, City Council approval is required before: seeking funding for surveillance technology; accepting funds for or donations of such technology; using surveillance technology in a way not previously approved; or agreeing with anyone outside the City to acquire, share or use surveillance technology or the information it provides. (Section 4.)

Before seeking Council approval, the City department must first seek review from the appropriate commission, e.g., the PRC for the Police Department, or the Disaster and Fire Safety Commission for the Fire Department. The department must submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed technology, to be considered by the reviewing commission at its next regular meeting. (Section 4.)

The Surveillance Impact Report describes the how the technology works; how and where it will be used; potential impacts on civil liberties and possible mitigation of such effects; types of data to be collected and how it will be secured; costs of the technology and funding sources; a summary of alternatives to the technology; and a summary of other entities’ experience with it. (Section 4.) The Surveillance Use Policy specifies the purpose of the technology; authorized and prohibited uses; information that may be collected, as well as who may access and collect the data; safeguards to protect the data; retention requirements; public accessibility; whether data will be shared with third parties; training to use the technology or use data; and how compliance with the Use Policy will be ensured. (Section 5.)

The reviewing commission may approve or object to proceeding, or take no action. Regardless of the commission’s decision or failure to act, the requesting department must still seek City Council approval and submit the Surveillance Impact Report and Surveillance Use Policy to the Council. (Sections 4 and 6.)

The City Council may approve a surveillance technology request only after considering the reviewing commission’s recommendation, and then making a determination that the benefits to the community outweigh the costs; that the proposal will safeguard civil
Proposed Ordinance on Surveillance Technology Use and Community Safety

January 23, 2018 (Continued from December 5, 2017)

liberties and civil rights; and that, in the Council’s judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective. (Section 7.)

Any City department possessing or using surveillance technology before the ordinance takes effect must seek approval for continued use, undergoing the review process for new technologies described above, and submit a Surveillance Impact Report and proposed Surveillance Use Policy to the City Council for approval within 180 days of the effective date of the ordinance. (Section 8.)

Following approval of a surveillance technology, the City Council must annually re-evaluate whether the technology continues to meet the thresholds required for initial approval. This occurs following the City department’s written Surveillance Report to the appropriate reviewing commission, which makes a recommendation to Council. The Council may direct that use of the technology cease or be modified if the balancing of interests and other concerns are not satisfied. The Council must annually publish a summary of all requests for approve of surveillance technology, as well as all Surveillance Reports submitted, and agendize them for discussion. (Section 9.)

In exigent circumstances, a City department may temporarily acquire or use surveillance technology without first going through the steps set forth above. Notice to the Council and the reviewing commission must, however, be provided within 30 days. If the use is anticipated to be ongoing, the department must submit a proposed Surveillance Use Policy to the reviewing commission, and then the Council, within 90 days. (Section 5.)

The proposed ordinance provides for a private right of action against the City if the ordinance or a Surveillance Use Policy is violated, but only after a 30-day notice of violation and opportunity to cure is given. A private right of action is also allowed against any third party who uses surveillance technology or data in violation of the ordinance. A person subjected to a surveillance technology in violation of the Ordinance, or about whom information has been gathered, may bring a suit for damages. (Section 10.)

As an additional enforcement mechanism, the Subcommittee’s recommendation to the Commission included a clause making a willful or intentional violation of the ordinance or Surveillance Use Policy a misdemeanor, punishable by a fine of up to $1000 per violation. This is the only provision that generated substantial disagreement in both the Subcommittee and the Commission. Proponents believe the criminal violations for flagrant violations shows that the City is serious about adhering to the ordinance, while opponents feel that criminalization is overkill and duplicative of existing law. In a 4-3 vote, the Commission voted to delete this provision from the draft ordinance presented to you. M/S/C (Yampolsky/Price) Ayes: Allamby, Halpern (temp.), Roberts, Yampolsky; Noes: Lippman, Price, Prichett; Abstain: None; Absent: Ford, DaSilva, Perezvelez.

Finally, the draft ordinance contains prohibitions on surveillance-related agreements that conflict with the ordinance and on non-disclosure agreements (Section 11); and
protects whistleblowers – employees who bring to light a violation of the ordinance – from adverse action by the City. (Section 12.)

ENVIRONMENTAL SUSTAINABILITY
No identifiable environmental effects or opportunities are associated with the subject of this report.

RATIONALE FOR RECOMMENDATION
The proposed ordinance responds to a Council referral. See Attachment 1.

CITY MANAGER
See companion report.

CONTACT PERSON
Katherine J. Lee, Police Review Commission Officer, 510-981-4960

Attachments:
1: July 12, 2016 Consent Calendar Item
2: Proposed Surveillance Technology Use and Community Safety Ordinance
To: Honorable Mayor and Members of the City Council  
From: Councilmember Kriss Worthington  
Subject: Referral to the City Manager, the Police Review Commission, and the Peace and Justice Commission to consider adopting a community control of surveillance measure similar to that of Ordinance No. NS-300.897 of Santa Clara County  

RECOMMENDATION:  
Referral to the City Manager, the Police Review Commission, and the Peace and Justice Commission to review and consider adopting a community control of surveillance measure similar to that of Ordinance No. NS-300.897 of Santa Clara County.

BACKGROUND:  
Santa Clara County Board of Supervisors unanimously approved a law which governs surveillance equipment used by police and other law enforcement officials - such as drones, license plate readers, cellphone trackers - including a broad public debate prior to equipment implementation. The law also requires, board approval of a Surveillance Use Policy that safeguards civil liberties and civil rights, and ongoing accountability including an annual audit. This law is vital in assuring civil liberties are not hindered and that there is the utmost transparency between law enforcement officials and the citizens which they serve. Santa Clara County Supervisor Joe Simitian spearheaded this effort because there would be a great deal of transparency and accountability.

Implementing a law similar to Ordinance No. NS-300.897 in Berkeley would provide the community with a strong footing in the public debate regarding transparency between citizens and law enforcement officials. The ACLU of California has issued recommendations for municipal ordinances regarding community control of surveillance, and the Santa Clara ordinance was modeled based on the ACLUs suggestions. Many of the technologies that are covered under this law pose serious risks for the health and safety of residents. Since April 2014, the Federal Aviation Administration reported that almost 1,000 near misses or other incidents nationally occurred with approximately 20 percent of those incidents coming from California. Drones and other surveillance technology pose risks to the constitutional rights to the citizens of Berkeley as well.

For more information:  
Santa Clara Ordinance http://tinyurl.com/znee97e  
FINANCIAL IMPLICATIONS:
Minimal.

ENVIROMENTAL SUSTAINABILITY:
Consistent with Berkeley’s Environmental Sustainability Goals and no negative impact.

CONTACT PERSON:
Councilmember Kriss Worthington  510-981-7170
ORDINANCE NO.       -N.S.
SURVEILLANCE TECHNOLOGY USE AND COMMUNITY SAFETY ORDINANCE

BE IT ORDAINED by the Council of the City of Berkeley as follows:

Section 1. Title

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

Section 2. Findings

The City Council finds as follows:

1) Through the enactment of this ordinance, the City seeks to establish a thoughtful process regarding the procurement and use of surveillance technology that carefully balances the City’s duty to protect public safety with its duty to protect the privacy and civil rights of its community members.

2) Transparency is essential when the City is considering procurement and use of surveillance technology.

3) Although such technology may be beneficial to public order and safety, it has the potential to put both privacy and civil liberties at risk. In U.S. history, government surveillance has had a disproportionately repressive effect on marginalized racial, ethnic, religious, and LGBT communities and social change movements.

4) No decisions relating to surveillance technology should occur without strong consideration of the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions.

5) Surveillance technology involves immediate, as well as ongoing, financial costs. Before the City acquires any surveillance technology, it must evaluate all costs associated with the procurement, installation, use and maintenance of the technology.

6) Decisions regarding whether and how surveillance technologies should be funded, acquired, or used should give significant weight to public input.

7) Legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is acquired or deployed.
8) 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 observed.

Section 3. Definitions

The following definitions apply to this Ordinance:

1) “Surveillance Report” means an annual written report concerning a specific surveillance technology that includes all of the following:

   a) A description of how the surveillance technology was used, including the quantity of data gathered or analyzed by the technology;

   b) Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, and the justification for the disclosure(s);

   c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

   d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by whatever geographical unit is used by the City entity;

   e) A summary of each community complaint received by the City entity or applicable reviewing commission about the surveillance technology;

   f) The results of any non-privileged 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 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;

   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 request by the City entity for modifications to the Surveillance Use Policy and a detailed basis for the request.
2) “City entity” means any department, bureau, division, or unit of the City of Berkeley.

3) “Surveillance technology” means any electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of covered surveillance technology include, but are not limited to: 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.

   a) “Surveillance technology” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 8(3): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (f) municipal agency databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology; or (g) electrocardiogram machines.

4) “Surveillance Impact Report” means a publicly-released written report that, if the surveillance technology were to be used or deployed, includes 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 reasons for deployment in the 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;

e) Mitigation: Information regarding specific, affirmative technical and procedural measures that will be implemented to appropriately safeguard the public from any impact identified in subsection (d);

f) Data Types and Sources: A list of all sources of data to be collected, analyzed, or processed by the surveillance technology, including “open source” data;

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 why the proposed technology is preferable; and,

k) Track Record: A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

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

a) Purpose: The specific purpose(s) that the surveillance technology is intended to advance;

b) Authorized Use: The uses that are authorized, the rules and processes required prior to such use, and the uses that are prohibited;
c) **Data Collection:** The information that may 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 may 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 may be accessed or used by members of the public;

h) **Third Party Data Sharing:** If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials;

j) **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including the job title category and number of 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.

6) “Exigent circumstances” means a City entity’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires use of the surveillance technology or the information it provides.
7) “Appropriate reviewing commission” means the existing citizens commission with reviewing responsibilities over the City entity. If no such commission exists, the City Manager may designate a citizens commission to act as the reviewing commission or ask the City entity to submit reports directly to the City Manager.

8) “Personal communication devices” means mobile telephones, personal digital assistants, wireless capable tablets and similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that are used in the regular course of business.

Section 4. City Council Approval Requirement

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

Upon notification by the City entity, the Chair shall place the item on the agenda at the next meeting for which it may be properly noticed, for discussion and possible action. At this meeting, the City entity shall inform the reviewing commission of the cost of the proposal, the need for the funds or equipment, or shall otherwise justify the action the entity intends to take. The reviewing commission may vote its approval to proceed, object to the proposal, recommend that the entity modify its proposal, or take no action. Neither opposition to the act or failure by the reviewing commission to act shall prohibit the City entity from proceeding. The City entity is still bound by subsection (2) regardless of the action taken by the reviewing commission under this subsection.

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

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

Section 5. Temporary Acquisition and Use of Surveillance Equipment

Notwithstanding the provisions of this ordinance, a City entity may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this ordinance before that acquisition or use. However, a City entity that acquires or uses surveillance technology in exigent circumstances must: (1) provide notice of that acquisition and use to the City Council and appropriate reviewing commission in writing within 30 days following the commencement of those circumstances; (2) if it is anticipated that the use will continue beyond the exigent need, submit a proposed Surveillance Use Policy to the City Council regarding that surveillance technology within 90 days following the commencement of those circumstances pursuant to Section 4; and (3) include that surveillance technology in the City entity’s next annual Surveillance Report to the City Council following the commencement of those circumstances.

Section 6. Information Required

1) Prior to seeking City Council approval under Section 4, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the appropriate reviewing commission for its review at a regularly noticed meeting.

2) The reviewing commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy.

3) After receiving the recommendation of the reviewing commission, the City entity seeking approval under Section 4 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy at least forty-five (45) days prior to the City Council meeting. The City Council shall publicly release in print and online the Surveillance Impact Report, proposed Surveillance Use Policy, and reviewing commission recommendation at least thirty (30) days prior to the City Council meeting.

4) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the City entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 4.
Section 7. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 4 (2) or Section 5 of this ordinance after first considering the recommendation of the appropriate reviewing commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will appropriately safeguard civil liberties and civil rights; and that, in the City Council’s judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 8. Compliance for Existing Surveillance Technology

Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy in compliance with Section 6 and no later than one hundred eighty (180) days following the effective date of this ordinance for review and approval by the City Council pursuant to Section 4. If such review and approval has not occurred within ninety (90) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 9. Oversight Following City Council Approval

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

   a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the appropriate reviewing commission for its review.

   b) The reviewing 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 appropriately safeguarded; that use of the surveillance technology cease; or propose modifications to the Surveillance Use Policy that will resolve the concerns.

2) Based upon information provided in the Surveillance Report and after considering the recommendation of the reviewing commission, the City Council shall determine whether the requirements of Section 7 are satisfied. If the requirements of Section 7 are not satisfied, the City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.
3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior calendar year:
   a) A summary of all requests for City Council approval pursuant to Section 4 or Section 8 and the pertinent reviewing commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval; and
   b) All Surveillance Reports submitted.

Section 10. Enforcement

1) 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 city entity, the City of Berkeley, 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, except a city employee, with possession, custody, or control of data subject to this Ordinance.
   a) Prior to the initiation of any legal proceeding under subsection 1), the City of Berkeley or City entity must be given notice of the violation(s) and an opportunity to correct such violation(s) within 30 days of receipt of the notice.

2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover actual damages.

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

Section 11. 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 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.
Section 12. Whistleblower Protections

1) It shall be a violation of Section 12 for the City or anyone acting on behalf of the City to take or fail to take, or threaten to take or fail to take, an adverse employment action with respect to any employee or applicant for employment, 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.

Section 13. Severability

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 14. Construction

The provisions of this Ordinance, including the terms defined in Section 3, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 15. Effective Date

This Ordinance shall take effect on [DATE].