



Office of the Mayor

## **REVISED AGENDA MATERIAL**

**Meeting Date: March 13, 2018**

**Item Number: 27c**

**Item Description: Proposed Ordinance: Surveillance Technology Use and  
Community Safety**

**Submitted by: Mayor Jesse Arreguin**

The proposed ordinance has been revised to reflect input from Police Review Commissioners, civil liberties organizations and privacy advocates.

ORDINANCE NO. -N.S.

ADDING CHAPTER 2.99 TO THE BERKELEY MUNICIPAL CODE, ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

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. That Chapter 2.99 is hereby added to the Berkeley Municipal Code to read as follows:

**Chapter 2.99**

**Acquisition and Use of Surveillance Technology**

**2.99.010 Purposes**

- A) Through the enactment of this Chapter, the City seeks to establish a thoughtful process regarding the procurement and use of Surveillance Technology that carefully balances the City's interest in protecting public safety with its interest in protecting the privacy and civil rights of its community members.
- B) Transparency is essential when the City is considering procurement and use of Surveillance Technology.
- C) Although such technology may be beneficial to public order and safety, it has the potential to put both privacy and civil liberties at risk.
- D) Decisions relating to Surveillance Technology should occur with strong consideration of the impact such technologies may have on civil rights and civil liberties, as with all rights guaranteed by the California and United States Constitutions.
- E) Surveillance Technology may involve 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.
- F) Decisions regarding whether and how Surveillance Technologies should be funded, acquired, or used should be governed by the City Council as the elected representatives of the City.

- G) In addition to applicable local, state, and federal law, legally enforceable safeguards, including robust transparency, oversight, and accountability measures, are important in the protection of civil rights and civil liberties.
- H) Data reporting measures will enable the City Council and public to confirm that mandated civil rights and civil liberties safeguards have been strictly observed.

## 2.99.020 Definitions

The following definitions apply to this Chapter:

- 1) “City Entity” means any department, bureau, division, or unit of the City of Berkeley.
- 2) “Surveillance Technology” means an electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to ~~remotely and surreptitiously~~ collect 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; body worn cameras; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems, except as allowed under Section 2(d); social media analytics software; gait analysis software; and video cameras that record audio or video and can remotely transmit or can be remotely accessed.

“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 2 (above):

- (a) Routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance functions;
- (b) Handheld Parking Citation Devices, that do not automatically read license plates;
- (c) Manually-operated, portable digital cameras, audio recorders, and video recorders that are not to be used remotely and whose functionality is limited to manually capturing, viewing, editing and downloading video and/or audio recordings, but not including body worn cameras;
- (d) Devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles or thermal imaging cameras used for fire operations, search and rescue operations and missing person; ~~or probable cause searches~~

(e) Manually-operated technological devices that are not designed and will not be used to surreptitiously collect surveillance data, such as two-way radios, email systems and city-issued cell phones;

(f) Municipal agency databases;

(g) Medical equipment used to diagnose, treat, or prevent disease or injury, including electrocardiogram machines.

(h) Cybersecurity capabilities, technologies and systems used by the City of Berkeley Department of Information Technology to predict, prevent, and protect the City of Berkeley and its community members from potential cybersecurity events (e.g. reconnaissance or monitoring systems, intrusion, interference or attack on our systems); and cybersecurity capabilities, technologies and systems used by the City of Berkeley in cybersecurity monitoring and cyber-forensic based investigations and prosecutions of illegal activity;

(i) Stationary security cameras affixed to City property or facilities.

3) “Surveillance Technology Report” means an annual written report by the City Manager covering all of the City of Berkeley’s Surveillance Technologies that includes all of the following information with regard to each type of Surveillance Technology:

(a) **Description:** A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about ~~categories of~~ recipient entities, including the names of the entities and purposes for such sharing;

(b) Geographic Deployment: Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically;

~~(c)~~ **Complaints:** A summary of each complaint, if any, received by the City about the Surveillance Technology;

~~(d)~~ **Audits and Violations:** 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;

(e) Data Breaches: 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;

~~(f)~~ **Effectiveness:** Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes;

(eg) **Costs:** Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

4) “Surveillance Impact Report” means a publicly-released written report produced prior to acquisition or permanent use in Exigent Circumstances of a type of Surveillance Technology that 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 general location(s) it may be deployed and reasons for deployment;

(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 technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified in subsection (d);

(f) **Data Types and Sources:** A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including “open source” data;

(g) **Data Security:** Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure;

(h) **Fiscal Cost:** The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding;

(i) **Third Party Dependence and Access:** 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, and whether a third-party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats;

(j) **Alternatives:** A summary of potentially viable alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed Surveillance Technology, including an overview of the costs and benefits associated with each potentially viable alternative; and,

(k) **Experience of Other Entities:** To the extent such information is available, a summary of the experience of other government entities with the proposed technology, including any unanticipated financial or community costs and benefits.

5) "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of each type 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:** Information collection that is allowed and prohibited. Where applicable, list any data sources the technology will rely upon, including "open source" data;

(d) **Data Access:** A general description of the title and position of the employees and entities authorized to access or use the collected information, and the rules and processes required prior to access or use of the information, and a description of any and all of the vendor's rights to access and use, sell or otherwise share information for any purpose;

(e) **Data Protection:** A general description of the safeguards that protect information from unauthorized access, including encryption and access control mechanisms, and safeguards that exist to protect data at the vendor level;

(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 such 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 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;

(h) **Training:** Training required for any employee authorized to use the Surveillance Technology or to access information collected;

(j) **Auditing and Oversight:** Mechanisms to ensure that the Surveillance Use Policy is followed, technical measures to monitor for misuse, and the legally enforceable sanctions for intentional violations of the policy; and

(k) **Maintenance:** The mechanisms and procedures to ensure maintenance of the security and integrity of the Surveillance Technology and collected information.

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.

### **2.99.030 City Council Approval Requirement**

1) A City Entity must obtain City Council approval, except in Exigent Circumstances, by placing an item on the Action Calendar at a duly noticed meeting of the City Council prior to any of the following:

(a) Seeking, Soliciting, or Accepting-accepting state or federal grant funds for the purchase of, 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 Surveillance Technology previously approved by the City Council for a purpose, or in a manner 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, or expanding a vendor’s permission to share or otherwise use Surveillance Technology or the information it provides.

2) A City Entity must present a Surveillance Use Policy for each Surveillance Technology to the appropriate reviewing commission prior to adoption by the City Council. No later than 30 days after receiving a Surveillance Use Policy for review, the reviewing commission must vote to recommend approval of the policy, object to the proposal, recommend modifications, or take no action. Neither opposition to approval of such a policy, nor failure by the reviewing commission to act shall prohibit the City Entity from proceeding with its own review and potential adoption.

23) A City Entity must submit for review a Surveillance Impact Report and obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in Ssubsection (1) (a)-(d).

### **2.99.040 Temporary Acquisition and Use of Surveillance Equipment**

Notwithstanding the provisions of this Chapter, a City Entity may borrow, acquire and/or temporarily use Surveillance Technology in Exigent Circumstances without following the requirements in Sections [2.99.030\(4\)](#) and [2.99.040\(5\)](#). However, a City Entity that borrows, acquires or temporarily uses Surveillance Technology in Exigent Circumstances must take all of the following actions:

- 1) Provide written notice of that acquisition or use to the City Council within 30 days following the commencement of such Exigent Circumstance;
- 2) If it is anticipated that the use will continue beyond the Exigent Circumstance, submit a proposed Surveillance Impact Report and Surveillance Use Policy, as applicable, to the City Council within 90 days following the borrowing, acquisition or temporary use, and receive approval, as applicable, from the City Council pursuant to Sections [2.99.030 \(4\)](#) and [2.99.040\(5\)](#); and
- 3) Include the Surveillance Technology in the City Manager's next annual Surveillance Technology Report.

#### **2.99.050 Compliance for Existing Surveillance Technology**

The City Manager shall submit to the Action Calendar for the first City Council meeting in November of 2018, a Surveillance Impact Report and a proposed Surveillance Use Policy for each Surveillance Technology possessed or used prior to the effective date of this ordinance.

#### **2.99.060 Determination by City Council that Benefits Outweigh Costs and Concerns**

The City Council shall only approve any action described in Section [2.99.030, 4 or 2.99.040, or Section 2.99.050](#) ~~Section 5~~ of this Chapter after making a determination that the benefits to the community of the Surveillance Technology, used according to its Surveillance Use Policy, outweigh the costs; that the proposal will appropriately safeguard civil liberties and civil rights to the maximum extent possible while serving its intended purposes; and that, in the City Council's judgment, no feasible alternative with similar utility and a lesser impact on civil rights or civil liberties could be implemented.

#### **2.99.070 Oversight Following City Council Approval**

The City Manager must submit to the Council Action Calendar a written Surveillance Technology Report, covering all of the City's Surveillance Technologies, annually at the first regular Council meeting in November. After review of the Surveillance Technology Report, Council may make modifications to Surveillance Use Policies or direct that the use of one or more Surveillance Technologies cease.

#### **2.99.080 Public Access to Surveillance Technology Contracts**



To the extent permitted by law, the City shall continue to make available to the public all of its surveillance-related contracts, including related non-disclosure agreements, if any.

### **2.99.090 Enforcement**

This Chapter does not confer any rights upon any person or entity other than the City Council to cancel or suspend a contract for a Surveillance Technology. The Chapter does not provide a private right of action upon any person or entity to seek injunctive relief against the City or any employee unless that person or entity has first provided written notice to the City Council by serving the City Clerk, regarding the specific alleged violations of this Chapter. If a specific alleged violation is not remedied within 90 days of that written notice, a person or entity may seek injunctive relief in a court of competent jurisdiction. If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous manner on the City's website that describes the corrective measures taken to address the violation. If it is shown that the violation is the result of ~~arbitrary or capricious action or willful~~ conduct by the City or an employee or agent thereof in his or her official capacity, the prevailing complainant in an action for relief may collect from the City reasonable attorney's fees in an amount not to exceed ~~\$7,500~~ 15,000 if he or she is personally obligated to pay such fees.

### **2.99.100 Whistleblower Protections**

All provisions of Berkeley's Protection of Whistleblowers Workplace Policy, as promulgated by the City Manager on November 2, 2016 and including any updates or replacements thereto, shall apply to employees reporting good faith suspicions of violations of this ordinance or of misconduct or misuse of any Surveillance Technology.

### **2.99.110 Severability**

If any word, phrase, sentence, part, section, subsection, or other portion of this Chapter, or any application thereof to any person or circumstance is declared void, unconstitutional, or invalid for any reason, then such word, phrase, sentence, part, section, subsection, or other portion, or the prescribed application thereof, shall be severable, and the remaining provisions of this Chapter, and all applications thereof, not having been declared void, unconstitutional or invalid, shall remain in full force and effect. The City Council hereby declares that it would have passed this title, and each section, subsection, sentence, clause and phrase of this Chapter, irrespective of the fact that any one or more sections, subsections, sentences, clauses or phrases is declared invalid or unconstitutional.

Section 3. Copies of this Ordinance shall be posted for two days prior to adoption in the display case located near the walkway in front of Council Chambers, 2134 Martin Luther King Jr. Way. Within 15 days of adoption, copies of this Ordinance shall be filed at each branch of the Berkeley Public Library and the title shall be published in a newspaper of general circulation.