



Disaster and Fire Safety Commission

ACTION CALENDAR
May 2, 2017

To: Honorable Mayor and Members of the City Council
 From: Disaster and Fire Safety Commission
 Submitted by: Paul Degenkolb, Chairperson, Disaster and Fire Safety Commission
 Subject: Proposed Surveillance and Community Safety Ordinance – Requested
 Assessment of Administrative Burden

RECOMMENDATION

At this time the Disaster and Fire Safety Commission takes no position on the proposed Surveillance and Community Safety Ordinance, but we have concerns about the impacts that this draft ordinance may have on the Berkeley Fire Department. The Disaster and Fire Safety Commission recommends that City Council direct the City Manager to assess the administrative impact of the proposed Surveillance and Community Safety Ordinance that is currently in draft form.

This assessment should include

- (a) a legal review to identify surveillance technology that is currently owned or used by city departments
- (b) an estimate by the City Manager of the administrative burden (including both fiscal and time-based costs) created by this ordinance on city departments, Commissions, and the City Council.

FISCAL IMPACTS OF RECOMMENDATION

The proposed Surveillance and Community Safety Ordinance will create an as of yet unknown cost due to the administrative actions that it requires by City staff. The recommendation here is for the City Manager to assess that cost.

CURRENT SITUATION AND ITS EFFECTS

There is currently no publicly-reviewed usage plan or formal internal policy for surveillance technology usage by Berkeley Fire Department.

Berkeley Fire Department currently uses surveillance technology regularly and extensively in life-safety operations, including examples such as:

- Use of thermal imaging devices to see hotspots in a fire or to see if there is a person or pet inside a building who needs to be rescued
- Use of drones to view locations, such as collapsed portions of buildings in a fire, that can't be safely reached by responders

- Using a drone to sample air overhead to determine if there is a toxin in the air, for example to determine if a toxic smoke condition exists from a Richmond Refinery fire
- Using a drone to search for a car or a person in search and rescue, for example, if a car has fallen down a cliff over Grizzly Peak at an inaccessible location, or in a water rescue to rapidly search for a person lost in the Bay
- GoPro cameras being worn by firefighter trainees to assess their activities, location and safety
- Use of medical monitoring tools that transmit medical data about a patient in the course of their emergency medical care and transport.

As a recent example, in the First Congregationalist Church fire on September 30, 2016, the Department used a thermal camera-equipped drone (from the Alameda County Sheriff's Office) to identify hot spots and better direct their water sprays. Use of drones by the Department was approved for disaster response purposes by the Berkeley City Council on February 24, 2015 and extended on February 9, 2016.

We are not aware of any complaint ever brought to Berkeley's Fire Department or City Council about inappropriate use of surveillance technology by the Berkeley Fire Department, or any specific concern that BFD is misusing surveillance technology at this time or will do so in the near future.

BACKGROUND

At the March 22, 2017 regular meeting of the Disaster and Fire Safety Commission, the commission voted to recommend that City Council direct the City Manager to assess the administrative impact of the proposed Surveillance and Community Safety Ordinance that is currently in draft form.

This assessment should include:

- (a) a legal review to identify surveillance technology that is currently owned or used by city departments
- (b) an estimate by the City Manager of the administrative burden (including both fiscal and time-based costs) created by this ordinance on city departments, Commissions, and the City Council.

Motion: G. Couzin, Second: R. Grimes,
Vote: (7 Ayes: Flasher, Jones, Golomb, Legg, Degenkolb, Couzin, Grimes; 0 Noe: Griffin; 0 Absent; 0 Abstain)

The proposed Surveillance and Community Safety Ordinance would create a process that requires all city departments to get Council approval via a public process prior to acquiring any surveillance technology, requires a review of existing surveillance technology, and requires yearly reports on usage. The ordinance does permit for the temporary use and acquisition of surveillance technology in exigent circumstances.

There is no specific or immediate concern about surveillance by Berkeley Fire Department; however, members of the community have expressed concern about the potential for abuse of civil liberties by government entities including BFD, in absence of an oversight process.

The Police Review Commission has sent a draft version of a Surveillance and Community Safety Ordinance to the Disaster and Fire Safety Commission for our review. In order to provide feedback on the proposed ordinance, the Disaster and Fire Safety Commission would like to better understand the administrative burden that this ordinance would create.

ENVIRONMENTAL SUSTAINABILITY

There is no environmental impact of this recommendation.

RATIONALE FOR RECOMMENDATION

The Disaster and Fire Safety Commission supports the goal of the proposed Surveillance and Community Safety Ordinance, which is to ensure that surveillance technology is used for the best interests of the public. We would like to ensure that if passed, it does not create an excessive administrative burden on the Fire Department.

We think any surveillance ordinance should strike a balance between the desire for a robust and thorough review process and the administrative burden it creates. In order to understand this balance, we think it's important to have a clear assessment of the administrative cost.

The use of surveillance tools is common and extensive at the Fire Department. The ordinance could create an unreasonable administrative burden for Fire Department staff who are already tightly stretched and chronically understaffed. The administrative burden is not just in the creation of the usage plan and proposal, but also the time spent shepherding a proposal through a multi-step, multi-month approval process, as well as documentation of use throughout the year.

Depending on what we learn from the City Manager regarding the resources that the Surveillance Ordinance is expected to use, we may ultimately support the ordinance in its present form, or we may suggest edits to the ordinance to make it a smaller administrative burden, or we may support it conditionally (e.g. only if more staff budget is approved), or we may oppose the ordinance and seek an alternate approach.

ALTERNATIVE ACTIONS CONSIDERED

We considered:

- (1) recommending fully exempting the BFD from this ordinance due to the administrative burden

- (2) supporting the adoption of the ordinance conditional on the Council gaining an assessment of the administrative burden and considering it in their deliberations

For both of these options, we deemed that it would be better to gain a clear understanding of the administrative burden before making either recommendation.

CITY MANAGER

The City Manager concurs with the content and recommendations of the Commission's Report and recommends that the item be referred to the Council Referral process.

CONTACT PERSON

Paul Degenkolb, Chairperson, Disaster and Fire Safety Commission
Keith May, Assistant Fire Chief, Berkeley Fire Department, 981-5508

Attachments:

- 1: Draft Ordinance

City of Berkeley

Surveillance 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 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 sSuch technology-imay bes often proposed as beneficial to public order and safety, it has but have 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. City Council Approval Requirement

- 1) A City entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public hearing prior to any of the following:

- a) Seeking funds for surveillance technology, including but not limited to applying for a grant or soliciting or accepting state or federal funds or in-kind or other donations;
 - 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) Soliciting proposals for or entering into an agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.
- 2) A City entity must obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (1)(b)-(d).

Section 4. Information Required

- 1) The City entity seeking approval under Section 3 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 public hearing. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.
 - a) Prior to seeking City Council approval under Section 3, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Police Review Commission for its review at a regularly noticed meeting.
 - b) The Police Review Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy.
- 2) After receiving the recommendation of the Police Review Commission, the City Council shall publicly release in print and online the Surveillance Impact Report, proposed Surveillance Use Policy, and Police Review Commission recommendation at least thirty (30) days prior to the public hearing.
- 3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 3(1).

Section 5. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 3, subsection (1) or Section 6 of this ordinance after first considering the recommendation of the Police Review Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 6. 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 4 (1) (a-b), 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 5. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 7. Oversight Following City Council Approval

- 1) A City entity which obtained approval for the use of surveillance technology must submit a written Surveillance Report for each such surveillance technology to the City Council within twelve (12) months of City Council approval and annually thereafter on or before November 1.
 - a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the Police Review Commission for its review.
 - b) The Police Review Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the Surveillance Use Policy that will resolve the concerns.
- 2) Based upon information provided in the Surveillance Report and after considering the recommendation of the Police Review Commission, the City Council shall determine whether the requirements of Section 5 are still satisfied. If the requirements of Section 5 are not satisfied, the City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.
- 3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:
 - a) A summary of all requests for City Council approval pursuant to Section 3 or Section 6 and the pertinent Police Review 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 8. Definitions

The following definitions apply to this Ordinance:

- 1) “Surveillance Report” means a 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, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

- c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
 - d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau;
 - e) A summary of community complaints or concerns about the surveillance technology, and an analysis of any discriminatory uses of the technology and effects on the public's civil rights and civil liberties, including but not limited to those guaranteed by the California and Federal Constitutions;
 - f) The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;
 - g) Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - h) Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - i) Statistics and information about public records act requests, including response rates;
 - j) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
 - k) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
- 2) "City entity" means any department, bureau, division, or unit of the City of Berkeley.
- 3) "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar 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.
- 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.

- 4) "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:
- a) **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - b) **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
 - c) **Location:** The location(s) it may be deployed and crime statistics for any location(s);
 - d) **Impact:** An assessment identifying any potential impact on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm. In addition, identify specific, affirmative measures that will be implemented to safeguard the public from each such impacts;
 - e) **Data Sources:** A list of all sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data;
 - 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;
 - 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;
 - 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;
 - 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,
 - j) **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 can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including “open source” data;
- d) **Data Access:** The individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- e) **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
- f) **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;
- g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
- h) **Third Party Data Sharing:** If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials;
- j) **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
- k) **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Section 9. 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 respective city agency, 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 with possession, custody, or control of data subject to this Ordinance.
- 2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used

in violation of this Ordinance or of a Surveillance Use Policy, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater) and punitive damages.

- 3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) or (2).
- 4) In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$1,000 per violation.

Section 10. Secrecy of Surveillance Technology

It shall be unlawful for the City of Berkeley or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Ordinance shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Ordinance.

Section 11. Whistleblower Protections.

1) No municipal entity or anyone acting on behalf of a municipal entity 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, conditions, access to information, restrictions on due process rights, privileges of employment, 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 municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Ordinance.

3) Any employee or applicant who is injured by a violation of Section 11 may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

Section 12. 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 13. Construction

The provisions of this Ordinance, including the terms defined in Section 8, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 14. Effective Date

This Ordinance shall take effect on [DATE].