



City of Cambridge

Executive Department

LOUIS A. DePASQUALE
City Manager

LISA C. PETERSON
Deputy City Manager

June 25, 2018

To the Honorable, the City Council:

I am pleased to submit to you a revised draft of the proposed Surveillance Technology Ordinance (“the Ordinance”), which I have attached in both clean and redlined version together with an explanatory memorandum from City Solicitor Nancy Glowa describing the lengthy and detailed process that went into drafting the proposed changes following multiple meetings and teleconferences held by City staff with Kade Crockford from the American Civil Liberties Union of Massachusetts (the “ACLU”). As you may recall, previous versions of the Ordinance were submitted to the Council, including an earlier iteration of the Ordinance that was discussed at a Public Safety Committee hearing on October 18, 2017, and one which was discussed at the April 17, 2018 Public Safety Committee Hearing. If the enclosed Ordinance is passed, Cambridge will be among the first municipalities in Massachusetts to adopt an ordinance governing the acquisition and use of surveillance technology by City departments.

At the April 17, 2018 Public Safety Committee Hearing, the feedback on the Ordinance was very positive. The ACLU submitted written comments, largely in support of the Ordinance and suggesting revisions in nine areas. City Staff have significantly revised the Ordinance in order to address several of the suggestions submitted by the ACLU during the Committee Meetings and during other meetings and conference calls. We have worked hard with the ACLU to understand, discuss, and address their concerns. While we are in agreement on most elements of the Ordinance, there are a few remaining disagreements, which are summarized in the attached memorandum from the City Solicitor to me.

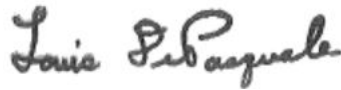
The most significant areas of disagreement are discussed in 1) Section (C) (2) at page 5 of the City Solicitor’s memorandum, which relates to the ACLU’s suggestion that the City Council have the ultimate authority to approve or disapprove the acquisition and use of certain surveillance technologies notwithstanding the position of the Police Commissioner and/or the City Manager that such surveillance technologies are needed for the investigatory and prosecutorial functions of the Police Department. As explained in her memorandum, the City



Solicitor advises that this could run afoul of the City's Plan E Charter, as these issues appear to relate more to operational issues and the City Manager's discretion to make such decisions than to the broad policy making role of the City Council; and 2) Section (E) at pages 7-9 of the City Solicitor's memorandum entitled "Enforcement", which discusses the ACLU's request for the Ordinance to provide a private cause of action so that individuals could sue not only the City but both elected and appointed City officials for violations of the Ordinance, including the award of attorneys' fees, and would provide for whistleblower protections. As discussed in the City Solicitor's memorandum, she believes that there are already sufficient remedies available to members of the public who may feel injured by a violation of the Ordinance, and the remedies suggested by the ACLU present potential conflicts with laws governing liability of public employers and employees.

I look forward to further discussion with the City Council as we work to ensure the safety and security of the public while protecting privacy, civil liberties and civil rights.

Very truly yours,

A handwritten signature in cursive script that reads "Louis A. DePasquale".

Louis A. DePasquale
City Manager

LAD/mec
Attachment(s)

Nancy E. Glowa
City Solicitor

Arthur J. Goldberg
Deputy City Solicitor

Vali Buland
First Assistant City Solicitor



Assistant City Solicitors

Paul S. Kawai
Samuel A. Aylesworth
Keplin K. U. Allwaters
Sean M. McKendry
Megan B. Bayer
Brian A. Schwartz

Public Records Access Officer

Jennifer Simpson

CITY OF CAMBRIDGE

Office of the City Solicitor
795 Massachusetts Avenue
Cambridge, Massachusetts 02139

June 25, 2018

Louis A. DePasquale
City Manager
City Hall
795 Massachusetts Avenue
Cambridge, MA 02139

Re: *Surveillance Ordinance - Explanatory Comments and Responses to Issues Raised by the ACLU at the 4/17/18 Public Safety Committee Meeting*

Dear Mr. DePasquale:

I am pleased to submit to you revisions to the proposed draft Surveillance Technology Ordinance (the "Ordinance"), both redlined and clean drafts of which are attached hereto for your review and submission to the City Council for its consideration.

By way of background, and as you are aware, City staff including you, Deputy City Manager Lisa Peterson, Police Commissioner Branville Bard, and members of this office have been meeting and conferring with Kade Crockford of the American Civil Liberties Union of Massachusetts (the "ACLU") on several occasions over the last year and a half, including numerous teleconferences with Ms. Crockford in order to discuss the concerns the ACLU and Digital Fourth have expressed with regard to the Ordinance. The ACLU had submitted questions concerning the Ordinance during the October 18, 2017 Public Safety Committee hearing to which the City responded in meetings and telephone conferences thereafter. During the April 17, 2018 Public Safety Committee hearing the Committee requested that a revised version of the Ordinance be prepared for a City Council meeting to be held in late May or early June. At the April 17, 2018 Committee Hearing, the ACLU also submitted a number of specific questions related to the Ordinance; City staff met with the ACLU on June 14, 2018 to discuss those questions as well as other questions that had previously been submitted to City staff, and City staff then had a teleconference with Ms. Crockford on June 18, 2018 to discuss the proposed revisions City staff made to the Ordinance in order to address the ACLU's questions.

Set forth in detail below are questions and issues raised by the ACLU together with our responses to the same and further explanation, if any, regarding the City staff's recommendations as to those issues.

A. DEFINITIONS.

1. Section 12.22.020(B)—Definitions—Exigent Circumstances: Whether to Include Significant Property Damage or Loss in the Definition of Exigent Circumstances (p. 2 of the redlined Ordinance).

The ACLU suggested that “significant property damage or loss” should be removed from the Ordinance’s definition of Exigent Circumstances in Section 12.22.020(B).

- City staff do not recommend that “significant property damage or loss” be removed from the definition of Exigent Circumstances in Section 12.22.020(B) of the Ordinance. By way of example, in the event that the Police Department receives a tip that a large property may be destroyed by one or more individuals, and such property destruction poses public health or similar risk to the general public, the Police Department needs the ability, under Section 12.22.040 of the Ordinance, to acquire and use on a temporary basis Surveillance Technology not previously approved by the Council, in order to mitigate or remove the risk that such property destruction poses. Indeed, other Surveillance Ordinances recently adopted in Berkeley and Davis, California, contain “property damage” in their definition of exigent circumstances. Moreover, there may be circumstances where the Police Department receives a tip that someone intends to destroy property used for emergency response purposes, i.e., someone could target all of the City’s fire trucks or ambulances, and in so doing, hamper the City’s ability to respond to fire and health emergencies, leading to loss of life. Given those risks, City staff strongly recommend that this language not be altered. However, in order to address the ACLU’s concerns, City staff have added the following language to the definition of Exigent Circumstances in Section 12.22.020(B): “The use of Surveillance Technology in Exigent Circumstances shall not infringe upon an individual’s right to peacefully protest.”

2. Section 12.22.020(F)(3)(c)—Definitions—Exemption for Cameras Installed In or On a Police Vehicle: Excluding Cameras with License Plate Reading Technology from the Exemption for Cameras Installed In or On a Police Vehicle (p. 5).

The next suggestion of the ACLU’s is to add “except license plate readers” to 12.22.020(F)(3)(c) which exempts cameras installed in or on a police vehicle from the requirements of the Ordinance, in other words, making “license plate readers” subject to the provisions of the Ordinance.

- That change is agreeable to City staff, and City staff have revised 12.22.020(F)(3)(c) to include: “cameras installed in or on a police vehicle, except cameras with license plate reading technology”, so that cameras with

such technology will not be exempt from the requirements of the Ordinance.

3. **Section 12.22.020(H)—Definitions—Technology-Specific Surveillance Use Policy: Adding a Definition of Technology-Specific Surveillance Use Policy (p. 8).**

Because the ACLU suggests that a City department should be required to submit a specific Surveillance Use Policy as to a specific technology when the City department is seeking Council approval of the specific Surveillance Technology, City staff have added a new definition for a “Technology-Specific Surveillance Use Policy” in Subsection (H) of 12.22.020.

B. ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY.

1. **Sections 12.22.030—Acquisition of Surveillance Technology and 12.22.040—Temporary Acquisition and Use of Surveillance Technology in Exigent Circumstances: Adding the Requirement that a Technology-Specific Surveillance Use Policy be Submitted with a Surveillance Impact Report (p.p. 8–12).**

As noted in the preceding paragraph, the ACLU has suggested that a City department should be required to submit a Surveillance Use Policy when the department is seeking Council approval of acquisition and use of a specific Surveillance Technology under 12.22.030(A) and (B), or when the department is submitting an Annual Surveillance Report to the Council under 12.22.060(A).

- That change is agreeable to City staff, and City staff have thus included the requirement that a Technology-Specific Use Policy be submitted along with a Surveillance Impact Report required in Sections 12.22.030(A) and (B), and 12.22.040 where the specific technology for which approval is sought is not already covered under the City’s Surveillance Use Policy.

2. **Section 12.22.030(C)—City Council Approval of Acquisition of Surveillance Technology: Language Revision (p. 9).**

Section 12.22.030(C) provides that “in approving, and/or disapproving any acquisition of Surveillance Technology, the City Council shall balance the safeguarding of individuals’ right to privacy against the investigative and prosecutorial functions of the Police Department and promoting and ensuring the safety and security of the general public.” The ACLU suggested that the City use the word “consider” in place of “balance.” In addition, during the June 14, 2018 meeting, the ACLU also suggested that the word “against” be replaced with the phrase “as well as.”

- Those changes are agreeable to City staff, and City staff have revised Section 12.22.030(C) as well as Section 12.22.050 (B) to read: “In

approving, and/or disapproving any acquisition of Surveillance Technology, the City Council shall consider the safeguarding of individuals' right to privacy as well as the investigative and prosecutorial functions of the Police Department and promoting and ensuring the safety and security of the general public.”

3. **Sections 12.22.030(D) and 12.22.040: Surveillance Impact Report and Technology-Specific Surveillance Use Policy to be Made Available No Fewer than 7 Days Prior to Council Meeting (p.p. 9–10).**

The ACLU also stated that the Ordinance does not allow for enough public input as written.

- In response, City staff have added the following language to the Ordinance:
 - i. A new section has been added to Section 12.22.030 as follows: “(D) Any Surveillance Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under Section 12.22.030 shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.”
 - ii. City staff also added the following language to 12.22.040: “Any Surveillance Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under this Section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.”

C. SURVEILLANCE USE POLICY.

1. **Section 12.22.050(A)—Submission of Surveillance Use Policy to the City Council: Surveillance Use Policy Shall be Made Publicly Available No Fewer than 7 Days Prior to Council Meeting (p. 10).**

As part of the revisions City staff made in order to address the ACLU's concern that there is not enough opportunity for public input in the Ordinance as written, City staff have also revised the language of the Ordinance with respect to the submission of the Surveillance Use Policy.

- City staff added the following language to 12.22.050(A): Any Surveillance Use Policy submitted under Section 12.22.050 shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

2. Section 12.22.050(B)—Council Approval of the Surveillance Use Policy: ACLU Concern re “Unlawfully Obstruct” Language (p. 10).

The ACLU suggested that the following sentence be removed from Section 12.22.050(B) regarding the Council’s authority to approve or disapprove a Surveillance Use Policy: “To the extent the City Manager determines that approving or disapproving the Surveillance Use Policy would unlawfully obstruct the investigative or prosecutorial functions of the Police Department, the City Council shall simply receive and discuss the applicable portions of the Surveillance Use Policy.”

- This change is not recommended, as it would allow the City Council to have ultimate decision making authority over critical decisions relating to the investigative and prosecutorial functions of the Police Department rather than the Police Commissioner and the City Manager. It also potentially runs afoul of the provisions of the City’s Plan F Charter, as it appears to relate more to operational issues and the discretion provided under the Charter to the City Manager than to the broader policy making role of the City Council. City staff discussed the ACLU’s suggested change with Ms. Crockford during the June 14, 2018 meeting with her and explained that this was not acceptable to the City. City staff also believe that this concern is addressed in Section 12.22.060(B)(1), which gives the City Council an opportunity to “recommend modifications to the Surveillance Use Policy that are designed to address the City Council’s concerns to the City Manager for his consideration.” Therefore, to the extent the City Council has a concern over a provision in the Surveillance Use Policy, the City Council will have an opportunity to recommend that the City Manager revise same accordingly.

D. ANNUAL SURVEILLANCE REPORT.

1. Section 12.22.060(A)—Submission of Annual Surveillance Report Approval: Language Revision (p.p. 10–11)

The ACLU stated that the following language in the second sentence of Section 12.22.060(A) is confusing and should be removed: “Similarly, if the City Council received but did not approve a Surveillance Impact Report from the Police Department because of concerns over obstructing the Police Department’s investigative or prosecutorial function, the Police Department must still submit an Annual Surveillance Report within twelve (12) months of the City Council’s receipt of the Surveillance Impact Report, and annually thereafter on or before March 1.”

- City staff is agreeable to revising the language of that section. After review, City staff suggest revising Section 12.22.060(A) by separating it into three subsections as follows:

“(1) A City department head who has obtained approval for the use of Surveillance Technology or the information it provides under Section 12.22.030 or Section 12.22.040 of this Chapter, must submit an Annual Surveillance Report within twelve (12) months of City Council approval, and annually thereafter on or before March 1.

(2) Where the Police Department submitted a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy that the Council did not approve prior to the Police Department’s use of the Surveillance Technology, the Police Department must still submit an Annual Surveillance Report within twelve (12) months of the City Council’s receipt of the Surveillance Impact Report, and annually thereafter on or before March 1.

(3) Any Annual Surveillance Report submitted under this section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.”

Section 12.22.060(A)(3) is also discussed in Section 2 below.

2. Section 12.22.060(A)(3)—Submission of Annual Surveillance Report: Annual Surveillance Report Shall be Made Publicly Available No Fewer than 7 Calendar Days Prior to Council Meeting (p. 11).

In response to the ACLU’s concern about allowing enough opportunity for public comment, City staff have revised Section 12.22.060(A) of the Ordinance to require that Annual Surveillance Report be submitted at least seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

“(3) Any Annual Surveillance Report submitted under this section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.”

3. Section 12.22.060(B)—Council Review of Annual Surveillance Reports: Enforcement (p. 11).

The ACLU stated that Section 12.22.060(B) is insufficient for enforcement purposes, and suggested that the language be revised to provide that . Section 12.22.060(B) currently reads: “. . . If the benefits or reasonably anticipated benefits do not outweigh the financial and/or operational costs or civil liberties or civil rights are not reasonably safeguarded, the City Council may consider (1) recommending modifications to the Surveillance Use Policy that are designed to address the City Council’s concerns to the City Manager for his consideration; and/or (2) requesting a report back from the City Manager regarding steps taken to address the City Council’s concerns.”

- In order to address the ACLU's concern, City staff have added the following language to Section 12.22.060(B): "and/or (3) recommend to the City Manager that use of the Surveillance Technology cease."

E. ENFORCEMENT OF THE ORDINANCE.

1. Section 12.22.070—Enforcement: Right of Action and Penalties for Violation (p.p. 11–12).

The ACLU submitted a comment stating that the Ordinance should provide for a private right of action, the award of attorneys' fees to successful litigants, and whistleblower protections.

- City staff do not recommend that the City provide such a private right of action for a variety of reasons, which City staff have explained to Ms. Crockford, and as explained below.

In cases where a City employee violates the Surveillance Use Policy or parts of the Surveillance Ordinance, the City Manager has the authority to discipline such an employee, including terminating the employee. Furthermore, the City's Employee Manual and Collective Bargaining Agreements contain provisions for disciplining employees, up to and including termination, where the employee violates a City policy or a municipal ordinance. In addition to the policy considerations that mitigate against the City providing for individuals to bring private causes of action against the City or City employees personally for alleged violations of a City ordinance, such a provision in a municipal ordinance would likely conflict with the provisions of the Massachusetts Tort Claims Act ("Chapter 258") which immunizes Massachusetts municipalities and their officials and employees from liability in, among others, claims based upon an act or omission of a public employee when the employee is exercising due care in the execution of any regulation of a public employer, or any municipal ordinance or by-law. The Legislature of the Commonwealth enacted Chapter 258 to act as a limited waiver of the common law doctrine of sovereign immunity, and thus, enabled the Commonwealth and its political subdivisions (i.e., cities and towns) to be sued in courts in limited circumstances. The Supreme Judicial Court has held that sovereign immunity is still in effect unless consent to suit has been expressed by the terms of a statute, or appears by necessary implication from them. To provide for a private right of action under the Surveillance Ordinance would be a significant deviation from Chapter 258, and would mean that any City employee or elected or appointed official could be subject to personal liability in actions stemming from alleged violations of the Ordinance regardless of whether the alleged violation was intentional. To the extent a City employee may commit an intentional tort or violate civil rights, there are existing remedies under state and federal laws which, depending on the allegations, permit individuals to file lawsuits against the City and City

employees for civil rights violations and intentional torts. For instance, an individual who was subject to surveillance without a warrant may file a lawsuit in state or federal court against both the City and the City employee for the alleged civil rights violation, and collect damages if successful, for such civil rights violation.

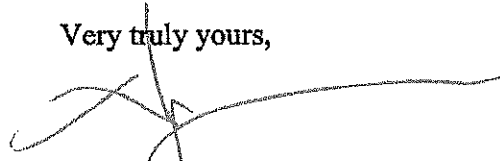
After careful consideration of this matter, however, and having reviewed the provisions of the Surveillance Technology ordinances adopted in Davis, California and Seattle, Washington, City staff recommend that the following language be included in Section 12.22.070 of the Ordinance. City staff believe that the below language meets the appropriate balance between the existing remedies available to individuals under state and federal law, the protections afforded to municipalities under Chapter 258, and providing members of the public with the ability to seek redress under this Ordinance:

- (A) Enforcement Officials. This Chapter shall be enforced by the City Manager or his/her designee.
- (B) Violation. Any person injured by a violation of this Chapter may institute proceedings for injunctive relief, declaratory relief, or a court order in a court of competent jurisdiction to enforce the provisions of this Chapter, subject to the provisions of Subsection (C) below. Any action instituted under this Subsection (B) shall be brought against the City of Cambridge, but not against City employees. No monetary damages or award of attorneys' fees shall be allowed in any legal proceeding for any alleged injuries arising out of any alleged violation(s) of this Chapter.
- (C) Notice and Procedure.
- (1) No legal proceeding under Subsection (B) above shall be brought unless the City has first been given written notice within thirty (30) days of the alleged violation(s) addressed to the City Clerk and specifying: (a) the name and address of the person(s) allegedly injured; (b) the date(s), time and place(s) of the alleged violation(s); and (c) a detailed description of the alleged injury.
 - (2) Prior to the initiation of any legal proceeding under Subsection (B) above, the City shall be permitted ninety (90) days from the date of the City's receipt of the written notice of the alleged violation(s) within which to investigate such alleged violation(s) and, if substantiated, to correct such alleged violation(s).
 - (3) If the alleged violation(s) is substantiated and subsequently cured, the City shall so notify the person(s) allegedly injured by such alleged violation(s) and a notice shall be posted on the City's website that

describes the corrective measure(s) taken to address the violation(s) and no legal proceedings to remedy the alleged violation(s) shall be allowed pursuant to Subsection (B) above.

- (D) Nothing in this Chapter shall be construed to limit or affect any individual's rights under state or federal laws.

Very truly yours,



Nancy E. Glowa
City Solicitor

Attachments: Clean and Redlined Revised Drafts of Surveillance Ordinance

Chapter 12.22 Surveillance Technology Ordinance**Section 12.22.010 Purpose**

The purpose of this Chapter is to provide for the regulation of Surveillance Technology acquisition or use by the City of Cambridge, to safeguard the right of individuals to privacy, to balance the public's right to privacy with the need to promote and ensure safety and security, to provide protocols for use of Surveillance Technology that include specific steps to mitigate potential impacts on the civil rights and liberties of any communities or groups including communities of color or other marginalized communities in the City, to balance any decision to use Surveillance Technology with an assessment of the costs and protection of privacy, civil liberties and civil rights, to allow for informed public discussion before deploying Surveillance Technology, to provide for transparency, oversight, and accountability, and to minimize the risks posed by use of Surveillance Technology in the City.

Section 12.22.020 Definitions

The following definitions apply to this Chapter:

- (A) **“Annual Surveillance Report”** means a written report concerning specific Surveillance Technology that includes all of the following:
- (1) A description of how the Surveillance Technology has been used, including whether it captured images, sound, or information regarding members of the public who are not suspected of engaging in unlawful conduct;
 - (2) 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;
 - (3) A summary of community complaints or concerns about the Surveillance Technology, if any;
 - (4) The results of any non-privileged internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
 - (5) Whether the Surveillance Technology has been effective at achieving its identified purpose;
 - (6) Statistics and information about public records requests;
 - (7) 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

- (8) ~~w~~Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City are disproportionately impacted by the deployment of the Surveillance Technology.
- (B) **“Exigent eCircumstances”** means the Police Commissioner’s or his/her designee’s good faith belief that an emergency involving danger of death, physical injury, or significant property damage or loss requires use of the Surveillance Technology or the information it provides. The use of Surveillance Technology in Exigent Circumstances shall not infringe upon an individual’s right to peacefully protest.
- (C) **“Surveillance”** means to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals 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 consented to provide the information, or had a clear and conspicuous opportunity to opt out of providing the information.
- (D) **“Surveillance Data”** means any electronic data collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology acquired by the City or operated at the direction of the City.
- (E) **“Surveillance Impact Report”** means a publicly-released written report including at a minimum the following:
- (1) Information describing the Surveillance Technology and how it works;
 - (2) Information on the proposed purpose(s) for the Surveillance Technology;
 - (3) The location(s) it may be deployed and when;
 - (4) The potential impact(s) on privacy in the City; the potential impact on the civil rights and liberties of any communities or groups, including, but not limited to, communities of color or other marginalized communities in the City, and a description of whether there is a plan to address the impact(s); and
 - (5) The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

(F) **“Surveillance Technology”** means any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

1. “Surveillance Technology” includes, but is not limited to:
 - (a) ~~i~~International mobile subscriber identity (IMSI) catchers and other cell site simulators;
 - (b) ~~a~~Automatic license plate readers;
 - (c) ~~e~~Electronic toll readers;
 - (d) ~~e~~Closed-circuit television cameras except as otherwise provided herein;
 - (e) ~~b~~Biometric Surveillance Technology, including facial, voice, iris, and gait-recognition software and databases;
 - (f) ~~m~~Mobile DNA capture technology;
 - (g) ~~g~~Gunshot detection and location hardware and services;
 - (h) ~~x~~X-ray vans;
 - (i) ~~v~~Video and audio monitoring and/or recording technology, such as surveillance cameras and wearable body cameras;
 - (j) ~~s~~Surveillance enabled or capable lightbulbs or light fixtures;
 - (k) ~~t~~Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network;
 - (l) ~~s~~Social media monitoring software;
 - (m) ~~t~~Through-the-wall radar or similar imaging technology;
 - (n) ~~p~~Passive scanners of radio networks;

- (o) ~~H~~Long-range Bluetooth and other wireless-scanning devices;
 - (p) ~~R~~Radio-frequency identification (RFID) scanners; and
 - (q) ~~S~~Software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software.
2. For the purposes of this Chapter, “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:
- (a) ~~R~~Routine office hardware, such as televisions, computers, and printers, that are in widespread public use and will not be used for any surveillance or surveillance-related functions;
 - (b) Parking Ticket Devices (“PTDs”) and related databases;
 - (c) ~~M~~Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is used for manually capturing and manually downloading video and/or audio recordings;
 - (d) ~~S~~Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
 - (e) City databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology;
 - (f) ~~M~~Manually-operated technological devices that are used primarily for internal City communications and are not designed to surreptitiously collect Surveillance Data, such as radios and email systems;
 - (g) ~~P~~Parking access and revenue control systems, including proximity card readers and transponder readers at City-owned or controlled parking garages; and

- (h) eElectronic card readers and key fobs used by City employees and other authorized persons for access to City-owned or controlled buildings and property.
3. For the purposes of this Chapter, the following Surveillance Technology is exempt from the requirements of this Chapter:
- a) Information acquired where the individual knowingly and voluntarily consented to provide the information, such as submitting personal information for the receipt of City services;
 - b) Information acquired where the individual was presented with a clear and conspicuous opportunity to opt out of providing the information;
 - c) Cameras installed in or on a police vehicle, except cameras with license plate reading technology;
 - d) Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations;
 - e) Cameras installed on City property solely for security purposes, including closed circuit television cameras installed by the City to monitor entryways and outdoor areas of City-owned or controlled buildings and property for the purpose of controlling access, maintaining the safety of City employees and visitors to City buildings, and protecting City property;
 - f) security cameras including closed circuit television cameras installed by the City to monitor cashiers' windows and other cash-handling operations and to maintain the safety of City employees and visitors to such areas;
 - g) Cameras installed solely to protect the physical integrity of City infrastructure; or
 - h) Technology that monitors only City employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of City resources.

4. The following situations are exceptions to the requirements of this Chapter:
- a) Surveillance conducted pursuant to a warrant using previously approved Surveillance Technology. Surveillance conducted pursuant to a warrant using previously approved Surveillance Technology is excepted from the requirements of 12.22.030(B) and 12.22.060(A) where: i) the City is prohibited from publicly releasing information pertaining to the surveillance under federal or state law, or pursuant to a Court Order; or ii) the Police Commissioner has determined that the release of information pertaining to the surveillance would compromise public safety and security, provided that the information is released in the next Annual Surveillance Report following the Police Commissioner's determination that public safety and security concerns pertaining to the release of such information no longer exist.
 - b) In the event of an emergency situation that poses an imminent risk of death or bodily harm or significant damage or loss, a City department head may, with the approval of the City Manager, acquire Surveillance Technology without prior City Council approval, for the sole purpose of preventing or mitigating such risk, if the department head reasonably believes the acquisition of Surveillance Technology will result in reduction of the risk. The department's use of Surveillance Technology must end when such risk no longer exists or the use of the Surveillance Technology can no longer reasonably reduce the risk. The use must be documented in the department's Annual Surveillance Report, and any future acquisition or use of such Surveillance Technology must be approved by the City Council as set forth in this Chapter.
 - c) A City department head may, with the approval of the City Manager, apply a technical patch or upgrade that is necessary to mitigate threats to the City's environment. The department shall not use the new surveillance capabilities of the technology until the requirements of Section 12.22.030 are met, unless the City Manager determines that the use is unavoidable; in that case, the department head shall request City Council approval as soon as possible. The request shall include a report to the City Council of how the altered surveillance capabilities

were used since the time of the upgrade.

- (G) **“Surveillance Use Policy”** means a publicly-released policy for the City’s use of the Surveillance Technology, approved by the City Solicitor and the City Manager, and submitted to and approved by the City Council. The Surveillance Use Policy shall at a minimum specify the following:
- (1) Purpose: The specific purpose(s) for the Surveillance Technology.
 - (2) Authorized Use: The uses that are authorized, the rules and processes required before that use, and the uses that are prohibited.
 - (3) Data Collection: The information that can be collected by the Surveillance Technology.
 - (4) Data Access: The individuals who can access or use the collected information, and the rules and processes required before access or use of the information.
 - (5) Data Protection: The safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms.
 - (6) Data Retention: The time period, if any, for which information collected by the Surveillance Technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the conditions that must be met to retain information beyond that period.
 - (7) Public Access: If and how collected information can be accessed by members of the public, including criminal defendants.
 - (8) Third-Party Data-Sharing: If and how other City or non-City entities can access or use the information, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the information.
 - (9) Training: The training, if any, required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology, including whether there are training materials.
 - (10) Oversight: The mechanisms to ensure that the Surveillance Use Policy is

followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy.

(H) “Technology-Specific Surveillance Use Policy” means a policy governing a City department(s)’s use of a specific Surveillance Technology not already covered under the City’s Surveillance Use Policy, approved by the City Solicitor and the City Manager, and submitted to the City Council with a Surveillance Impact Report under Section 12.22.030(A), 12.22.030(B), or 12.22.040 of this Chapter. A Technology-Specific Surveillance Use Policy shall not conflict with any provision of the City’s Surveillance Use Policy.

Section 12.22.030 Acquisition of Surveillance Technology

- (A) City Departments Other than the Police Department. Unless it is not reasonably possible or feasible to do so (e.g., Exigent Circumstances, a natural disaster, or technological problems prevent it, etc.), any department head other than the Police Commissioner seeking approval under Section 12.22.030 of this Chapter must submit to the City Council a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy pertaining to the specific Surveillance Technology for which approval is sought and obtain City Council approval before doing any of the following:
- (1) Seeking funds for Surveillance Technology, including but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;
 - (2) Acquiring new Surveillance Technology, including but not limited to procuring that Surveillance Technology without the exchange of monies or other consideration;
 - (3) Using Surveillance Technology for a purpose, in a manner, or in a location not previously approved; or
 - (4) Entering into an agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology or the information it provides.
- (B) Police Department. Other than with respect to Surveillance Technology limited to use in Exigent Circumstances in law enforcement investigations and prosecutions as

specifically defined in Section 12.22.040 of this Chapter, the Police Commissioner must submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy pertaining to the specific Surveillance Technology for which approval is sought to the City Council and obtain City Council approval, before doing any of the following:

- (A) Seeking funds for Surveillance Technology, including but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;
 - (B) Acquiring new Surveillance Technology, including but not limited to procuring that technology without the exchange of monies or other consideration;
 - (3) Using Surveillance Technology for a purpose, in a manner, or in a location not previously approved; or
 - (4) Entering into an agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology.
- (C) In approving, and/or ~~denying-disapproving~~ any acquisition of Surveillance Technology, the City Council shall ~~balance-consider~~ the safeguarding of individuals' right to privacy ~~against-as well as~~ the investigative and prosecutorial functions of the Police Department and promoting and ensuring the safety and security of the general public.
- (D) Any Surveillance Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under Section 12.22.030(A) or 12.22.030(B) shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

Section 12.22.040 Temporary Acquisition and Use of Surveillance Technology in Exigent Circumstances

Notwithstanding the provisions of this Chapter, the Police Department may temporarily acquire or temporarily use Surveillance Technology in Exigent Circumstances without following the provisions of this Chapter before that acquisition or use. However, if the Police Department acquires or uses Surveillance Technology in Exigent Circumstances under this Section, the Police Commissioner must (1) report that acquisition or use to the City Council in writing within 90 days following the end of those Exigent Circumstances; (2) submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy to the City Council regarding that Surveillance

Technology within 90 days following the end of those Exigent Circumstances; and (3) include that Surveillance Technology in the Police Department's next Annual Surveillance Report to the City Council following the end of those Exigent Circumstances. If the Police Commissioner is unable to meet the 90-day timeline to submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy to the City Council, the Police Commissioner may notify the City Council in writing of his or her request to extend this period. The City Council may grant extensions beyond the original 90-day timeline to submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy. Any Surveillance Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under this Section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

Section 12.22.050 Compliance for Existing Surveillance Technologies

- (A) The City Manager shall submit to the City Council for its review and approval a proposed Surveillance Use Policy applicable to each City department that possesses or uses Surveillance Technology before the effective date of this Chapter or for future use and acquisition of Surveillance Technology, no later than one-hundred eighty (180) days following the effective date of this Chapter, for review and approval by the City Council. If the City Manager is unable to meet this 180-day timeline, he or she may notify the City Council in writing of his or her request to extend this period. The City Council may grant an extension to the City Manager to submit a proposed Surveillance Use Policy. Any Surveillance Use Policy submitted under Section 12.22.050 shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.
- (B) In approving or denying the Surveillance Use Policy, the City Council shall balance the safeguarding of individuals' right to privacy ~~against as well as~~ the investigative and prosecutorial function of the Police Department and promoting and ensuring the safety and security of the general public. To the extent the City Manager ~~or a court of law~~ determines that approving or ~~denying disapproving~~ the Surveillance Use Policy would unlawfully obstruct the investigative or prosecutorial functions of the Police Department, the City Council shall simply receive and discuss the applicable portions of the Surveillance Use Policy.

Section 12.22.060 Oversight Following City Council Approval

- (A) (1) A City department head who has obtained approval for the use of Surveillance Technology or the information it provides under Section

12.22.030 or Section 12.22.040 of this Chapter, must submit an Annual Surveillance Report within twelve (12) months of City Council approval, and annually thereafter on or before March 1.

~~Similarly, (2) Where the Police Department has submitted a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy that the Council has not approved prior to the Police Department's use of the Surveillance Technology, if the City Council received but did not specifically approve or disapprove a Surveillance Impact Report from the Police Department because of concerns over obstructing the Police Department's investigative or prosecutorial function,~~ the Police Department must still submit an Annual Surveillance ~~Use~~ Report within twelve (12) months of the City Council's receipt of the Surveillance Impact Report, and annually thereafter on or before March 1.

(3) Any Annual Surveillance Report submitted under this section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

- (B) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether the benefits to the impacted City department(s) and the community of the Surveillance Technology outweigh the financial and operational costs and whether reasonable safeguards exist to address reasonable concerns regarding privacy, civil liberties, and civil rights impacted by deployment of the Surveillance Technology. If the benefits or reasonably anticipated benefits do not outweigh the financial and/or operational costs or civil liberties or civil rights are not reasonably safeguarded, the City Council may ~~consider~~ (1) recommending modifications to the Surveillance Use Policy that are designed to address the City Council's concerns to the City Manager for his consideration; and/or (2) requesting a report back from the City Manager regarding steps taken to address the City Council's concerns; and/or (3) recommend to the City Manager that use of the Surveillance Technology cease.
- (C) No later than May 31 of each year, the City Council shall hold a meeting to discuss the City departments' Annual Surveillance Reports, and shall publicly release a report that includes a summary of all requests for approval of Surveillance Impact Reports received by the City Council during the prior year pursuant to Section 12.22.030 or Section 12.22.040 of this Chapter, including whether the City Council approved, ~~rejected~~disapproved, or required modifications to the Surveillance Impact Report.

Section 12.22.070 **Enforcement**

- (A) Enforcement Officials. This Chapter shall be enforced by the City Manager or his/her designee. _
- (B) Violation. Any person injured by a violation of this Chapter may institute proceedings for injunctive relief, declaratory relief, or a court order in a court of competent jurisdiction to enforce the provisions of this Chapter, subject to the provisions of Subsection (C) below. Any action initiated under this Subsection (B) shall be brought against the City of Cambridge, but not against City employees. No monetary damages or award of attorneys' fees shall be allowed in any legal proceeding for any alleged injuries arising out of any alleged violation(s) of this Chapter
- (C) Notice and Procedure. (1) No legal proceeding under Subsection (B) above shall be brought unless the City has first been given written notice within thirty (30) days of the alleged violation(s) addressed to the City Clerk and specifying: (a) the name and address of the person(s) allegedly injured; (b) the date(s), time and place(s) of the alleged violation(s); and (c) a detailed description of the alleged injury. (2) Prior to the initiation of any legal proceeding under Subsection (B) above, the City shall be permitted ninety (90) days from the date of its receipt of the written notice of the alleged violation(s) within which to investigate such alleged violation(s) and, if substantiated, to correct such alleged violation(s). (3) If the alleged violation(s) is substantiated and subsequently cured, the City shall so notify the person(s) allegedly injured by such violation(s) and a notice shall be posted on the City's website that describes the corrective measure(s) taken to address the violation(s) and no legal proceeding to remedy the alleged violation(s) shall be allowed pursuant to Subsection (B) above.
- (D) Nothing in this Chapter shall be construed to limit or affect any individual's rights under state or federal laws.

Section 12.22.080 **Severability**

The provisions in this Chapter are severable. If any part or provision of this Chapter, or the application of this Chapter to any person or circumstance, is held invalid by a court of competent jurisdiction, the remainder of this Chapter shall not be affected by such holding and shall continue to have full force and effect.

Section 12.22.090 **Effective Date**

This Chapter shall take effect nine months after its adoption.

DRAFT

Chapter 12.22 Surveillance Technology Ordinance

Section 12.22.010 Purpose

The purpose of this Chapter is to provide for the regulation of Surveillance Technology acquisition or use by the City of Cambridge, to safeguard the right of individuals to privacy, to balance the public's right to privacy with the need to promote and ensure safety and security, to provide protocols for use of Surveillance Technology that include specific steps to mitigate potential impacts on the civil rights and liberties of any communities or groups including communities of color or other marginalized communities in the City, to balance any decision to use Surveillance Technology with an assessment of the costs and protection of privacy, civil liberties and civil rights, to allow for informed public discussion before deploying Surveillance Technology, to provide for transparency, oversight, and accountability, and to minimize the risks posed by use of Surveillance Technology in the City.

Section 12.22.020 Definitions

The following definitions apply to this Chapter:

- (A) **“Annual Surveillance Report”** means a written report concerning specific Surveillance Technology that includes all of the following:
- (1) A description of how the Surveillance Technology has been used, including whether it captured images, sound, or information regarding members of the public who are not suspected of engaging in unlawful conduct;
 - (2) 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;
 - (3) A summary of community complaints or concerns about the Surveillance Technology, if any;
 - (4) The results of any non-privileged internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
 - (5) Whether the Surveillance Technology has been effective at achieving its identified purpose;
 - (6) Statistics and information about public records requests;
 - (7) 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

- (8) Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City are disproportionately impacted by the deployment of the Surveillance Technology.
- (B) **“Exigent Circumstances”** means the Police Commissioner’s or his/her designee’s good faith belief that an emergency involving danger of death, physical injury, or significant property damage or loss requires use of the Surveillance Technology or the information it provides. The use of Surveillance Technology in Exigent Circumstances shall not infringe upon an individual’s right to peacefully protest.
- (C) **“Surveillance”** means to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals 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 consented to provide the information, or had a clear and conspicuous opportunity to opt out of providing the information.
- (D) **“Surveillance Data”** means any electronic data collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology acquired by the City or operated at the direction of the City.
- (E) **“Surveillance Impact Report”** means a publicly-released written report including at a minimum the following:
- (1) Information describing the Surveillance Technology and how it works;
 - (2) Information on the proposed purpose(s) for the Surveillance Technology;
 - (3) The location(s) it may be deployed and when;
 - (4) The potential impact(s) on privacy in the City; the potential impact on the civil rights and liberties of any communities or groups, including, but not limited to, communities of color or other marginalized communities in the City, and a description of whether there is a plan to address the impact(s); and
 - (5) The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

(F) **“Surveillance Technology”** means any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

1. “Surveillance Technology” includes, but is not limited to:
 - (a) International mobile subscriber identity (IMSI) catchers and other cell site simulators;
 - (b) Automatic license plate readers;
 - (c) Electronic toll readers;
 - (d) Closed-circuit television cameras except as otherwise provided herein;
 - (e) Biometric Surveillance Technology, including facial, voice, iris, and gait-recognition software and databases;
 - (f) Mobile DNA capture technology;
 - (g) Gunshot detection and location hardware and services;
 - (h) X-ray vans;
 - (i) Video and audio monitoring and/or recording technology, such as surveillance cameras and wearable body cameras;
 - (j) Surveillance enabled or capable lightbulbs or light fixtures;
 - (k) Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network;
 - (l) Social media monitoring software;
 - (m) Through-the-wall radar or similar imaging technology;
 - (n) Passive scanners of radio networks;

- (o) Long-range Bluetooth and other wireless-scanning devices;
 - (p) Radio-frequency identification (RFID) scanners; and
 - (q) Software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software.
2. For the purposes of this Chapter, “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:
- (a) Routine office hardware, such as televisions, computers, and printers, that are in widespread public use and will not be used for any surveillance or surveillance-related functions;
 - (b) Parking Ticket Devices (“PTDs”) and related databases;
 - (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 used for 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) City databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology;
 - (f) Manually-operated technological devices that are used primarily for internal City communications and are not designed to surreptitiously collect Surveillance Data, such as radios and email systems;
 - (g) Parking access and revenue control systems, including proximity card readers and transponder readers at City-owned or controlled parking garages; and

- (h) Electronic card readers and key fobs used by City employees and other authorized persons for access to City-owned or controlled buildings and property.
3. For the purposes of this Chapter, the following Surveillance Technology is exempt from the requirements of this Chapter:
- a) Information acquired where the individual knowingly and voluntarily consented to provide the information, such as submitting personal information for the receipt of City services;
 - b) Information acquired where the individual was presented with a clear and conspicuous opportunity to opt out of providing the information;
 - c) Cameras installed in or on a police vehicle, except cameras with license plate reading technology;
 - d) Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations;
 - e) Cameras installed on City property solely for security purposes, including closed circuit television cameras installed by the City to monitor entryways and outdoor areas of City-owned or controlled buildings and property for the purpose of controlling access, maintaining the safety of City employees and visitors to City buildings, and protecting City property;
 - f) security cameras including closed circuit television cameras installed by the City to monitor cashiers' windows and other cash-handling operations and to maintain the safety of City employees and visitors to such areas;
 - g) Cameras installed solely to protect the physical integrity of City infrastructure; or
 - h) Technology that monitors only City employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of City resources.
4. The following situations are exceptions to the requirements of this Chapter:

- a) Surveillance conducted pursuant to a warrant using previously approved Surveillance Technology. Surveillance conducted pursuant to a warrant using previously approved Surveillance Technology is excepted from the requirements of 12.22.030(B) and 12.22.060(A) where: i) the City is prohibited from publicly releasing information pertaining to the surveillance under federal or state law, or pursuant to a Court Order; or ii) the Police Commissioner has determined that the release of information pertaining to the surveillance would compromise public safety and security, provided that the information is released in the next Annual Surveillance Report following the Police Commissioner's determination that public safety and security concerns pertaining to the release of such information no longer exist.
- b) In the event of an emergency situation that poses an imminent risk of death or bodily harm or significant damage or loss, a City department head may, with the approval of the City Manager, acquire Surveillance Technology without prior City Council approval, for the sole purpose of preventing or mitigating such risk, if the department head reasonably believes the acquisition of Surveillance Technology will result in reduction of the risk. The department's use of Surveillance Technology must end when such risk no longer exists or the use of the Surveillance Technology can no longer reasonably reduce the risk. The use must be documented in the department's Annual Surveillance Report, and any future acquisition or use of such Surveillance Technology must be approved by the City Council as set forth in this Chapter.
- c) A City department head may, with the approval of the City Manager, apply a technical patch or upgrade that is necessary to mitigate threats to the City's environment. The department shall not use the new surveillance capabilities of the technology until the requirements of Section 12.22.030 are met, unless the City Manager determines that the use is unavoidable; in that case, the department head shall request City Council approval as soon as possible. The request shall include a report to the City Council of how the altered surveillance capabilities were used since the time of the upgrade.

- (G) **“Surveillance Use Policy”** means a publicly-released policy for the City’s use of the Surveillance Technology, approved by the City Solicitor and the City Manager, and submitted to and approved by the City Council. The Surveillance Use Policy shall at a minimum specify the following:
- (1) **Purpose**: The specific purpose(s) for the Surveillance Technology.
 - (2) **Authorized Use**: The uses that are authorized, the rules and processes required before that use, and the uses that are prohibited.
 - (3) **Data Collection**: The information that can be collected by the Surveillance Technology.
 - (4) **Data Access**: The individuals who can access or use the collected information, and the rules and processes required before access or use of the information.
 - (5) **Data Protection**: The safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms.
 - (6) **Data Retention**: The time period, if any, for which information collected by the Surveillance Technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the conditions that must be met to retain information beyond that period.
 - (7) **Public Access**: If and how collected information can be accessed by members of the public, including criminal defendants.
 - (8) **Third-Party Data-Sharing**: If and how other City or non-City entities can access or use the information, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the information.
 - (9) **Training**: The training, if any, required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology, including whether there are training materials.
 - (10) **Oversight**: The mechanisms to ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the

technology or access to information collected by the Surveillance Technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy.

- (H) **“Technology-Specific Surveillance Use Policy”** means a policy governing a City department(s)’s use of a specific Surveillance Technology not already covered under the City’s Surveillance Use Policy, approved by the City Solicitor and the City Manager, and submitted to the City Council with a Surveillance Impact Report under Section 12.22.030(A), 12.22.030(B), or 12.22.040 of this Chapter. A Technology-Specific Surveillance Use Policy shall not conflict with any provision of the City’s Surveillance Use Policy.

Section 12.22.030 Acquisition of Surveillance Technology

- (A) City Departments Other than the Police Department. Unless it is not reasonably possible or feasible to do so (e.g., Exigent Circumstances, a natural disaster, or technological problems prevent it, etc.), any department head other than the Police Commissioner seeking approval under Section 12.22.030 of this Chapter must submit to the City Council a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy pertaining to the specific Surveillance Technology for which approval is sought and obtain City Council approval before doing any of the following:
- (1) Seeking funds for Surveillance Technology, including but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;
 - (2) Acquiring new Surveillance Technology, including but not limited to procuring that Surveillance Technology without the exchange of monies or other consideration;
 - (3) Using Surveillance Technology for a purpose, in a manner, or in a location not previously approved; or
 - (4) Entering into an agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology or the information it provides.
- (B) Police Department. Other than with respect to Surveillance Technology limited to use in Exigent Circumstances in law enforcement investigations and prosecutions as specifically defined in Section 12.22.040 of this Chapter, the Police Commissioner must submit a Surveillance Impact Report, and, if necessary, a Technology-

Specific Surveillance Use Policy pertaining to the specific Surveillance Technology for which approval is sought to the City Council and obtain City Council approval, before doing any of the following:

- (A) Seeking funds for Surveillance Technology, including but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;
 - (B) Acquiring new Surveillance Technology, including but not limited to procuring that technology without the exchange of monies or other consideration;
 - (3) Using Surveillance Technology for a purpose, in a manner, or in a location not previously approved; or
 - (4) Entering into an agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology.
- (C) In approving, and/or disapproving any acquisition of Surveillance Technology, the City Council shall consider the safeguarding of individuals' right to privacy as well as the investigative and prosecutorial functions of the Police Department and promoting and ensuring the safety and security of the general public.
- (D) Any Surveillance Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under Section 12.22.030(A) or 12.22.030(B) shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

Section 12.22.040 Temporary Acquisition and Use of Surveillance Technology in Exigent Circumstances

Notwithstanding the provisions of this Chapter, the Police Department may temporarily acquire or temporarily use Surveillance Technology in Exigent Circumstances without following the provisions of this Chapter before that acquisition or use. However, if the Police Department acquires or uses Surveillance Technology in Exigent Circumstances under this Section, the Police Commissioner must (1) report that acquisition or use to the City Council in writing within 90 days following the end of those Exigent Circumstances; (2) submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy to the City Council regarding that Surveillance Technology within 90 days following the end of those Exigent Circumstances; and (3) include that Surveillance Technology in the Police Department's next Annual Surveillance Report to the City Council following the end of those Exigent Circumstances. If the

Police Commissioner is unable to meet the 90-day timeline to submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy to the City Council, the Police Commissioner may notify the City Council in writing of his or her request to extend this period. The City Council may grant extensions beyond the original 90-day timeline to submit a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy. Any Surveillance Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under this Section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.

Section 12.22.050 Compliance for Existing Surveillance Technologies

- (A) The City Manager shall submit to the City Council for its review and approval a proposed Surveillance Use Policy applicable to each City department that possesses or uses Surveillance Technology before the effective date of this Chapter or for future use and acquisition of Surveillance Technology, no later than one-hundred eighty (180) days following the effective date of this Chapter, for review and approval by the City Council. If the City Manager is unable to meet this 180-day timeline, he or she may notify the City Council in writing of his or her request to extend this period. The City Council may grant an extension to the City Manager to submit a proposed Surveillance Use Policy. Any Surveillance Use Policy submitted under Section 12.22.050 shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.
- (B) In approving or denying the Surveillance Use Policy, the City Council shall balance the safeguarding of individuals' right to privacy as well as the investigative and prosecutorial function of the Police Department and promoting and ensuring the safety and security of the general public. To the extent the City Manager determines that approving or disapproving the Surveillance Use Policy would unlawfully obstruct the investigative or prosecutorial functions of the Police Department, the City Council shall simply receive and discuss the applicable portions of the Surveillance Use Policy.

Section 12.22.060 Oversight Following City Council Approval

- (A) (1) A City department head who has obtained approval for the use of Surveillance Technology or the information it provides under Section 12.22.030 or Section 12.22.040 of this Chapter, must submit an Annual Surveillance Report within twelve (12) months of City Council approval, and annually thereafter on or before March 1.

- (2) Where the Police Department has submitted a Surveillance Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy that the Council has not approved prior to the Police Department's use of the Surveillance Technology, the Police Department must still submit an Annual Surveillance Report within twelve (12) months of the City Council's receipt of the Surveillance Impact Report, and annually thereafter on or before March 1.
- (3) Any Annual Surveillance Report submitted under this section shall be made publicly available no fewer than seven (7) calendar days prior to the date of the Council meeting where it shall be discussed.
- (B) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether the benefits to the impacted City department(s) and the community of the Surveillance Technology outweigh the financial and operational costs and whether reasonable safeguards exist to address reasonable concerns regarding privacy, civil liberties, and civil rights impacted by deployment of the Surveillance Technology. If the benefits or reasonably anticipated benefits do not outweigh the financial and/or operational costs or civil liberties or civil rights are not reasonably safeguarded, the City Council may (1) recommend modifications to the Surveillance Use Policy that are designed to address the City Council's concerns to the City Manager for his consideration; and/or (2) request a report back from the City Manager regarding steps taken to address the City Council's concerns; and/or (3) recommend to the City Manager that use of the Surveillance Technology cease.
- (C) No later than May 31 of each year, the City Council shall hold a meeting to discuss the City departments' Annual Surveillance Reports, and shall publicly release a report that includes a summary of all requests for approval of Surveillance Impact Reports received by the City Council during the prior year pursuant to Section 12.22.030 or Section 12.22.040 of this Chapter, including whether the City Council approved, disapproved, or required modifications to the Surveillance Impact Report.

Section 12.22.070 Enforcement

- (A) Enforcement Officials. This Chapter shall be enforced by the City Manager or his/her designee.
- (B) Violation. Any person injured by a violation of this Chapter may institute

proceedings for injunctive relief, declaratory relief, or a court order in a court of competent jurisdiction to enforce the provisions of this Chapter, subject to the provisions of Subsection (C) below. Any action initiated under this Subsection (B) shall be brought against the City of Cambridge, but not against City employees. No monetary damages or award of attorneys' fees shall be allowed in any legal proceeding for any alleged injuries arising out of any alleged violation(s) of this Chapter

- (C) **Notice and Procedure.** (1) No legal proceeding under Subsection (B) above shall be brought unless the City has first been given written notice within thirty (30) days of the alleged violation(s) addressed to the City Clerk and specifying: (a) the name and address of the person(s) allegedly injured; (b) the date(s), time and place(s) of the alleged violation(s); and (c) a detailed description of the alleged injury.
- (2) Prior to the initiation of any legal proceeding under Subsection (B) above, the City shall be permitted ninety (90) days from the date of its receipt of the written notice of the alleged violation(s) within which to investigate such alleged violation(s) and, if substantiated, to correct such alleged violation(s).
- (3) If the alleged violation(s) is substantiated and subsequently cured, the City shall so notify the person(s) allegedly injured by such violation(s) and a notice shall be posted on the City's website that describes the corrective measure(s) taken to address the violation(s) and no legal proceeding to remedy the alleged violation(s) shall be allowed pursuant to Subsection (B) above.
- (D) Nothing in this Chapter shall be construed to limit or affect any individual's rights under state or federal laws.

Section 12.22.080 Severability

The provisions in this Chapter are severable. If any part or provision of this Chapter, or the application of this Chapter to any person or circumstance, is held invalid by a court of competent jurisdiction, the remainder of this Chapter shall not be affected by such holding and shall continue to have full force and effect.

Section 12.22.090 Effective Date

This Chapter shall take effect nine months after its adoption.