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.

(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;

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.

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 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 to the City Council 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 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 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.

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 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 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.

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.

(B) In approving or denying the Surveillance Use Policy, the City Council shall balance the safeguarding of individuals' right to privacy against 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 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 <u>Oversight Following City Council Approval</u>

(A) 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, 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 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.

(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.

(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, or required modifications to the Surveillance Impact Report.

Section 12.22.070 Enforcement

This Chapter shall be enforced by the City Manager or his/her designee.

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.