



City of Cambridge

Executive Department

LOUIS A. DePASQUALE
City Manager

LISA C. PETERSON
Deputy City Manager

April 24, 2017

To the Honorable, the City Council:

I am writing in response to Council Order Number 7 of 11/21/16, Awaiting Report Item Number 17-15 and Council Order No. 2 of 3/27/17, an update on language in a proposed surveillance technology ordinance (the “Proposed Ordinance”).

The Law Department has been working with staff from a number of other City departments in order to comprehensively review the Proposed Ordinance in detail and to work on developing proposed revisions to it. The City team has met a number of times in order to discuss the operational ramifications of various sections of the Proposed Ordinance in connection with the operational needs of City departments, and how best to achieve the objectives of the Proposed Ordinance without unduly burdening City operations.

The Proposed Ordinance as drafted is complex and covers many areas of legislation in its scope. It is important that the Proposed Ordinance balance the goals of protecting the safety of people and property and promoting technological advances that will assist the City in its operations with the rights of individuals under the United States and Massachusetts Constitutions and other laws. The Proposed Ordinance as currently drafted is overly broad and prescriptive, in that, for example, it would require the City Manager to submit a lengthy surveillance use policy and surveillance impact report to the City Council for consideration and approval each time a City department seeks funds to purchase surveillance technology equipment.¹

¹ The Proposed Ordinance’s definition of surveillance technology is “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,” including, but not limited to, international mobile subscriber identity catchers and other cell site simulators, automatic license plate readers, electronic toll readers, closed-circuit television cameras, and surveillance enabled or capable lightbulbs or light fixtures, among other things. The Proposed Ordinance’s definition of surveillance technology does not include routine office hardware, such as televisions, computers, and printers, parking ticket devices, manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings, among other things.



The surveillance impact report would be required to contain demographic and statistical reporting including detailed analysis by the City department seeking approval of a purchase as to how the use of surveillance technology would impact various populations in the City and what efforts would be undertaken to prevent abuse of surveillance data obtained with respect to heavily impacted groups. This would likely involve a significant commitment of time and other resources for even fairly routine expenditures that might delay or even forestall the work that such technologies is intended to accomplish. These expenditures could more optimally be addressed through broader legislative decisions established by the City Council in the Proposed Ordinance that are then implemented by the City Manager at an administrative level as to specific acquisitions and use of such technologies. The Law Department therefore does not recommend adoption of those portions of the Proposed Ordinance which could result in significant additional administrative hurdles that could cause operational difficulties for City departments. The Law Department also recommends against adopting those portions of the Proposed Ordinance which refer to data retention and requests for surveillance data, as such provisions are already covered by the Massachusetts Public Records Law and the Massachusetts Municipal Records Retention Schedule.

In order to put the issue into context, we thought it would be helpful to give the City Council a brief description of some of the surveillance practices that are currently employed by the City. For example, the Police Department utilizes a number of devices, software, and hardware that would likely be considered “surveillance technology” under the proposed surveillance technology ordinance. In today’s policing world, much of this technology is considered essential police equipment, and under the current law, is legally permitted without requiring a search warrant or other court approval prior to being utilized and/or obtained. Technologies such as Automated Fingerprint Identification Systems (AFIS), Combined DNA Index Systems (CODIS), Shot Spotter, Analyst Notebook, RMS/GIS mapping software, and public facing surveillance cameras are used by law enforcement agencies across the country on a daily basis to effectively solve crime and are legally utilized and/or obtained and without prior court approval. However, different technologies implicate different privacy concerns and constitutional rights, and can often require court approval or legal process prior to being utilized and/or obtained. Technology involving Cell Site Location Information (real time and historical), GPS tracking (by phone and device), and phone interception (i.e., wiretap) can often require prior judicial approval or legal process prior to being utilized and/or obtained; absent exigent circumstances, the Cambridge Police Department will seek a search warrant, court order or subpoena prior to utilizing and/or obtaining this type of surveillance data and technology.

In addition to the technologies employed by the Police Department, the below technologies are presently used by the Traffic, Parking, and Transportation Department:

- Permanently installed traffic cameras for counting users (permanent count stations);
- Temporarily installed traffic cameras for counting users, for traffic studies (these can be for both City projects and for private development projects);
- Permanently installed traffic cameras for controlling signals (video detectors);
- Security cameras in the cashier area within the Parking Services unit (which is responsible for parking ticket payment and issuing resident parking permits);
- Security cameras in the entry and exit lanes within the First Street Garage (and the Department is investigating a similar system for use at the Green Street Garage);
- Parking Access and Revenue Control Systems (PARCS) at both garages, which include proximity card readers (First Street Garage) and transponder readers (Green Street Garage); and
- The Parking Management Information System (PMIS) contains data on license plates, addresses, phone numbers, and email addresses. Of note, as Parking Control Officers are doing enforcement, they are often using their handheld computers to note the time and location that they observe license plates, even if they are not writing a ticket (this is done principally as part of enforcing

overtime violations at meters and the use of visitor permits in resident permit parking areas, both of which are critical enforcement functions); this information is then stored in the PMIS.

There are other surveillance technologies used by various other City departments, including cameras that are used in cashier windows in the City such as the Treasurer's Office and other departments, and key fobs for entry into numerous City buildings, including City Hall, as part of the overall system installed by the Department of Public Works, to name a few. Requiring the City Manager to submit a lengthy surveillance use policy and surveillance impact report to the City Council for consideration and approval each time a City department seeks funds to purchase or replace the above surveillance equipment would tie up a significant amount of staff time, whereas if the City Manager developed and followed a policy that comported with the goals of the City Council as established by the Proposed Ordinance, such staff time could likely be more productively spent on the other important responsibilities of City departments.

The Law Department recommends an alternative approach to the Proposed Ordinance whereby the City Manager would be required to develop and issue a policy that would codify the directives on surveillance use that would be set forth in a more succinct and streamlined ordinance. The City Manager could report back to the City Council to the extent any updates are sought by the Council. Consistent with that approach, City staff propose to revise the Proposed Ordinance so that it would establish the policy limits for the City's use of surveillance technologies in general, as opposed to delving into very specific details which could result in operational problems for various City departments. For surveillance technologies not being used for law enforcement purposes, the Law Department recommends that the City post on the City's website descriptions of various surveillance technologies that are in use. For example, the City could use the website as a venue to post a map of locations where cameras are being used to collect traffic counts, a description of the City's key fob system, or a listing of the types of data being collected through the Parking Management Information System.

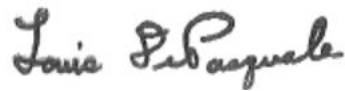
The Law Department recommends that the Proposed Ordinance require the City Manager to develop and issue a surveillance use policy for the City that would address some or all of the following:

- Purpose: what specific purpose(s) the surveillance technology is intended to advance;
- Authorized Use: a) what specific surveillance technology use(s) will be authorized, including how the surveillance technology will be operated, b) what rules will govern, and what processes will be required prior to each use of the surveillance technology, including what existing legal standard must be met before the technology is used or, where such a standard does not currently exist, what is the proposed standard to be followed, and c) what potential capabilities and uses of the surveillance technology will be prohibited;
- Data Collection: what types of surveillance data are capable of being collected, captured, recorded, intercepted, or retained by the surveillance technology; what surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data;
- Data Access: under what circumstances an individual will be allowed to request access to surveillance data, who will be responsible for authorizing access to the surveillance data, what rules and processes must be followed prior to accessing or interacting with the surveillance data, and what the acceptable grounds are for requesting access to the surveillance data;
- Data Protection: what safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms;
- Surveillance Data Sharing: if the City intends to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, the City shall detail how it will require that the collection, retention, and storage of surveillance data be conducted, how it will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable surveillance use policy and does not further

- disclose the surveillance data to unauthorized persons and entities;
- Training: what training, including training materials, will be required for any individual authorized to use the surveillance technology or to access surveillance data;
 - Maintenance: how the security and integrity of the surveillance technology will be maintained and how City departments will present any substantive changes in the surveillance technology's functionality to the City Manager for approval; and
 - Auditing and Oversight: what mechanisms will be implemented to ensure the surveillance use policy is followed, including what internal personnel will be assigned to ensure compliance with the policy, what independent persons or entities will be given oversight authority, and what sanctions will be put in place for violations of the policy.

Significant progress has been made to date toward revising the language in the Proposed Surveillance Technology Ordinance. The City staff who are working on this project are completing the additional work that needs to be done in order to present a comprehensively revised draft of the Proposed Ordinance to the Council for consideration. We expect that a proposed draft ordinance will be brought before the Council within the next few weeks.

Very truly yours,



Louis A. DePasquale
City Manager

LAD/mec