Ordinance X.X Public Oversight of Surveillance Technology

2019 September 8 - Draft v7

Contents

Section 1.1 Purpose

The purpose of this Ordinance is to provide for the regulation of Surveillance Technology acquisition or use by the City of Somerville or the use of the Surveillance Data it provides; 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 or Surveillance Data that include specific steps to mitigate potential impacts on the civil rights and liberties of any individuals, 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. Once in effect, this Ordinance shall override Somerville's Executive Order of October 4, 2017 entitled "Executive Policy on Surveillance Technology.

Section 1.2 Definitions

The following definitions apply to this Ordinance:

(A) **"Annual Surveillance Report"** means a written report submitted by the Mayor's Office on an annual basis concerning specific Surveillance Technology used by any City

department during the previous year and containing the information set forth in 1.6(B) of this Ordinance.

(B) **"Exigent Circumstances"** means the Police Chief's or the Police Chief's designee's good faith and reasonable belief that an emergency involving danger of death, physical injury, or significant property damage or loss, similar to those that would render impracticable to obtain a warrant, requires use of the Surveillance Technology or the Surveillance Data it provides. The use of Surveillance Technology in Exigent Circumstances shall not infringe upon an individual's right to peacefully protest and exercise other lawful and protected Constitutional Rights.

(C) **"Identifiable Individuals"** means an individual whose identity can be revealed by data, including Surveillance Data, or revealed by data when it is analyzed and/or combined with any other type of record.

(D) **"Surveillance"** means the act of observing or analyzing the movements, behavior, or actions of Identifiable Individuals.

(E) **"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.

(F) **"Surveillance Technology"** means any 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 specifically associated with, or capable of being associated with, any Identifiable Individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software. Examples of Surveillance Technology include, but are not limited to:

i. International Mobile Subscriber Identity ("IMSI") catchers and other cell site simulators;
ii. Automatic license plate readers;
iii. Electronic toll readers;
iv. Closed-circuit television cameras except as otherwise provided herein;
v. Biometric Surveillance Technology, including facial, voice, iris, and gait-recognition software and databases;
vi. Mobile DNA capture technology;
vii. Gunshot detection and location hardware and services;
viii. X-ray vans;
ix. Video and audio monitoring and/or recording technology, such as surveillance cameras;
x. Surveillance enabled or capable lightbulbs or light fixtures;

xi. Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network;
xii. Social media monitoring software;
xiii. Through-the-wall radar or similar imaging technology;
xiv. Passive scanners of radio networks;
xv. Long-range Bluetooth and other wireless-scanning devices;
xvi. Thermal imaging or "Forward Looking Infrared" devices or cameras;
xvii. Radio-frequency identification (RFID) scanners; and
xviii. Software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software.

(G) **"Surveillance Technology Impact Report"** means a written report submitted by the Mayor's Office with a request for approval of acquisition or use of Surveillance Technology, and which includes, at a minimum, the requirements set forth in Subsection 1.5(B).

(H) **"Surveillance Use Policy"** means a policy for the City's use of Surveillance Technology, approved by the City Solicitor and the Mayor's Office, and submitted by the Mayor's Office to and approved by the City Council. The Surveillance Use Policy shall at a minimum satisfy the requirements set forth in Section 1.4.

(I) **"Technology-Specific Surveillance Use Policy"** means a policy governing the City's use of a specific Surveillance Technology not already covered under the City's Surveillance Use Policy, approved by the City Solicitor and the Mayor, and submitted by the Mayor to the City Council with a Surveillance Technology Impact Report under Section 1.5of this Ordinance.

Section 1.3 Exceptions and Exemptions

(A) For the purposes of this Ordinance, the following do not constitute Surveillance Data or Surveillance Technology, and the requirements of this Ordinance do not apply to them:
i. Surveillance Data acquired where the individual knowingly and voluntarily consented to provide the information, such as submitting personal information for the receipt of City services;
ii. Surveillance Data acquired where the individual was presented with a clear and conspicuous opportunity to opt out of providing the information;

(B) For the purposes of this Ordinance, Surveillance Technology and Surveillance Data do not include the following devices, software, or hardware and are exempt from the requirements of this Ordinance, unless the devices, hardware, or software are modified to include additional surveillance capabilities as defined in Section 1.2:
i. 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;

ii. Parking Ticket Devices ("PTDs") and related databases.

iii. 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;

iv. Body-worn cameras;

v. Cameras installed in or on a police vehicle;

vi. Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations or traffic patterns, provided that the Surveillance Data gathered is used only for that purpose;

vii. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

viii. City databases that do not and will not contain any Surveillance Data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology;

ix. 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;

x. Parking access and revenue control systems, including proximity card readers and transponder readers at City- owned or controlled parking garages; and

xi. Card readers and key fobs used by City employees and other authorized persons for access to City- owned or controlled buildings and property.

xii. 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;

xiii. 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;

xiv. Cameras installed solely to protect the physical integrity of City infrastructure; or

xv. Technology that monitors only City employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of City resources.

(C) The following situations are exceptions to the requirements of this Ordinance:

i. Notwithstanding the provisions of this Chapter, the Police Department may temporarily acquire or temporarily use Surveillance Technology in Exigent Circumstances for a period not to exceed 90-days 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 Technology 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 Technology 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 requesting to extend this period. The City Council may grant extensions beyond the original 90-day timeline to submit a Surveillance Technology Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy. Any Surveillance Technology Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under this Section shall be made publicly available upon submission to the City Council.

ii. A City department head may 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 1.5 are met, unless the Mayor, or his/her designee, determines that the use is unavoidable; in that case, the Mayor 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.

Section 1.4 Submission to the City Council of Surveillance Use Policy

(A) The Mayor 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 Ordinance. Any Surveillance Use Policy submitted under Section 1.4 shall be made publicly available upon submission to the City Council.

(B) A Surveillance Use Policy shall at a minimum specify the following:

i. Purpose: The specific purpose(s) for the Surveillance Technology;

ii. Authorized Use: The uses that are authorized, the rules and processes required before that use, and the uses that are prohibited;
iii. Data Collection: The Surveillance Data that can be collected by the Surveillance Technology;
iv. Data Access: The individuals who can access or use the collected Surveillance Data, and the rules and processes required before access or use of the information;
v. Data Protection: The safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms;
vi. 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 has elapsed, and the conditions that must be met to retain information beyond that period;
vii. Public Access: If and how collected Surveillance Data can be accessed by members of the public, including criminal defendants;
viii. Third-Party Data-Sharing: If and how other City or non-City entities can access or use the Surveillance Data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the Surveillance Data;
ix. 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; and
x. 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.

(C) In considering 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.

Section 1.5 Submission to the City Council of Surveillance Technology Impact Report and Technology-Specific Surveillance Use Policy

The Mayor's Office must seek and obtain approval from the City Council as set forth in this Section prior to the City acquiring, using or entering into an agreement to acquire, share or otherwise use, Surveillance Technology or Surveillance Data as defined in this Ordinance. The

City may seek, but not accept, funds for Surveillance Technology without approval from the City Council, provided that the City shall notify the City Council of the funding application at the time it is submitted, and include in this notification (i) the deadline of the funding opportunity, and (ii) details regarding the nature of the Surveillance Technology for which funding is sought.

(A) **Acquisition of Surveillance Technology by City Departments**. Unless exempted or excepted from the requirements of this Ordinance pursuant to section 1.3, any City department intending to i) acquire new Surveillance Technology or Surveillance Data, including but not limited to procuring that Surveillance Technology without the exchange of monies or other consideration, or ii) using approved Surveillance Technology or Surveillance Data for a purpose, in a manner, or in a location, not previously approved, shall, prior to acquisition or use, obtain Council approval of the acquisition or use. The process for obtaining approval shall be as follows:

i. The City department shall submit a Surveillance Technology Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy, as described in subsections 1.5B and 1.5C below, to the Mayor's Office for review and approval.
ii. If the request is approved by the Mayor's Office, the Mayor's office shall submit the request, including copies of the City department's Surveillance Technology Impact Report and, if applicable, Technology-Specific Surveillance Use Policy, to the City Council for review.
iii. The City Council shall have sixty (60) days, which shall not include June, July, nor August, from the date of submission to approve or deny a request for the acquisition of Surveillance Technology. If the City Council fails to approve or deny the request within that time frame, the request shall be approved by default.
iv. Any Surveillance Technology approved by default under the provisions in 1.5(A)(iii) must be subsequently approved or rejected by the City Council during the following Annual Report.

(B) **Contents of Surveillance Technology Impact Report.** A Surveillance Technology Impact Report submitted pursuant to Subsections (A) above shall include all of the following:

i. Information describing the Surveillance Technology and how it works;
ii. Information on the proposed purpose(s) for the Surveillance Technology;
iii. Information describing the kind of surveillance the Surveillance Technology is going to conduct and what Surveillance Data is going to be gathered;
iv. The location(s) it may be deployed and when;
v. A description of the privacy and anonymity rights affected and a mitigation plan describing how the department's use of the equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse.
vi. The potential impact(s) on privacy in the City; the potential impact on the civil rights and liberties of any individuals, 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);

vii. An estimate of the fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding; and

viii. An explanation of how the Surveillance Use Policy will apply to this Surveillance Technology and, if it is not applicable, a Technology-Specific Surveillance Use Policy.

(C) **Contents of Technology-Specific Surveillance Use Policy**. A Technology Specific Surveillance Use Policy shall be required if the purpose, authorized use, data collection, data access, data protection, data retention, public access, third party data sharing, training, or oversight of the requested Surveillance Technology submitted under Subsection (A) above differ from the standards in the Surveillance Use Policy submitted under Section 1.4. A Technology Specific Surveillance Use Policy shall not conflict with any provision of the City's Surveillance Use Policy. To the extent a conflict arises between the provisions of the City's Surveillance Use Policy and a Technology-Specific Surveillance Use Policy, the City's Surveillance Use Policy shall govern. A Technology-Specific Surveillance Use Policy shall include all of the elements of the Surveillance Use Policy as outlined in Section 1.4(B) i.-x.

(D) In approving or disapproving any acquisition or use 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.

(E) Any Surveillance Technology Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under Section 1.5(B) or 1.5(C) shall be made publicly available upon submission to the Council.

Section 1.6 Submission to the City Council of Annual Surveillance Report

(A) Within twelve (12) months of the effective date, and annually thereafter, all City Departments shall submit to the Mayor an Annual Surveillance Report pertaining to each City Department for which approval for the use of Surveillance Technology or Surveillance Data has been obtained under Section 1.5 of this Ordinance. Upon receipt of such reports, the Mayor shall promptly submit them to the City Council. Any Annual Surveillance Report submitted under this section shall be made publicly available upon submission to the Council.

(B) The Annual Surveillance Report submitted pursuant to this Section shall include all of the following:

i. A description of how 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;

ii. Whether and how often data acquired through the use of the

Surveillance Technology was shared with local, state, and federal, 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;

iii. A summary of community complaints or concerns about the Surveillance Technology, if any;

iv. The results of any non-privileged internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;

v. Whether the Surveillance Technology has been effective at achieving its identified purpose;

vi. The number of public records requests received by the City seeking documents concerning Surveillance Technology approved during the previous year;

vii. An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known; and

viii. 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.

(C) 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 Mayor for his consideration; and/or (2) request a report back from the Mayor regarding steps taken to address the City Council's concerns.

(D) Nothing in this Ordinance shall prohibit the City Council from enacting a separate Ordinance to ban or otherwise regulate any surveillance technology, whether previously approved or not.

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 Technology received by the City Council during the prior year, including whether the City Council approved or disapproved of the Surveillance Technology.

Section 1.7 Enforcement

(A) Enforcement Officials. This Ordinance shall be enforced by the Mayor's Office or the Mayor's designee.

(B) Suppression: No data collected or derived from any use of Surveillance Technology in violation of this ordinance and no evidence derived therefrom may be received in evidence in any proceeding in or before any department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of the City of Somerville.

(C) Cause of Action: Any violation of this Ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the City and, if necessary to effectuate compliance with this Ordinance, any other governmental agency with possession, custody, or control of data subject to this Ordinance.

(D) The City will address alleged violations of this ordinance in accordance with its usual practices, applicable law and contractual obligations.

(E) Violation. Any person injured by a violation of this Ordinance may institute proceedings for injunctive relief, declaratory relief, or a court order in a court of competent jurisdiction to enforce the provisions of this Ordinance. Any action initiated under this Subsection (B) shall be brought against the City of Somerville, but not against City employees. No monetary damages shall be allowed in any legal proceeding for any alleged injuries arising out of any alleged violation(s) of this Ordinance.

(F) Whistleblower Protections. Subject to the limitations and requirements set forth in G. L. c. 149, §185 (the "Massachusetts Whistleblower Statute" or "Section 185") as it may be amended from time to time, any City employee as defined in Section 185 who reports an alleged violation of this Ordinance, shall be afforded protections against retaliation if applicable pursuant to Section 185, as set forth in and subject to the limitations and requirements of Section 185.

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

Section 1.8 Severability

The provisions in this Ordinance are severable. If any part or provision of this Ordinance, or the

application of this Ordinance to any person or circumstance, is held invalid by a court of competent jurisdiction, the remainder of this Ordinance shall not be affected by such holding and shall continue to have full force and effect.

Section 1.9 Effective Date

This Ordinance shall take effect nine months after its adoption.