OFFERED BY COUNCILORS RICARDO ARROYO & KIM JANEY

WU, FLAHERTY, EDWARDS, MEJIA, CAMPBELL, BREADON, BOK, FLYNN AND O'MALLEY

CITY OF BOSTON
IN CITY COUNCIL

ORDINANCE ON SURVEILLANCE OVERSIGHT AND INFORMATION SHARING

WHEREAS, Governments around the world are responding to the COVID-19 pandemic with an unprecedented use of surveillance tools, despite public health and privacy experts agreeing that public trust is essential to an effective response to the pandemic; *and*

WHEREAS, Surveillance technology and electronic data gathering can be useful tools for advancing effective delivery and analysis of constituent services, public safety and security; *and*

WHEREAS, Usage of surveillance technology must include safeguards with accountability to the public in order to protect privacy rights and civil liberties; *and*

WHEREAS, Boston Public Schools should be welcoming and safe environments for all students regardless of immigration status or race. Due to COVID-19, Boston Public Schools has transitioned entirely to online learning where it is expected that even after returning to in-person learning, technology will be a larger part of education; *and*

WHEREAS, As people in Boston and across the state are sheltering in place, we are growing more dependent on technology to connect us to each other and to our government; *and*

WHEREAS, Cities around the country such as Cambridge, Somerville, Santa Clara, and Providence have created ordinances governing the acquisition and use of surveillance technology and electronic data in order to protect the civil liberties of their citizens while allowing for appropriate use to assist in the charge of improving delivery of services and public safety; *and*

WHEREAS, As more municipalities move toward electronic data collection used to manage assets and resources efficiently and new technologies are becoming available, the public would benefit from proactive discussion of current practices and future acquisitions; *NOW THEREFORE BE IT ORDERED*,

That the following shall take effect immediately upon passage:

Chapter 1 - Purpose.

The purpose of this ordinance is to provide accountability, transparency, and oversight regarding the acquisition and use of Surveillance Technology and Surveillance Data by the City of Boston and its agencies and officers, and to protect privacy, civil rights, and racial and immigrant justice.

Chapter 2 - Generally

Section 1 - Definitions.

1. The following definitions apply to this Ordinance:
    1.1. *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 this ordinance.
    1.2. *Exigent Circumstances* means the police commissioner or the police commissioner'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 the 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 or exercise other lawful and protected constitutional rights.
    1.3. *Identifiable Individual* 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.
    1.4. *Surveillance* means the act of observing or analyzing the movements, behavior, or actions of Identifiable Individuals.
    1.5. *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.
    1.6. *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, associational, 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.

1.7. Examples of Surveillance Technology include, but are not limited to:

1.7.1. International mobile subscriber identity (IMSI) catchers and other cell-site simulators;

1.7.2. Automatic license plate readers;

1.7.3. Electronic toll readers;

1.7.4. Closed-circuit television cameras except as otherwise provided herein;

1.7.5. Biometric Surveillance Technology, including facial, voice, iris, and gait-recognition software and databases;

1.7.6. Mobile DNA capture technology;

1.7.7. Gunshot detection and location hardware and services;

1.7.8. X-ray vans;

1.7.9. Video and audio monitoring and/or recording technology, such as surveillance cameras;

1.7.10. Surveillance enabled or capable light bulbs or light fixtures;

1.7.11. Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network;

1.7.12. Social media monitoring software;

1.7.13. Through-the-wall radar or similar imaging technology;

1.7.14. Passive scanners of radio networks;

1.7.15. Long-range Bluetooth and other wireless-scanning devices;

1.7.16. Thermal imaging or "forward-looking infrared" devices or cameras;

1.7.17. Electronic database systems containing Surveillance Data about Identifiable Individuals;

1.7.18. Radio-frequency identification (RFID) scanners; and

1.7.19. Software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software.

1.8. *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 this ordinance.

1.9. *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 this ordinance.

1.10. *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 this ordinance.

1.11. *BPS* means the Boston Public Schools.

1.12. *BPS personnel* means any employee or agent of the Boston Public Schools, excluding BSP officers.

1.13. *BSP officers* means any officials or general employees that belong to the Boston School Police and that are licensed by the Boston Police Department as special police officers.

1.14. *BPD* means the City of Boston Police Department.

1.15. *Student Report* means a written record created by a BSP officer that pertains to student activity. This includes but is not limited to School Safety Reports, BPD Form 1.1 Incident Reports, Field Interrogation and Observation Reports, Intelligence Reports, and Face Sheets.

1.16. *Seriously body harm* means bodily injury that results in permanent disfigurement, loss or impairment of a bodily function, limb or organ, or substantial risk of death.

Section 2 - Exceptions and Exemptions.

2. The following situations are exceptions and exemptions from this ordinance:

2.1. The following do not constitute Surveillance Data and the requirements of this ordinance do not apply to them:

2.1.1. 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; and

2.1.2. Surveillance Data acquired where the individual was presented with a clear and conspicuous opportunity to opt-out of providing the information.

2.2. Surveillance Technology does not include the following devices, software, or hardware, which are exempt from the requirements of this ordinance, unless the devices, hardware, or software are modified to include additional surveillance capabilities:

2.2.1. 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;

2.2.2. Parking ticket devices (PTDs) and related databases;

2.2.3. 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;

2.2.4. Cameras installed in or on a police vehicle;

2.2.5. 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;

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

2.2.7. 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;

2.2.8. 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;

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

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

2.2.11. 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;

2.2.12. 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;

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

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

2.3. Notwithstanding the provisions of this ordinance, the police Department may temporarily acquire or temporarily use Surveillance Technology in Exigent Circumstances for a period not to exceed 30 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 Commissioner of police must:

2.3.1.1. Report that acquisition or use to the City Council in writing as soon as possible;

2.3.1.2. Submit a Surveillance Technology Impact Report, and, if necessary, a technology-specific Surveillance Use Policy to the City Council regarding that Surveillance Technology within 30 days following the end of those Exigent Circumstances; and

2.3.1.3. Include that Surveillance Technology in the police Department's next Annual Surveillance Report to the City Council following the end of those Exigent Circumstances.

2.3.1.4. If the Commissioner of Police is unable to meet the 30-day timeline to submit a Surveillance Technology Impact Report and, if necessary, a technology-specific Surveillance Use Policy to the City Council, the Commissioner of police must notify the City Council in writing requesting to extend this period. The City Council may grant extensions beyond the original 30-day timeline to submit a Surveillance Technology Impact Report, and, if necessary, a technology-specific Surveillance Use Policy.

2.3.1.5. Any Surveillance Technology Impact Report, and, if necessary, any Technology-Specific Surveillance Use Policy submitted to the City Council under this subsection shall be made publicly available on the City's website upon submission to the City Council.

2.3.1.6. Any Surveillance Technology Impact Report and, if necessary, technology-specific Surveillance Use Policy submitted to the City Council under this section may be redacted to the extent required to comply with an order by a court of competent jurisdiction, or to exclude information that, in the reasonable discretion of the Commissioner of police, if disclosed, would materially jeopardize an ongoing investigation or otherwise represent a significant risk to public safety and security provided, however, that any information redacted pursuant to this paragraph will be released in the next Annual Surveillance Report following the point at which the reason for such redaction no longer exists.

2.4. 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 this ordinance 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.

Chapter 3 - Community Control Over Surveillance

Section 3 - Surveillance Use Policy.

3. Surveillance Use Policy
   - 3.1. 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.
   - 3.2. Any Surveillance Use Policy submitted under this section shall be made publicly available upon submission to the City Council.
   - 3.3. A Surveillance Use Policy shall at a minimum specify the following:
     - 3.3.1. Purpose: the specific purpose(s) for the Surveillance Technology;
     - 3.3.2. Authorized use: the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited;
     - 3.3.3. Data collection: the Surveillance Data that can be collected by the Surveillance Technology;
     - 3.3.4. 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;
     - 3.3.5. Data protection: the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms;
     - 3.3.6. 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 has elapsed, and the conditions that must be met to retain information beyond that period;
     - 3.3.7. Public access: if and how collected Surveillance Data can be accessed by members of the public, including criminal defendants;
     - 3.3.8. Information and data-sharing: if and how other City or non-City entities can access or use the Surveillance Data, how information is shared among City agencies or between City agencies and non-City entities and organizations, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the Surveillance Data;

3.3.9. Training: the training, if any, required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology, including whether there are training materials;

3.3.10. 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, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy;

3.3.11. Legal Authority: the statutes, regulations, or legal precedents, if any, that control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology; and

3.3.12. Child Rights: special considerations specific to Surveillance Technology and Surveillance Data pertaining to minor children.

3.4. The City Council shall vote to approve or deny the Surveillance Use Policy by a vote of a simple majority.

Section 4 - Surveillance Technology Impact Report and technology-specific Surveillance Use Policy.

4. Surveillance Technology Impact Report and technology-specific Surveillance Use Policy.

4.1. 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, unapproved Surveillance Technology or Surveillance Data as defined in this ordinance.

4.1.1. 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 the deadline of the funding opportunity and details regarding the nature of the Surveillance Technology for which funding is sought.

4.2. Acquisition of Surveillance Technology by City Departments. Unless exempted or excepted from the requirements of this ordinance, any City Department intending to 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 use Surveillance Technology or Surveillance Data for a purpose or in a manner 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:

4.2.1. The City Department shall submit a Surveillance Technology Impact Report, and, if necessary, a technology-specific Surveillance Use Policy, as described below, to the Mayor's office for review and approval.

4.2.2. 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.

4.2.3. The City Council shall have 90 days from the date of submission to approve or deny a request by majority vote for the acquisition or use of Surveillance Technology.

4.2.4. Contents of Surveillance Technology Impact Report. A Surveillance Technology Impact Report submitted shall include all of the following:

4.2.5. Information describing the Surveillance Technology and how it works;

4.2.6. Information on the proposed purpose(s) for the Surveillance Technology;

4.2.7. Information describing the kind of surveillance the Surveillance Technology will conduct and what Surveillance Data will be gathered, including a detailed accounting of which entities may have access to any Surveillance Data, under what circumstances (e.g. ongoing automated access, subject to an informal request, subject to subpoena, subject to a warrant, etc.);

4.2.8. The location(s) the Surveillance Technology may be deployed and when;

4.2.9. 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 and anonymity, and to limit the risk of abuse;

4.2.10. 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 a plan to address these impact(s);

4.2.11. 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

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

4.3. 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 differ from the standards in the Surveillance Use Policy submitted under sections 3 and 4.

4.3.1. A Technology-Specific Surveillance Use Policy shall not conflict with any provision of the City's Surveillance Use Policy.

4.3.2. 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 3.

4.4. Any Surveillance Technology Impact Report, and, if necessary, technology-specific Surveillance Use Policy submitted to the City Council under sections 3 or 4 shall be made publicly available on the City's website upon submission to the council.

Chapter 4 - Student Information Sharing Policies

Section 5 - Boston Public Schools and Boston Police Department Information-Sharing Policy

5. Boston Public Schools and Boston Police Department Information-Sharing Policy

5.1. Student Reports

5.1.1. BSP officers may create a Student Report only when:

5.1.1.1. Serious bodily harm to an individual has occurred as a result of willful conduct by a student;

5.1.1.2. A true and credible threat to the safety of the school arises that would amount to criminal conduct;

5.1.1.3. A student is in possession of firearms; or

5.1.1.4. A student unlawfully possesses or uses controlled substances, provided those substances are not marijuana, nicotine, or alcohol.

5.1.2. BSP officers may not create a Student Report relating to matters that are not described above.

5.1.3. Student reports shall not contain information pertaining to:

5.1.3.1. Immigration status

5.1.3.2. Citizenship

5.1.3.3. Neighborhood of residence

5.1.3.4. Religion

5.1.3.5. National origin

5.1.3.6. Ethnicity

5.1.3.7. Students' native or spoken language
5.1.3.8. Suspected gang affiliation
5.1.3.9. Participation in school activities, extracurricular activities outside of school, sports teams, or school clubs or organizations
5.1.3.10. Degrees, Honors, or Awards
5.1.3.11. Post-high school plans

5.1.4. Principals and Headmasters of schools where Student Reports are written must receive copies of all Student Reports written under this section immediately upon writing.

5.1.5. Within 24 hours of the writing of a Student Report under this section, the Principal or Headmaster of the school where the Student Report was written must provide any student named in the Student Report and their family a copy of the Student Report.

5.2. Transmitting information to the BPD and other entities outside the Boston Public Schools

5.2.1. BSP officers may transmit Student Reports written under section 5.1.1 to the BPD.

5.2.2. BSP officers shall not transmit to BPD any information about students through any official or unofficial channels, including but not limited to text, phone, email, database, and in-person communication, except in Exigent Circumstances and through Student Reports as authorized in section 5.1.1.

5.2.3. BPS personnel and BSP officers may not send information relating to Boston Public Schools students to the Boston Regional Intelligence Center (BRIC) under any circumstances.

5.2.4. Before a Student Report, or any other information relating to a student, is transmitted to the BPD or any other entity outside of the Boston Public Schools, the following must take place, absent Exigent Circumstances:

5.2.4.1. Any student named in a Student Report or other record, and their parent or guardian, must be notified in writing and receive a copy of any written report and an explanation of the incident prompting the communication to BPD. All written materials must be provided in both English and the language spoken by the family, if applicable.

5.2.4.2. The Boston Public Schools must schedule a meeting with the student and the student's parent or guardian as soon as practicable, and an interpreter of the family's choosing must be present for any party that requires one. The interpreter cannot be the student or other individual who is participating in the meeting in another

capacity. If the family does not have a preferred interpreter, BPS must provide a qualified translator.

5.2.4.3. The student and family may have an attorney and/or advocate present at the meeting. Before the meeting, BPS must provide the family with a list of available legal services vetted by the Mayor's Office of Immigrant Advancement.

5.2.4.4. The Principal/Headmaster of the school where the incident took place, the Superintendent, and the Legal Advisor for the School Department must review the Student Report and the Legal Advisor for BPS must verify that at least one of the criteria in 5.1.1 is present. If the Legal Advisor finds that the incident did not meet the criteria in 5.1.1, they must place a note in the record attesting to this fact, and the Student Report may not be transmitted to the BPD or any entity outside of BPS.

5.2.4.5. Students and families may amend a student's record by placing a note with information relating to any Student Report in which the student is named in the student's file.

5.2.5. BPS personnel may not transmit to the BPD any student information, including but not limited to a Student Report, unless in response to a judicial warrant issued upon a finding of probable cause, as required under MGL c. 269, sec. 10(j) and MGL c. 71, sec. 37L, or as otherwise required by state or federal law. Nothing in this ordinance shall limit the ability of Boston Public Schools to release information as required by state or federal laws and regulations, or when the information directly pertains to exigent circumstances.

5.3. Transparency and Communication

5.3.1. Students, families, school administrators, teachers, and counselors must be made aware of this ordinance by including a copy of the ordinance in the Guide to Boston Public Schools.

5.4. Community Information-Sharing Oversight Board

5.4.1. A community oversight board shall be created to provide oversight regarding the implementation of Section 5 of this ordinance.

5.4.2. The board shall be appointed by the Mayor and shall include at least one representative from each of the following groups: a student chosen by the Boston Student Advisory Council, a parent or guardian chosen by the Citywide Parent Council, a teacher chosen by the Boston Teachers Union, a local immigration advocate chosen by the Student Immigrant Movement, a civil rights advocate chosen by Lawyers for Civil Rights, and an immigration attorney familiar with the immigration consequences of

criminal proceedings chosen by the Political Asylum/Immigration Representation Project.

5.4.3. The Superintendent shall report monthly to the board:

5.4.3.1. The number of Student Reports created, disaggregated by school;

5.4.3.2. The number of Student Reports shared with any outside entity, disaggregated by school and receiving entity;

5.4.3.3. The number of Student Reports reviewed by the Legal Advisor for the School Department that did not meet the criteria specified in 5.1.1, disaggregated by school, and including the date of each incident, a description of each incident, the race, gender, age, and grade level of each student who is named in the report, the location of the incident, and whether the report was transmitted to BPD or to any other outside entity.

5.4.3.4. The number of Student Reports written under section 5.1, disaggregated by school, including the date of the incident, a description of the incident including the justification for the creation of the report per Section 5.1.1, the type of report, the race, gender, age and grade of each student who is named in the report, the location of the incident, and whether the report was transmitted to BPD or to any other outside entities.

5.4.4. The board will review the information provided under 5.4.3 and may request that BSP or District personnel respond to questions, either in writing or at a public meeting, relating to the information provided.

5.4.5. The board shall review the information for patterns and compliance with this ordinance. It shall issue findings and report such findings to the City Council and School Committee on a quarterly basis.

5.5. Accountability and Training

5.5.1. All BSP officers and school administrators must receive training on this policy, and the training will be designed in collaboration with the Student Immigrant Movement and Boston Teachers Union's Unafraid Educators. The training will also be provided by the Central Office and not by individual schools. Training materials will be made publicly available.

5.5.2. All BSP officers and BPS personnel, including school administrators, will sign an acknowledgment of responsibility for safeguarding student information under Section 5 of this ordinance, FERPA, and state student records law.

5.5.3. All new BSP officers will receive training on the requirements of Section 5 of this ordinance as part of their orientation.

5.5.4. All BSP officers must be trained every three years or at the discretion of

the community oversight board.

5.5.5. Any transfer of information about students in violation of Section 5 of this ordinance shall result in appropriate disciplinary action, up to and including dismissal, in accordance with the rules of collective bargaining.

5.5.6. Should any BSP officer be found to have violated this policy, the Superintendent will instruct the Chief of Safety Services to suspend all authorization of BSP report submissions to BPD pending a full investigation of such violation.

Chapter 5 - Annual Surveillance Report

Section 6 - Annual Surveillance Report

6. **Annual surveillance report.**

6.1. Within 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 3 and 4 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 on the City's website upon submission to the council.

6.2. The Annual Surveillance Report submitted pursuant to this section shall include all of the following:

6.2.1. A description of how Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct;

6.2.2. 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, any legal standard(s) under which the information was disclosed, and the justification for the disclosure;

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

6.2.4. The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City;

6.2.5. A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose;

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

6.2.7. 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;

6.2.8. 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; and

6.2.9. A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using Surveillance Technology or the Surveillance Data it provides.

6.3. 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 the 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 recommend modifications to the Surveillance Use Policy that are designed to address the City Council's concerns to the Mayor for his consideration; withdraw authorization for continued use of Surveillance Technology by a majority vote of the City Council; and/or request a report back from the Mayor regarding steps taken to address the City Council's concerns.

6.4. 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.

6.5. 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 denied the City's request for acquisition or use of the Surveillance Technology.

Chapter 6 - Miscellaneous

Section 7 - Enforcement

7. Enforcement**.**

7.1. Enforcement officials: This ordinance shall be enforced by the Mayor's office or the Mayor's designee.

7.2. 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 Boston.

7.3. 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.

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

7.5. 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.

7.6. Nothing in this ordinance shall be construed to limit or affect any individual's rights under state or federal laws.

Section 8 - Severability

8. Severability**.**

8.1. 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 9 - Effective Date

9. Effective date.

9.1. Sections 1, 5, 7, and 8 shall take effect one month after its adoption.

9.2. Sections 2, 3, 4, and 6 shall take effect nine months after its adoption.

Filed on: May 6, 2020