

Section 50, Article III - An Ordinance To Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology

Section 50–70. - Purpose and Intentions.

The purpose of this Ordinance is to provide for the regulation of Surveillance Technology acquisition or use by the City of Medford or the use of the Surveillance Data it provides, to:

- safeguard the right of individuals to privacy;
- balance the public's right to privacy with the need to promote and ensure safety and security;
- 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;
- balance any decision to use Surveillance Technology with an assessment of the costs and protection of privacy, civil liberties, and civil rights;
- allow for informed public discussion before deploying Surveillance Technology;
- provide for transparency, oversight, and accountability;
- and to minimize the risks posed by use of Surveillance Technology in the City.

Nothing in this ordinance should be interpreted as:

- preventing compliance with warrants or court orders;
- requiring disclosures or any other actions that would violate explicit confidentiality provisions contained within warrants or court orders;
- preventing compliance with federal or state authorities' requests to use surveillance technology or share surveillance data where such use is authorized pursuant to this ordinance.
- requiring disclosures that are so detailed and specific as to imperil ongoing police investigations or impinge upon the privacy of individual actors.

Section 50–71. - Definitions

For the purposes of this Ordinance:

- (A) "Surveillance" shall mean the act of observing or analyzing the movements, behavior, or actions of Identifiable Individuals.

(B) "Identifiable Individual" shall mean 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.

(C) "Municipal entity" shall mean any municipal government, agency, department, bureau, division, or unit of this City.

(D) "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, similar to those that would render it 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 or protected constitutional rights.

(E) "Surveillance Data" shall mean any data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by Surveillance Technology.

(F) "Viewpoint-based" shall mean targeted at any community or group or its members because of their exercise of rights protected under the First Amendment of the United States Constitution.

(G) "Surveillance Technology" shall mean 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, behavioral, 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; (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, wide-angle cameras, and wearable body cameras; (j) surveillance enabled or capable light-bulbs 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 I.D. (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 Ordinance, the following do not constitute Surveillance Data or Surveillance Technology, and the requirements of this Ordinance do not apply to them:

- a. 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;

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

3. For the purposes of this Ordinance, "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 in this section:

- a. Office hardware, such as televisions, computers, smart phones or handheld devices, credit card machines, copy machines, telephones, and printers that are in widespread use by the City and are used for routine City business and transactions;
- b. City databases and enterprise systems that contain information kept in the ordinary course of City business, including, but not limited to, human resources, permits, licenses, and business records;
- c. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology, including payroll, accounting, or other fiscal databases;
- d. Information technology security systems, including firewalls and other cybersecurity systems;
- e. Physical access control systems, employee identification management systems, inventory control systems, and other physical control systems;
- f. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

- g. LiDAR technology and systems used for Geographic Information Systems imagery purposes;
- h. Global Positioning System technology used to collect field data or track City-owned vehicles that are stored on City property when not in use;
- i. Computers, software, hardware, or other devices used in monitoring the work and work-related activities involving City employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
- j. Cameras installed on the exterior or the interior of City property solely for security purposes, such as to monitor entryways and outdoor areas of City-owned or controlled buildings and property for the purpose maintaining the safety of City employees and visitors to City buildings, protecting City property, or to protect the physical integrity of City infrastructure;
- k. Cameras, computers, software, hardware, or devices used for videoconferencing or to facilitate broadcast or recording of public meetings;
- l. Police department interview room, holding cell, and police department internal security audio/video recording systems;
- m. Police department computer-aided dispatch (CAD), records/case management, DCJIS, III, Live Scan, booking, Department of Motor Vehicles, 9-1-1, and related dispatch and operation or emergency services systems;
- n. Police department early warning systems;
- o. Parking Ticket Devices ("PTDs") and related databases;
- p. Manually-operated, handheld cameras, audio recorders, and video recorders whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;
- q. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- r. Manually-operated technological devices that are used primarily for internal City communications, such as radios, personal communications devices, and email systems; and
- s. Parking access and revenue control systems, including proximity card readers and transponder readers at City-owned or controlled parking garages.

4. For the purposes of this Ordinance, traffic monitoring technologies, as well as recording and streaming technologies used for the broadcast of live events, shall be exempted.

Section 50–72. - City Council Approval Mandatory for Surveillance Technology Funding, Acquisition, or Use

(A) A municipal entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public City Council hearing at which the public is afforded a fair and adequate opportunity to provide online, written, and oral testimony, prior to engaging in any of the following:

1. Seeking funds for new Surveillance Technology, including but not limited to soliciting or accepting state or federal funds or in-kind or other donations;
2. Acquiring or borrowing new Surveillance Technology, whether or not that acquisition is made through the exchange of monies or other consideration;
3. Using new or existing Surveillance Technology for a purpose or in a manner not previously approved by the City Council in accordance with this Ordinance, including the sharing of Surveillance Data therefrom; or
4. Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share or otherwise use Surveillance Technology or Surveillance Data.
5. Further, 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.

(B) Body Worn Cameras shall be exempt from Section 50–72 of this Ordinance until January 1, 2028.

Section 50–73. - Surveillance Impact Report and Surveillance Use Policy Submission

(A) As a part of the process of seeking City Council approval, pursuant to Section 50-72(A), to fund, acquire, or use Surveillance Technology or to enter into an agreement concerning such funding, acquisition, or use, a municipal entity shall submit to the City Council and make publicly available a **Surveillance Impact Report and Surveillance Use Policy** concerning the technology at issue.

1. No use of Surveillance Technology by a municipal entity pursuant to Section 50-72(A) shall be permitted without the City Council's express approval of the related

Surveillance Impact Report and Surveillance Use Policy submitted by the municipal entity pursuant to Section 50-73(A).

2. Prior to approving or rejecting a Surveillance Impact Report or Surveillance Use Policy submitted pursuant to Section 50-73(A), the City Council may request revisions be made by the submitting municipal entity.

(B) Surveillance Impact Report: A Surveillance Impact Report submitted pursuant to Section 50-73(A) shall be a publicly-released, mandatory written report. This shall contain a description of the Surveillance Technology so as to provide the public and City Council with a general understanding of the Surveillance Technology's workings and the reasons for which it is sought for use in the city. Nothing in this section should be interpreted as requiring information that is substantially more detailed or technical than what is publicly available from the manufacturer of a surveillance technology, i.e. on a product website, unless the description of the capabilities to be used by the city are not publicly available. The Surveillance Impact Report shall include, at a minimum, the following:

1. Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers;
2. Information on the proposed purpose(s) of the Surveillance Technology;
3. If the Surveillance Technology will not be uniformly deployed or targeted throughout the city, what factors will be used to determine where the technology is deployed or targeted;
4. The fiscal impact of the Surveillance Technology; and
5. An assessment identifying with specificity:
 - a. Any potential adverse impacts the Surveillance Technology, if deployed, might have on civil liberties and civil rights; and
 - b. What specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts identified pursuant to Section 50-73(B)(5)(a).

(C) Surveillance Use Policy: A Surveillance Use Policy submitted pursuant to Section 50-73(A) shall be a publicly-released, legally enforceable written policy governing the municipal entity's use of the Surveillance Technology that, at a minimum, includes and addresses the following:

1. Purpose: What specific purpose(s) the Surveillance Technology is intended to advance.

2. Authorized Use: For what specific capabilities and uses of the Surveillance Technology is authorization being sought, and
 - a. What legal and procedural rules will govern each authorized use;
 - b. What potential uses of the Surveillance Technology will be expressly prohibited, such as the warrantless surveillance of public events and gatherings; and
 - c. How and under what circumstances will Surveillance Data that was collected, captured, recorded, or intercepted by the Surveillance Technology be analyzed and reviewed.
3. Data Collection:
 - a. What types of Surveillance Data will be collected, captured, recorded, intercepted, or retained by the Surveillance Technology;
 - b. 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; and
 - c. How inadvertently collected Surveillance Data will be expeditiously identified and deleted.
4. Data Protection: What safeguards will be used to protect Surveillance Data from unauthorized access, including encryption and access control mechanisms.
5. Data Retention: Insofar as the privacy of the public can be severely compromised by the long-term storage of mass Surveillance Data, what rules and procedures will govern the retention of Surveillance Data, including those governing:
 - a. For what time period Surveillance Data will be retained. Such information shall include a statement explaining why the designated retention period is no greater than that which is absolutely necessary to achieve the specific purpose(s) enumerated in the Surveillance Use Policy;
 - b. What specific conditions must be met to retain Surveillance Data beyond the retention period stated in Section 50-73(C)(5)(a);
 - c. By what process Surveillance Data will be regularly deleted after the retention period stated in Section 50-73(C)(5)(a) elapses and what auditing procedures will be implemented to ensure data is not improperly retained;
6. Surveillance Data Sharing: If a municipal entity is seeking authorization to share access to Surveillance Technology or Surveillance Data with any other governmental agencies, departments, bureaus, divisions, or units, it shall detail:
 - a. How it will require that the collection, retention, and storage of Surveillance Data be conducted;
 - b. Which governmental agencies, departments, bureaus, divisions, or units will be approved for (i) Surveillance Technology sharing, and for (ii) Surveillance Data sharing;
 - c. How such sharing is necessary for the stated purpose and use of the Surveillance Technology;

- d. 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; and
 - e. What processes will be used to seek approval of future Surveillance Technology or Surveillance Data sharing agreements from the municipal entity and City Council.
- 7. Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to Surveillance Data.
 - 8. Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use Policy is followed, including what independent persons or entities will be given oversight authority, and what legally enforceable sanctions will be put in place for violations of the policy.
 - 9. Complaints: What procedures will be put in place by which members of the public can register complaints or concerns or submit questions about the deployment or use of a specific Surveillance Technology, and how the municipal entity will ensure each question and complaint is responded to in a timely manner.

(D) Any Surveillance Technology Impact Report and Surveillance Use Policy submitted to the City Council under this Section may be redacted (a) to the extent required to comply with an order by a court of competent jurisdiction or (b) to exclude information that in the, reasonable discretion of the Chief 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.

(E) Body Worn Cameras shall be exempt from Section 50-73 of this Ordinance until January 1, 2028.

Section 50–74. - Review of Preexisting Uses Mandatory

(A) No later than ninety (90) days following the effective date of this Ordinance or prior to implementation of any new Surveillance Technology use covered by this Ordinance, any municipal entity seeking to continue the use of any Surveillance Technology that was in use prior to the effective date of this Ordinance, or the sharing of Surveillance Data

therefrom, must commence a City Council approval process in accordance with Section 50-72(A)(3). If the City Council has not approved the continuing use of the Surveillance Technology, including the Surveillance Impact Report and Surveillance Use Policy submitted pursuant to Section 50-73(A), within one hundred eighty (180) days of their submission to the City Council, the municipal entity shall cease its use of the Surveillance Technology and the sharing of Surveillance Data therefrom until such time as City Council approval is obtained in accordance with this Ordinance.

(B) Body Worn Cameras shall be exempt from Section 50-74 of this Ordinance until January 1, 2028.

Section 50–75. - Lead Entity Identification

If more than one municipal entity will have access to the Surveillance Technology or Surveillance Data, a lead municipal entity shall be identified. The lead municipal entity shall be responsible for maintaining the Surveillance Technology and ensuring compliance with all related laws, regulations, and protocols.

Section 50–76. - Standard for Approval

The City Council shall only approve a request to fund, acquire, or use a Surveillance Technology if it determines the benefits of the Surveillance Technology outweigh its costs, that the proposal will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or group.

To assist the public in participating in such an analysis, all approved Surveillance Impacts Reports and Surveillance Use Policies shall be made available to the public, at a designated page on the relevant municipal entity's public website, and in hard-copy form for review and photocopying at City Hall and the Medford Public Library, for as long as the related Surveillance Technology remains in use. An approval for the funding, acquisition and/or use of a Surveillance Technology by the City Council, where the risk of potential adverse impacts on civil rights or civil liberties has been identified in the Surveillance Impact Report pursuant to Section 50-73(B)(5)(a), shall not be interpreted as an acquiescence to such impacts, but rather as an acknowledgement that a risk of such impacts exists and must be proactively avoided.

Section 50–77. - Annual Surveillance Report

(A) A municipal entity that obtains approval for the use of a Surveillance Technology must submit to the City Council and make available on its public website and in hard-copy form

at Medford City Hall and the Medford Public Library, an Annual Surveillance Report for each specific Surveillance Technology used by the municipal entity within twelve (12) months of City Council approval, and annually thereafter on or before March 15.

(B) Scope and Intentions: The Annual Surveillance Report is to provide a written report on an annual basis that contains a high-level and generalized summary of policies and usages concerning surveillance technology used by any city department during the previous year and containing the information set forth in Section 50-77 of this ordinance. This ordinance should not be interpreted as requiring disclosures of personally identifying information. If a municipal entity seeking surveillance technology or data use approval brings forth information in a request for approval that they feel would be detrimental to discuss in a public setting, the City Council may review that portion of their application in Executive Session. Further, nothing in this ordinance should be interpreted as:

- requiring disclosures that would violate the integrity of ongoing investigations, nor that would detail past, current or planned MPD investigations;
- requiring disclosures that would violate confidentiality in compliance with state and federal law and court orders, should they apply;
- requiring disclosures that would violate the Family Educational Rights and Privacy Act (FERPA) or other federal or state-level privacy protections;
- requiring disclosures that would in any way divulge or imperil sensitive information, i.e. information involving juveniles or medical records.

(C) The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:

1. 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;
2. Whether the Surveillance Technology has been effective at achieving its identified purpose;
3. Whether and how often collected Surveillance Data was shared with any external persons or entities, the name(s) of any recipient person or entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
4. The number of public records requests received by the City seeking documents concerning Surveillance Technology approved during the previous year;
5. A summary of complaints or concerns that were received about the Surveillance Technology;

6. 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;
7. 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;
8. 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
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.

(D) Within thirty (30) days of submitting and publicly releasing an Annual Surveillance Report pursuant to Section 50-77(A), the Subcommittee on Public Health & Community Safety, or the current most relevant subcommittee, shall hold one or more well-publicized and conveniently located community engagement meetings at which the general public is invited to discuss and ask questions regarding the Annual Surveillance Report and the municipal agency's use of surveillance technologies.

(E) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether the benefits to the impacted municipal agency or City department(s) and the community of the Surveillance Technology identified in response to Section 50-77(A), as used by the report-submitting entity, 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; and if deployment/usage otherwise meets the standard for approval set forth in Section 50-76. 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; (2) request a report back from the Mayor or municipal agency regarding steps taken to address the City Council's concerns; and/or (3) direct the use of the Surveillance Technology be discontinued.

Section 50–78. - Annual Public Reporting

Not later than April 15 of each year, the City Council or its appointed designee shall release an annual public report, in print and on its public website, containing the following information for the preceding calendar year:

- (A) The number of requests for approval submitted to the City Council under this Ordinance for the funding, acquisition, or new use of Surveillance Technology;
- (B) The number of times the City Council approved requests submitted under this Ordinance for the funding, acquisition, or new use of Surveillance Technology;
- (C) The number of times the City Council rejected requests submitted under this Ordinance for the funding, acquisition, or new use of Surveillance Technology;
- (D) The number of times the City Council requested modifications be made to Surveillance Impact Reports and Surveillance Use Policies before approving the funding, acquisition, or new use of Surveillance Technology; and
- (E) All Annual Surveillance Reports submitted pursuant to Section 50–77. Printed copies of the public report may contain pinpoint references to online locations where the Annual Surveillance Reports are located, in lieu of reprinting the full reports.

Section 50–79. - Enforcement; Remedies; Penalties; Whistleblower Protections.

- (A) Enforcement: This ordinance shall be enforced by the Mayor’s office or the Mayor’s designee.
- (B) 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 mandamus 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.
- (C) The City will address alleged violations of this ordinance in accordance with its usual practices, applicable law, and contractual obligations.
- (D) Municipal employees or agents, except in the event of exigent circumstances, or in response to a declared municipal, state, or federal state of emergency, shall not use any Surveillance Technology except in a manner consistent with policies approved pursuant to the terms of this Ordinance, and may in no circumstances utilize Surveillance Technology in a manner which is discriminatory, viewpoint-based, or violates the City Charter, the Massachusetts Constitution, or United States Constitution.
- (E) 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.

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

Section 50–80. - Certain Public-Private Contracts Prohibited


It shall be unlawful for the City to enter into any contract for monetary value with a commercial entity that provides the City with the mass acquisition of privately generated and owned bulk Surveillance Data. Any contracts or agreements signed prior to the enactment of this Ordinance that violate this section shall not be renewed after the completion of the term of said contracts or agreements. Section 50-80 shall not apply to any contract or agreement executed for law enforcement operations or purposes.

Section 50–81. - 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, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 50–82. - Effective Date

This Ordinance shall take effect immediately after its adoption.

APPROVED  MAYOR

IN COUNCIL

FEBRUARY 14, 2023

FIRST READING

ADVERTISED

MARCH 9, 2023

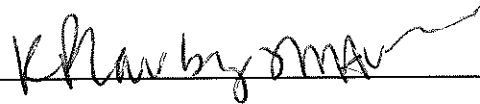
MEDFORD TRANSCRIPT

IN COUNCIL

MARCH 28, 2023

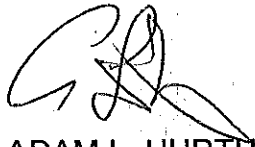
PASSED TO TAKE ITS THIRD
READING TO BE ORDAINED

APPROVED



CITY SOLICITOR

A TRUE COPY, ATTEST



ADAM L. HURTUBISE
CITY CLERK