CHAPTER 21 - POLICE

ARTICLE IV. LAW ENFORCEMENT SURVEILLANCE OVERSIGHT

Sec. 21-60. Purpose.

The purpose and intent of this Article is to formally adopt a process for public notification and review of new law enforcement Surveillance Technology before such technology is acquired or used, and to ensure that approved Surveillance Technology is used in accordance with policies that protect citizens' privacy, civil rights, and civil liberties. This process is not intended to discourage the adoption of Surveillance Technology that will make Columbia citizens more secure. Rather, this Article is intended to: (i) Establish safeguards, including transparency, oversight, approval, and accountability measures to protect civil rights and civil liberties before new Surveillance Technology is acquired or deployed by the police department; (ii) Ensure that a public hearing is held before any such new technology is acquired or used by the police department; (iii) Establish data reporting measures regarding the use and implementation of Surveillance Technology by the police department; (iv) Improve public confidence in law enforcement and new technology and equipment that is approved for use; and (v) provide mechanisms for continued oversight and annual evaluation.

Sec. 21-61. Definitions.

For the purposes of this Article, the following words, terms and phrases shall have these definitions:

1) "Annual Surveillance Report" means an annual written report concerning specific Surveillance Technology that is used by the police department.

   (a) The Annual Surveillance Report will include the following:

      (1) A general description of how the Surveillance Technology was used, including general locations and neighborhoods where Surveillance Technology was deployed;

      (2) A general description of how often data acquired through the use of the Surveillance Technology was shared with outside entities, the types of data shared with outside entities, and general justification for the sharing of such information;

      (3) A summary of complaints received about use of any type of Surveillance Technology;

      (4) The results of any internal audits required by any Technology Use Policy, including data regarding violations of the policy;

      (5) Information including crime statistics, where applicable, that help the City Council assess whether the Surveillance Technology has been effective at achieving its identified purposes;

      (6) Total costs, to the extent possible, including personnel, maintenance, and other ongoing costs, for the Surveillance Technology and anticipated funding needed for continued use of the technology;

      (7) Any requested modifications to a Technology Use Policy for any Surveillance Technology; and

      (8) Aggregate information concerning technology or tools exempted from public disclosure pursuant to Missouri Sunshine Law.

2) "Exigent Circumstances" The good faith belief of the Police Chief that there exists an emergency involving imminent danger of death, serious physical injury to any person, or imminent danger of significant property damage, that requires the use of the Surveillance Technology or the information it provides.

3) "Personal Communication Device" means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way

communications and/or portable Internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of conducting city business.

4) “Police Chief” means the Chief of Police, or designee.

5) "Surveillance Impact Report" means a written report for use of proposed Surveillance Technology, which at a minimum includes the following:

   (a) Information describing the technology and how it works;

   (b) Information on the proposed purpose(s) and use(s) for the technology; along with any existing independent evaluations demonstrating that the technology can help achieve that purpose;

   (c) If applicable, the general location(s) where the technology may be deployed and crime statistics for such location(s);

   (d) The known fiscal costs for the technology, including initial purchase, personnel and other known ongoing costs, and any current or potential sources of funding;

   (e) A description of any possible adverse impacts the use of the technology may have on civil rights and liberties, and 1) the safeguards that will be implemented to prevent these impacts; and 2) the potential uses of the technology that will be expressly prohibited.

   (f) A description of community engagement activities that have been undertaken in preparation of the report and proposed Technology Use Policy, including but not limited to groups representing communities of color, immigrants and others who may be impacted by technology; and

   (g) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.

6) "Surveillance Technology" means any device or system designed or used or intended to be used to collect, retain, process or share audio, electronic, visual, location, thermal, olfactory or similar information associated with, or capable of being associated with, any specific individual or group of specific individuals by the police department. Examples of surveillance technologies include, but are not limited to, the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors; facial recognition software; gait analysis software; surveillance enabled or capable light bulbs or light fixtures; social media monitoring software; video cameras that record audio or video and can transmit or be remotely accessed; software designed to integrate or analyze data from surveillance technology, including surveillance target tracking and predictive policing software based on surveillance. The enumeration of Surveillance Technology examples in this subsection shall not be interpreted as an endorsement or approval of their use by the police department.

   (a) "Surveillance Technology" does **not** include the following devices, hardware or software:

      (1) Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers, that are in widespread use by city departments and used for routine city business and transactions;

      (2) City databases and enterprise systems that contain information kept in the ordinary course of city business and do not contain any data or other information collected, capture, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including, but not limited to. human resource, permit, license, business records, payroll, accounting, or other fiscal databases;

      (3) Information technology security systems, including firewalls and other cybersecurity systems;

      (4) Physical access control systems, employee identification management systems, and other physical control systems;

      (5) Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

(6) Manually-operated technological devices used primarily for internal city and department communications and are not designed to surreptitiously collect surveillance data, such as radios, Personal Communication Devices and email systems;

(7) Manually-operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

(8) Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;

(9) Computers, software, hardware, security cameras or devices used in monitoring the work and work-related activities involving city buildings, employees, contractors and volunteers or used in conducting internal investigations involving city employees, contractors and volunteers;

(10) Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the ordinary course of providing city services;

(11) Parking Ticket Devices;

(12) Photo Enforcement Cameras, provided the cameras and the data collected therefrom are used and maintained solely to enforce traffic laws;

(13) Police department interview room, holding cell and police department internal security audio/video recording systems;

(14) Police department computer aided dispatch (CAD), records/case management, Live Scan, booking, Bureau of Motor Vehicles, Missouri Uniform Law Enforcement System, 9-1-1 and related dispatch and operation or emergency services systems, and any similar state or federal maintained criminal history record information or database.

(15) Technology or tools used to investigate specific criminal incidents where such technology or tools are not readily known to the public and for which the effectiveness of the technology or tool would be compromised by disclosure.

(16) Any technology that collects information exclusively on or regarding city employees or contractors.

(17) Technology or tools used by police officers solely while they are working as part of an established federal task force.

7) "Technology Use Policy" means a policy adopted by the Chief of Police and approved by the City Manager for use of a specific item or category of Surveillance Technology. Such policy shall be posted and available to the public on the city website for as long as the Surveillance Technology is in effect. The policy must, at a minimum, specify the following:

(a) Purpose: The specific purpose(s) that the Surveillance Technology item is intended to advance,

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to and associated with such use.

(c) Data Collection: The information that can be collected by the Surveillance Technology, including "open source" data.

(d) Data Access: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

(e) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on an information technology system of the city.

(f) Data Retention: The time period, if any, for which information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

(g) Location Notification: The provision of notice by the police department of the general location of fixed Surveillance Technology whenever fixed Surveillance Technology is deployed or moved. At a minimum the policy must provide for posting the notice on the city website and through social media within 72 hours of deploying the Surveillance Technology. Such notice will not be required to be provided if the Surveillance Technology is being used to investigate specific criminal incidents or the disclosure would otherwise impair a police investigation.

(h) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

(i) Third Party Data Sharing: If and how other city or non-city entities can access, use, or retain the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

(j) Training: The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology.

(k) Accountability: The mechanisms to ensure that the Technology Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person with oversight authority outside the police department, and the sanctions for violations of the policy. The policy shall provide for an audit of all technology used by the police department, which shall include technology or tools exempt from this Article and will restrict the use of information obtained from such exempt technology or tools.

Sec. 21-62. Council review of new technology.

(a) The City Council shall hold a public hearing to consider a request by the police department for any of the following activities:

(1) Acquiring new Surveillance Technology, including but not limited to procuring such technology without the exchange of monies or consideration;

(2) Using new Surveillance Technology or using existing Surveillance Technology for a purpose, scope, scale, or in a manner contrary to the Technology Use Policy for that technology or the Surveillance Impact Report; and

(3) Entering into an agreement with a non-city person or entity to share or otherwise use Surveillance Technology or the information or data it provides, including data sharing agreements.

(b) The police department seeking approval for acquisition of new Surveillance Technology under subsection 21-62(a)(1) shall submit a Surveillance Impact Report and a proposed Technology Use Policy for such technology at least fourteen (14) days prior to the public hearing required under subsection (a). The Surveillance Impact Report and proposed Technology Use Policy shall be posted on the city website along with the notice of public hearing. The notice of public hearing shall be published at least fourteen (14) days prior to the date of the scheduled public hearing and shall be posted on social media.

(c) Upon consideration of the Surveillance Impact Report, the proposed Technology Use Policy, and public comment received the City Council may approve any request by a majority vote.

(d) Notwithstanding any other provision in this Article, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence derived from Surveillance Technology to a law enforcement agency for the purposes of conducting a criminal investigation, nor require the city to violate the Missouri Sunshine Law.

Sec. 21-63. Compliance for existing surveillance technology.

Within 180 calendar days of the passage of the ordinance adopting this Article, the Chief of Police shall adopt a Technology Use Policy or policies covering existing Surveillance Technology, which is/are approved by the City Manager. Policies for existing technology shall be made publicly available on the city website. Any change to a policy for existing technology will be posted on the city website and provided to the City Council in the form of a report; provided, however, any Technology Use Policy change that creates a new purpose, scope, scale or surveillance manner contrary to the previous Technology Use Policy for that technology or the Surveillance Impact Report is subject to City Council review and approval after a public hearing as provided in Section 21-62 of this Article for new technology.

Existing Surveillance Technology shall be subject to the annual reporting requirements contained in this Article.

Sec. 21-64. Use of unapproved technology during exigent circumstances.

The Police Chief may authorize the temporary acquisition or temporary use of Surveillance Technology by the police department in exigent circumstances without following the provisions of this Article. If the police department acquires or uses surveillance technology pursuant to this Section, the police department shall:

(a) Use the Surveillance Technology to solely respond to the exigent circumstance;

(b) Cease using the surveillance technology within 30 days or when the exigent circumstance ends, whichever is sooner. Unless authorized under this Article for further use, all use must end when the exigent circumstances end;

(c) Only keep and maintain data related to the exigent circumstance and dispose of any data that is not relevant to an ongoing investigation;

(d) Within 30 days after the end of the exigent circumstances submit a report to the City Manager. The report must explain the exigent circumstances, why the technology or equipment was needed to address the exigent circumstances, how the exigent circumstances prevented the police department from following the approval process in this Article, and describe how the technology or equipment was used.

Sec. 21-65. Oversight following council approval.

Prior to March 15 of each year, the Police Chief shall present a written Annual Surveillance Report to the City Council covering activities for the prior calendar year. If the police department is unable to meet the deadline, the Police Chief shall notify the City Manager in writing and request an extension, including the reasons for that request. The City Manager may grant reasonable extensions to comply with this Section and shall notify the City Council of the extension.

Within five (5) business days of the submission of the Annual Surveillance Report, the report shall be made publicly available on the city website. At least 30 days, but no more than 60 days, after the posting of the report the City Council shall have on its agenda a presentation of the report. At such meeting citizens will be given an opportunity to comment on the report.-

Sec. 21-66. Prohibitions and penalties.

The City shall not enter into any contract or agreement that conflicts with the provisions of this Article.

Any city employee who knowingly violates this Article shall be subject to appropriate discipline pursuant to the procedures set forth in the City Employee Personnel Manual and a report shall be made to the City Manager.

Failure to comply with the provisions of this Article shall not be deemed to prevent the use of any evidence or data obtained from use of Surveillance Technology being utilized by law enforcement officials in the prosecution or defense of any criminal or civil litigation.