

DRAFT

1st & Second Reading

EMERGENCY MEASURE
1 Reading, 2 Separate Meetings _____
2 Readings at One Meeting ✓

12.

BY.....

NO. 31886-21.....

AN ORDINANCE

Enacting Sections 34.09 through 34.15 of the Revised Code of General Ordinances to Establish a Process to Approve and Regulate New Law Enforcement Surveillance Technology, and Declaring an Emergency.

WHEREAS, The City of Dayton is obligated to protect the public and promote the peace and welfare of its citizens; and

WHEREAS, The City of Dayton is committed to openness as a foundation for a better-informed citizenry, which leads to better government and better public policy; and

WHEREAS, The Commission recognizes that Surveillance Technology can be a valuable tool for law enforcement to more effectively and efficiently investigate and prevent crimes, and protect crime victims and society from those who commit crimes; and

WHEREAS, The Commission has determined it is in the best interest of the City of Dayton to require a public hearing before any new Surveillance Technology is acquired or used by the Dayton Police Department; and

WHEREAS, The Commission finds it is essential to have an informed public discussion about decisions related to Surveillance Technology and its potential impact on privacy, civil rights and civil liberties, including those rights guaranteed by the United States and Ohio Constitutions; and

WHEREAS, The Commission finds that safeguards, including transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before new Surveillance Technology is deployed by the City; and

WHEREAS, The Commission finds that an annual surveillance technology report should be provided by City staff to the Commission for the purpose of providing information on the use of such technologies to the public;

WHEREAS, To provide for the immediate preservation of the public peace, property, health and safety, it is necessary that this Ordinance take effect at the earliest possible date, now, therefore,

BE IT ORDAINED BY THE COMMISSION OF THE CITY OF DAYTON:

Section 1. That Sections 34.09 through 34.15 of the Revised Code of General Ordinances be enacted to read as follows:

§ 34.09 Purpose.

Sections 34.09 through 34.15 shall be known as the Law Enforcement Surveillance Oversight Ordinance and referred to herein as the “Oversight Ordinance.”

The purpose and intent of the Oversight Ordinance is to formally adopt a process for citizen notification and review of new law enforcement Surveillance Technology before such technology is acquired or used, and to ensure that approved 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 Dayton’s citizens more secure. Rather, this ordinance is intended to: 1) 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 Dayton Police Department; 2) Ensure that a public hearing is held before any such new technology is acquired or used by the Dayton Police Department; 3) Establish data reporting measures regarding the use and implementation of Surveillance Technology by the Dayton Police Department; 4) Improve public confidence in law enforcement and new technology and equipment that is approved for use; and 5) provide mechanisms for continued oversight and annual evaluation.

§ 34.10 Definitions.

For the purposes of Sections 34.09 through 34.14, 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 Dayton Police Department.
 - (a) The Annual Surveillance Report will include all of the following:
 - (1) A general description of how the Surveillance Technology was used, including general locations and neighborhoods where technology or equipment was deployed;
 - (2) A general description of whether and how often data acquired through the use of the Surveillance Technology was shared with outside entities, the type(s) of data and general justification for the disclosure(s);
 - (3) A summary of community complaints about the Surveillance Technology item;
 - (4) The results of any internal audits required by the Surveillance Use Policy and information about violations of the Use Policy;
 - (5) Information including crime statistics, where applicable, that help the Commission assess whether the Surveillance Technology has been effective at achieving its identified purposes;

(6) An analysis of any discriminatory or other adverse impacts the use of the surveillance technology may have had on the public's civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution and the Ohio Constitution; and

(7) Total costs, to the extent possible, including personnel, maintenance, and other ongoing costs, for the Surveillance Technology and anticipated funding for the technology as needed; and

(8) Any requested modifications to the Surveillance Technology Use Policy applicable to the item; and

(9) Aggregate information concerning technology or tools exempted pursuant to R.C.G.O. Section 34.10(5)(a)(15).

2) "*Exigent Circumstances*" The Chief of the Dayton Police Department or his or her designee's good faith belief 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) "*Surveillance Impact Report*" means a written report including at a minimum the following:

(a) Information describing the Surveillance Technology and how it works;

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

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

(d) The known fiscal costs for the Surveillance 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 Surveillance 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 Surveillance Technology that will be expressly prohibited.

(f) A description of community engagement activities that have been undertaken in preparation of the report and proposed use policy, including but not limited to the Neighborhood Presidents Forum and similar groups representing communities of color, immigrants and others who may be impacted by Surveillance Technology. Descriptions may include comments, input, or any formal action taken by the organizations; and

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

5) “*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 Dayton Police Department. Examples of surveillance technologies include but are not limited to: 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 Dayton 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 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, Ohio Law Enforcement Administrative Database, 9-1-1 and related dispatch and operation or emergency services systems.

(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 Dayton Police Officers solely while they are working as part of an established federal task force.

6) “*Surveillance Use Policy*” means a policy adopted by the City Manager for use of the Surveillance Technology. Such policy shall be posted and available to the public on the

City's website for as long as the policy 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) Whenever fixed Surveillance Technology is moved or deployed the Dayton Police Department shall provide notice of the location of the Surveillance Technology in accordance with its Policy. The Dayton Police Department will attempt to provide notice as soon as practicable, but at a minimum will require posting the notice on the City of Dayton's Website and providing email notice to those that request such notice from the Division of Public Affairs within 72 hours of deploying the Surveillance Technology. The Dayton Police Department will also provide notice through social media. Such notice will not 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) Auditing and Oversight: The mechanisms to ensure that the Surveillance 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 or entity with oversight authority, and the legally enforceable sanctions for violations of the Policy. The Policy will provide for an audit of all technology used by the Dayton Police Department, which shall include technology or tools exempt from this Ordinance and will restrict the use of information obtained from such exempt technology or tools.

§ 34.11 Commission Review and Decisions

(a) The Commission shall consider a request by Dayton Police Department made pursuant to this ordinance following a public hearing with proper notice and the opportunity for residents to submit written and verbal comments conducted at a regular Commission meeting, prior to any of the following:

(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 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 Dayton Police Department seeking approval under subsection 34.11(a)(1)-(3) shall submit to the Commission a Surveillance Impact Report and a proposed Surveillance Use Policy at least thirty (30) days prior to the public hearing required under subsection (a). Within twenty-four (24) hours of submission, notice of the public hearing, the Surveillance Impact Report and proposed Surveillance Use Policy shall be posted on the City's website with a notice that any written public comment must be filed with the Clerk of the Commission no later than seven (7) days prior to the scheduled public hearing. The Clerk of the Commission shall post the timely received public comments on the website. In addition, notice of the public hearing, the Surveillance Impact Report, and the proposed use policy shall be promptly emailed to all individuals that have filled out a request for notice of the Reports with the Division of Public Affairs and shall be posted to the City's social media channels.

(c) Prior to approving or rejecting any action described in subsection (a), the Commission may request that revisions be made by the City Manager or Dayton Police Department as appropriate.

(d) Upon consideration of the Surveillance Impact Report and any public comment, and consideration and reliance upon the proposed Use Policy, the Commission may approve any action described in subsection 34.11(a)(1)-(3) by a majority vote.

(e) Notwithstanding any other provision in this Oversight Ordinance, 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 Ohio Public Record Law.

§ 34.12 Compliance for Existing Surveillance Technology

Within one hundred and eighty (180) calendar days of the passage of this Oversight Ordinance, the City Manager shall adopt a Use Policy or policies covering existing Surveillance Technology. Use Policies for existing technology shall be made publicly available on the City's website. Such policy or policies will be submitted to and reviewed by the Commission. The Commission may recommend modifications of the use policy or policies to the City Manager. Any changes to the Policy will be posted on the City of Dayton Police Department's website, emailed to individuals that have requested email notification through the Division of Public Affairs, and provided to the City of Dayton Commission. Policy changes that create a new purpose, scope, scale or manner contrary to the previous use policy for that technology or the Surveillance Impact Report are subject to Commission review under §34.11(a)(2) of this ordinance.

Existing Surveillance Technology shall be subject to the annual reporting requirements under § 34.10(1)(a) and § 34.14.

§ 34.13 Use of Unapproved Technology During Exigent Circumstances

The Chief of Police or his/her designee may authorize the Dayton Police Department's temporary acquisition or temporary use of Surveillance Technology in exigent circumstances without following the provisions of this Oversight Ordinance before that acquisition or use. If the Dayton Police Department acquires or uses surveillance technology pursuant to this Section, the Dayton Police Department shall:

- (a) Use the Surveillance Technology to solely respond to the exigent circumstance;
- (b) Cease using the surveillance technology within thirty (30) days or when the exigent circumstance ends, whichever is sooner. 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 thirty (30) days after the end of the exigent circumstances submit a report to the City Manager to be shared with the Commissioners. 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 Department from following the approval process in this ordinance, and describe how the technology or equipment was used. This report shall be promptly posted on the City's website and shall be

promptly emailed to all individuals that have filled out a request for notice of the Reports within the Division of Public Affairs.

§ 34.14 Oversight Following Commission Approval

By the end of each fiscal year, the Dayton Police Department must present a written Annual Surveillance Report to the Commission. If the Dayton Police Department is unable to meet the deadline, the Chief of Police shall notify the Commission in writing and request an extension, including the reasons for that request. The Commission may grant reasonable extensions to comply with this Section.

Within five (5) business days of the submission of the annual report, the report shall be promptly emailed to all individuals that have completed a request for notice of the Reports with the Division of Public Affairs and the report shall be made publicly available on the City's website. At least thirty days after the posting of the report, the Commission shall have on its agenda a presentation of the report. At such meeting citizens will be given an opportunity to comment on the report. Citizens may also submit written comments pursuant to Commission meeting rules. After citizen comments the Commission need not take any action but may vote to cease the use of any particular Surveillance Technology or may propose modifications to the use policy for any of the Surveillance Technologies in the report.

§ 34.15 Prohibitions and Penalties

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

Any City employee who knowingly violates this Chapter 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 Commission.

Section 2. This Ordinance is not intended and shall not be interpreted to create a private right of action for damages or equitable relief on behalf of any person or entity against the City or any of its officers or employees.

Section 3. The provisions of this Sections 34.09 through 34.15 are declared to be separate and severable. The invalidity of any clause, phrase, sentence, paragraph, subdivision, section or portion of these Sections, or the invalidity of the application thereof to any person or circumstance shall not affect the validity of the remainder of these Sections, or the validity of its application to other persons or circumstances.

Section 4. That for the reasons set forth in the preamble hereof, the Dayton City Commission declares this Ordinance to be an emergency measure, which shall take effect immediately upon its passage.

PASSED BY THE COMMISSION....., 2021

SIGNED BY THE MAYOR....., 2021

Mayor of the City of Dayton, Ohio

ATTEST:

Clerk of the Commission

APPROVED AS TO FORM:

Jim Must

City Attorney