ORDINANCE NO. 2026-06-17-13

AN ORDINANCE OF THE CITY OF ROLLINGWOOD, TEXAS, CREATING ARTICLE III, SURVEILLANCE TECHNOLOGY, OF CHAPTER 14, LAW ENFORCEMENT, OF PART I, CODE OF ORDINANCES, OF THE CITY'S CODE OF ORDINANCES

WHEREAS, the City Council of the City of Rollingwood ("City Council") wishes to deter criminal activity within its jurisdiction, and aid in the investigation of criminal activity, through the deployment or use of surveillance technologies; and

WHEREAS, the City Council, recognizing that the use of surveillance technologies affects individual privacy and sense of personal wellbeing; and

WHEREAS, the City Council wishes to mitigate such privacy concerns through the adoption of regulations related to the deployment and use of surveillance technologies within the city limits of Rollingwood; and

WHEREAS, the City Council finds and determines that the regulations and reporting requirements provided for herein are in the best interests of public safety.

NOW THEREFORE BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF ROLLINGWOOD, TEXAS, THAT:

SECTION 1. All the above premises are hereby found to be true and correct legislative and factual findings of the City Council and are hereby approved and incorporated into the body of this Ordinance as if copied in their entirety.

SECTION 2. Article III, Surveillance Technology, of Chapter 14, Law Enforcement, of Part I, Code of Ordinances, of the City's Code of Ordinances is hereby created to read as follows:

ARTICLE III. – SURVEILLANCE TECHNOLOGY

DIVISION 1. – GENERALLY

Sec. 14-50. - Definitions

In this chapter:

Exigent Circumstances means a single or multiple related events, incidents, or circumstances creating or involving imminent risk of serious injury, loss of life, significant property damage, destruction of evidence in a criminal case, or damage to the public welfare, that require the immediate use of surveillance technology or the information it provides to mitigate the risk.

Privacy Impact Assessment means an assessment of the risks to civil liberties and privacy rights posed by a surveillance technology.

Sensitive Personal Information means information specifically associated with, or capable of being associated with, an individual, including:

(a) social security number, driver's license number, or government-issued identification number;

(b) financial data, including account numbers and credit card numbers;

(c) precise geolocation;

(d) religious beliefs, ethnic origin, or trade union membership;

(e) contents of emails and electronic text messages unless the City is the sender or an intended recipient;

(f) information about a person's sex life, sexual orientation, or gender identity; or

(g) any personal data collected from a known child, as "child" is defined in 16 C.F.R. § 312.2 (Definitions).

Surveillance Technology means any electronic device, system using an electronic device, software, or similar technology that is used, designed, or primarily intended to monitor, collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, neural, or similar information specifically associated with, or capable of being associated with, an individual or group, including sensitive personal information.

(a) Surveillance technology includes drones with cameras or monitoring capabilities, automated license plate readers, fixed or mobile surveillance cameras, cell-site simulators, international mobile subscriber identity trackers, global positioning system technology, radio frequency identification technology, biometric surveillance technology, facial recognition technology, and surveillance systems that aggregate or analyze data for the purpose of monitoring persons or locations in public spaces.

(b) Surveillance technology does not include:

(1) widely available and commonly used consumer electronics, including smartphones and digital recording devices that are used with the consent of those being recorded;

(2) physical access control systems, including badge/keycard access locks and systems, password-access technology, metal detectors, and motion sensors without biometric functionality;

(3) standard business software and hardware such as word processors, spreadsheets, computers, copy machines, and printers;

(4) information technology protection tools and software, including firewalls, data backup infrastructure, and antivirus software;

(5) medical equipment, devices, and systems used to diagnose, treat, or prevent disease or injury;

(6) City data repositories used in the ordinary course of City business, including case and records management systems, personnel records, systems for receiving and tracking customer service requests or complaints, information acquired voluntarily from an individual who was given an opportunity to decline to provide the information, that a City department requires to provide a City benefit or service, and where the information will not be shared by the City or used for any other purpose, City records that must be stored and kept pursuant to retention schedules or applicable law, and systems for searching and retrieving City data from City data repositories;

(7) Systems and devices specifically used to monitor the safety and security of City properties, vehicles, property and equipment, including which do not surveil the public at large. Examples include systems for geolocating City vehicles, property, and equipment. Examples of surveillance technologies not covered by this exception include surveillance cameras in City parks or on City streets.

(8) publicly available databases and internet search tools;

(9) non-digital observation tools used for direct observation without recording capabilities, including binoculars, telescopes, and night-vision goggles;

(10) widely used and commercially available communication and financial transaction systems, including standard telephone systems, standard voicemail systems, and equipment and systems used to process financial transactions;

(11) technologies used solely for forensic investigation and identification or verification of lawfully collected evidence in connection with a criminal incident and which do not surveil the public at large. Examples include forensic laboratory and field equipment, criminal justice databases used exclusively for booking, criminal history record management, or post-incident forensic identification (e.g., fingerprint, DNA, or ballistics), evidence management systems, and advanced 3D scanning technologies for static post-incident crime scene documentation;

(12) interview room security and recording systems;

(13) court-ordered monitoring, recording, or tracking systems; and

(14) systems, devices, and cameras used for infrastructure and mechanical control, including cameras for traffic control and traffic signal timing that do not retain footage.

Surveillance Use Policy means a written policy that governs the use of certain surveillance technologies by City departments.

Sec. 14-51 - Purpose

The purpose of this chapter is to govern the adoption, acquisition, deployment, use, and review of surveillance technology by City departments, with the goal of increasing transparency, promoting community participation, protecting civil liberties, and ensuring the responsible use of surveillance technology.

DIVISION 2. – REGULATION OF SURVEILLANCE TECHNOLOGY.

Sec. 14-52. - Council approval required.

Except as otherwise permitted in this chapter, City departments must obtain approval of the city council before:

(a) accepting funds for surveillance technology outside of the annual budget process, including private, state, or federal grants, or donations;

(b) acquiring new surveillance technology;

(c) using new or existing surveillance technology, or the information it collects, for a purpose or in a manner not previously approved by the city council or otherwise required by law; or

(d) entering into an agreement with a third-party entity outside of the City to acquire, share, or use surveillance technology or the information it provides.

Sec. 14-53. - Privacy impact assessment.

(a) A City department must prepare a privacy impact assessment for each surveillance technology the City department seeks to acquire or use in a manner not previously approved by the city council.

(b) A privacy impact assessment must be prepared and developed in consultation with the chief information security officer and the city attorney, or their respective designees.

(c) A privacy impact assessment must determine whether the surveillance technology poses more than a minimal risk to civil liberties and privacy rights, and must include at a minimum an analysis of whether the surveillance technology:

(1) allows the indiscriminate collection of data without a warrant, probable cause, or reasonable suspicion of criminal activity, or a criminal nexus where the data is capable of being associated with individuals or groups engaged in legal behavior;

(2) routinely transmits sensitive personal information through data networks subject to legal or illegal access by third parties, other than networks that are completely internal to the City;

(3) can store sensitive personal information in a manner allowing for broad or unrestricted sharing of or access to the information with or by third parties outside of the criminal justice system;

(4) can collect sensitive personal information without a warrant, probable cause, or reasonable suspicion of criminal activity or a criminal nexus, or where the technology allows for the creation of data records associated with particular individuals or groups;

(5) collects data in such a manner that it can be used by third parties to develop or expand products, services, or technology, including training of artificial intelligence, other than for the exclusive use by and ownership of the City;

(6) can be directly controlled or accessed, or its data can be directly controlled or accessed, by third parties outside of the criminal justice system;

(7) collects data in such a manner that even if anonymized or compiled, the data can be analyzed or reverse engineered to associate it with individuals or groups;

(8) collects data in a manner that is disproportionately associated with a particular demographic, protected class, or the exercise of a constitutionally or statutorily protected right;

(9) can collect sensitive personal information of individuals on their own private property; and

(10) is known to be associated with frequent violations of law, policies, or guidelines in other jurisdictions, the private sector, or previously by the City.

(d) The presence of any one or more of the factors in Subsection (c) shall weigh strongly against a determination that the surveillance technology presents no or minimal risk to civil liberties and privacy rights.

(e) The privacy impact assessment shall also analyze whether the benefits of the technology can be achieved through an alternative means that pose a lower risk to civil liberties and/or have a lesser financial cost.

(f) A City department must submit a privacy impact assessment to the city council before the city council meeting at which the City department will seek council approval pursuant to Section 14-52 or at which the City department will seek approval of the privacy impact assessment under Section 14-57.

(g) A City department must post the privacy impact assessment on a publicly available City website. The city administrator or designee may create a website for the purpose of hosting privacy impact assessments.

Sec. 14-54. - Surveillance use policy.

(a) The city administrator or designee must submit a proposed surveillance use policy to the city council for each surveillance technology that requires council approval under Section 14-52.

(b) A surveillance use policy must be prepared and developed in consultation with the City department seeking approval of the surveillance technology.

(c) A surveillance use policy must contain, at a minimum, the following:

(1) the specific purposes for the surveillance technology;

(2) a description of the surveillance technology and how it works;

(3) provisions related to authorized and unauthorized use of the surveillance technology and data obtained with the surveillance technology, including:

a. An exclusive list of the authorized uses;

b. The rules and processes required before using the technology and the data obtained with the surveillance technology;

c. If applicable, the general location, or types of locations, where the technology may be deployed, unless revealing the locations would compromise criminal investigations; and

d. A description of the machine learning and/or artificial intelligence capabilities and features of the surveillance technology, whether use of the surveillance technology will provide data for any machine learning and/or artificial intelligence tools, and any guidelines or prohibitions relating to machine learning algorithms and/or artificial intelligence;

(4) the information and data elements that the surveillance technology collects, including metadata;

(5) the individuals and entities, including any City department, vendor, subcontractor, service provider, or other third party, who can access or use the collected information, and the rules and processes governing access or use, including whether data will be used by or integrated with artificial intelligence or machine learning algorithms;

(6) safeguards that protect information from unauthorized access, including:

a. Encryption;

b. Access control;

c. Anonymization of data;

d. Differential privacy techniques;

e. Prohibitions on attempting, directly or indirectly, to re-identify any person from anonymized or de-identified data; and

f. Access oversight mechanisms;

(7) the time period for which information collected by the surveillance technology will routinely be retained, the reason why the retention period is necessary to achieve the purposes of the technology, the process by which the information is regularly deleted after that period lapses, and the conditions that must be met to retain information beyond that period;

(8) if and how collected information can be accessed by members of the public;

(9) if and how non-City entities can access, disclose, or use the information, including:

a. Any required justification and legal standards and requirements to access, disclose, or use the information;

b. Any limitations on non-City entities' ability to disclose data, including to third-party service providers; and

c. Any obligations imposed on, or agreements required by, the recipient of the information;

(10) the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are or will be any training materials; and

(11) the mechanisms to ensure that the surveillance use policy is followed, including, as applicable, a description of:

a. Personnel responsible for oversight;

b. Internal and external recordkeeping of use or access to the technology or the information collected, including detailed logging of data accessing events;

c. Technical measures to monitor for misuse;

d. Any audit requirements, including whether vendors or other relevant third parties will be required to provide City representatives or independent auditors hired by the City the ability to access any records needed to ensure compliance with the surveillance use policy;

e. Any independent person or entity, inside or outside of the City, with oversight authority; and

f. Sanctions for violations of the surveillance use policy.

(d) The city attorney or designee must review each surveillance use policy before it is submitted to the city council for approval.

(e) The city administrator or designee must submit a surveillance use policy to the city council no less than two weeks before the city council meeting at which the City department will seek council approval pursuant to Section 14-52.

(f) The city administrator or designee must post the surveillance use policy on a publicly available City website. The city administrator or designee may create a website for the purpose of hosting surveillance use policies.

Sec. 14-55. - Contracts for surveillance use technologies.

(a) The city administartor or designee must ensure that a City contract with a third party for acquisition or use of a surveillance technology must incorporate all applicable and relevant provisions of the council-approved surveillance use policy for that surveillance technology.

(b) To the extent permitted by law, the responsible City department must submit proposed contracts for acquisition or use of a surveillance technology to the city council before the meeting at which the City department will seek council approval of the contract.

(c) The city administrator must ensure that each City contract with a third party for acquisition or use of a surveillance technology includes one or more provisions that provide for penalties or, including monetary damages, specific performance, and early termination, if the third party breaches contractual provisions incorporating the applicable surveillance use policy.

Sec. 14-56. - Exception: exigent circumstances.

(a) Council approval under Section 14-52 and Section 14-54 is not required if the city administrator or designee determines that exigent circumstances exist which require the immediate temporary acquisition or use of a surveillance technology to mitigate or address the exigent circumstances, provided that:

(1) the city administrator or designee provides written authorization for the temporary acquisition or use of the surveillance technology due to exigent circumstances;

(2) within thirty-one (31) days of the use or acquisition of the surveillance technology, whichever comes first, the city administrator or designee reports and discloses to city council:

a. The written authorization;

b. The exigent circumstances that justified immediate acquisition or use of the surveillance technology, and the specific facts on which that determination was based;

c. A general description of the data collected; and

d. As applicable, the identities of any third parties with whom the data were shared;

(3) the responsible City department ceases the use of the surveillance technology when the exigent circumstances end.

(b) The city administrator or designee may extend the use of a surveillance technology under this section for a definite period beyond 120 days if the chief of police or designee certifies in writing to the city council that disclosing the acquisition or use of the surveillance technology within 120 days would compromise the safety or integrity of an active criminal investigation. Such certification must:

(1) specify the duration of the extension beyond 120 days;

(2) be disclosed in a city administrator's monthly report to the city council following the conclusion of the exigent circumstances;

(3) provide that the extension will not continue beyond the minimum time needed to ensure the safety and integrity of an active criminal investigation; and

(4) affirm that the extension is not for a purpose or an investigation unrelated to the exigent circumstances that justified the initial exception.

(c) This section shall not permit the acquisition or use of a surveillance technology for mere convenience to meet standard public safety policies or goals, including general crime reduction, traffic safety, or routine law enforcement activities.

(d) The city council must approve any continued use of the surveillance technology, as required by Sections 14-52 through 14-55, after the exigent circumstances end.

Sec. 14-57. - Exception: minimal or no risk to civil liberties and privacy rights.

Council approval under Section 14-52 is not required for a surveillance technology if the city council approves a privacy impact assessment for the surveillance technology and that privacy impact assessment determines that there is minimal or no risk to civil liberties and privacy rights posed by the surveillance technology.

Sec. 14-58. - Prohibited technologies.

The following surveillance technologies or data uses are not permitted:

(a) facial recognition technology, except as consistent with City policy, or with any state or federal requirements;

(b) artificial intelligence or machine learning tools, except as consistent with City policy; and

(c) collection of data by any vendor or third party for marketing purposes, product development purposes, or any other use that is not necessary to fulfill the terms of a contract but is instead related to the vendor's or other third party's own interests.

DIVISION 3. - ANNUAL REPORTING AND COMPLIANCE.

Sec. 14-59. - Annual reporting.

(a) The city administrator or designee must submit and present an annual surveillance report to the city council at a public meeting within 120 days after the end of each fiscal year. The annual surveillance report must be made available to the public prior to the public meeting.

(b) The annual surveillance report must list each surveillance use policy the city council approved in the prior fiscal year.

(c) For each surveillance technology approved in the prior fiscal year, the annual surveillance report must describe the surveillance technology and its intended use(s), and must include, at a minimum, the following information for the prior fiscal year:

(1) a summary of material non-compliance issues, including violations of surveillance use policies that impacted privacy, civil liberties, or civil rights, and any action taken to address the issues;

(2) a summary of whether and, if so, how often data acquired through the use of the surveillance technology was shared with outside entities (other than routine sharing through the criminal justice system), the name of any recipient entity, how often the data was shared, the type(s) of data disclosed, and the justification for the disclosure;

(3) a summary of whether and how the surveillance technology was used, including whether it captured information regarding members of the public who were not suspected of engaging in unlawful conduct;

(4) the results of any non-privileged internal audits, City department self assessments, or assessments conducted by the city administrator or designee;

(5) total annual costs for the surveillance technology, including personnel and ongoing support and maintenance; and

(6) an assessment of whether the surveillance technology has been effective at achieving its identified purpose and any obstacles identified to achieving that purpose.

(d) The annual surveillance report shall also include a list of all instances in which the exigent circumstances exception under Section 14-56 was utilized, including a summary of the technology used, the reasons for the exception being employed, and the length of time that the technology was in use without council approval of a surveillance use policy; and

(e) The annual surveillance report shall identify any third-party entities who are not employed or retained by the city that contributed to the report and the information they contributed.

Sec. 14-60. - Compliance required.

(a) As applicable, City employees must comply with this chapter, including with any surveillance use policy adopted by the city council. Violations of this chapter by City employees may be considered a violation of applicable personnel policies.

(b) Allegations of misconduct, including allegations that a City employee has violated a surveillance use policy, may be reported to the city administrator, the department director for the employee accused of misconduct, the city attorney, or any member of the city council.

(c) Allegations of misconduct, including allegations that a City employee has violated a surveillance use policy, shall be handled and investigated in the same manner as other violations of applicable personnel policies.

Sec. 14-61. - Retaliation prohibited.

(a) Retaliation against any City employee who makes a good faith complaint of a violation of this chapter, including a violation of a surveillance use policy, is prohibited and shall be considered a violation of applicable personnel policies.

(b) Allegations of retaliation shall be handled and investigated in the same manner as other violations of applicable personnel policies.

SECTION 3. For existing surveillance technology acquired, adopted, deployed, or in use by any City department prior to the effective date of this ordinance, the city administrator or designee shall determine, after consultation with the mayor and the city attorney, or their designees, whether the surveillance technology implicates civil liberties or privacy rights based on the criteria in City Code Section 14-53.

(A) If such existing surveillance technology is determined to implicate civil liberties or privacy rights, each responsible City department must develop a surveillance use policy and obtain the approval of the city administrator or designee of the surveillance use policy within 270 days of the effective date of this ordinance.

(B) Except in exigent circumstances, if a responsible City department does not obtain city administrator or designee approval of a surveillance use policy within those 270 days, the department must suspend the use of such existing surveillance technology until the surveillance use policy is approved by the city manager or designee.

(C) The city administrator or designee shall not approve any proposed surveillance use policy not in compliance with applicable City Code and policies, including provisions enacted in this ordinance and other technology policies, including those concerning artificial intelligence and data security.

(D) Any surveillance use policy approved by the city administrator or designee under this Section 3 of the ordinance shall be made publicly available and included in the next annual surveillance report required under Section 14-53.

SECTION 4. All provisions of the ordinances of the City of Rollingwood in conflict with the provisions of this ordinance are hereby repealed to the extent of such conflict, and all other provisions of the ordinances of the City of Rollingwood not in conflict with the provisions of this ordinance shall remain in full force and effect.

SECTION 5. Should any sentence, paragraph, clause, phrase or section of this ordinance be adjudged or held to be unconstitutional, illegal or invalid, the same shall not affect the validity of this ordinance as a whole, or any part or provision thereof other than the part so decided to be invalid, illegal or unconstitutional, and shall not affect the validity of the Code of Ordinances as a whole.

SECTION 6. This ordinance shall take effect immediately from and after its passage.

APPROVED, PASSED AND ADOPTED by the City Council of the City of Rollingwood, Texas, on the 17th day of June, 2026.

APPROVED:

_____
Gavin Massingill, Mayor

ATTEST:

_____
Alun Thomas, City Administrator