



Submitted by: Assembly Member McCormick  
Assembly Vice Chair Volland  
Assembly Member Scout  
Prepared by: Assembly Legal Services  
For reading: August 18, 2026

**ANCHORAGE, ALASKA**  
**AO No. 2026-108**

1 **AN ORDINANCE OF THE ANCHORAGE MUNICIPAL ASSEMBLY REPEALING**  
2 **AND REPLACING ANCHORAGE MUNICIPAL CODE CHAPTER 3.102 AND**  
3 **AMENDING AMC SECTION 7.15.040 TO CLARIFY EXISTING RESTRICTIONS**  
4 **ON SURVEILLANCE TECHNOLOGY AND ESTABLISH NEW RESTRICTIONS**  
5 **ON AUTOMATED LICENSE PLATE READER SYSTEMS, REAL-TIME CRIME**  
6 **CENTER OPERATIONS, AND LIVE CAMERA MONITORING, TO LIMIT THE**  
7 **RETENTION OF SURVEILLANCE DATA, TO PROHIBIT PARTICIPATION IN**  
8 **EXTERNAL SURVEILLANCE DATA NETWORKS, TO REQUIRE ASSEMBLY**  
9 **APPROVAL FOR THE ACQUISITION OF SURVEILLANCE TECHNOLOGY, AND**  
10 **TO PROVIDE FOR AUDIT AND ENFORCEMENT.**

11  
12  
13 **WHEREAS**, Article I, Section 22 of the Constitution of the State of Alaska provides  
14 that "the right of the people to privacy is recognized and shall not be infringed," and  
15 the Alaska Supreme Court has held in *State v. Glass*,<sup>1</sup> that the scope of that  
16 guarantee is not determined by federal Fourth Amendment doctrine; and

17  
18 **WHEREAS**, in *State v. McKelvey*,<sup>2</sup> the Alaska Supreme Court held that law  
19 enforcement must obtain a warrant before conducting technologically enhanced  
20 aerial surveillance of private property, and rejected the argument that the  
21 commonality of aircraft overflight in Alaska diminishes the reasonable expectation  
22 of privacy; and

23  
24 **WHEREAS**, on June 29, 2026, the Supreme Court of the United States held in  
25 *Chatrie v. United States*<sup>3</sup> that an individual retains a reasonable expectation of  
26 privacy in records of that individual's location, even when those records are held by  
27 a third party and even when the period of collection is limited; and

28  
29 **WHEREAS**, the Anchorage Assembly has previously legislated the Municipality's  
30 use of surveillance technologies in Anchorage Municipal Code chapter 3.102,  
31 establishing restrictions on unmanned aircraft systems, restrictions on facial  
32 recognition technology, standards governing body-worn cameras, and an annual  
33 reporting requirement; and

34  
35 **WHEREAS**, on September 23, 2025, the Assembly approved a five-year contract  
36 with Axon Enterprise, Inc., in the approximate amount of \$11,800,000, providing the  
37 Anchorage Police Department with a Real-Time Crime Center designed to receive  
38 up to 750 camera feeds, automated license plate readers, unmanned aircraft

<sup>1</sup> 583 P.2d 872 (Alaska 1978).

<sup>2</sup> 544 P.3d 632 (Alaska 2024).

<sup>3</sup> 146 S.Ct. 2193 (2026).

capable of remote deployment, and technology for the detection of unmanned aircraft and their operators;<sup>4</sup> and

**WHEREAS**, the Assembly approved that contract without corresponding amendment to Anchorage Municipal Code chapter 3.102, with the result that the operation of these technologies is presently governed only by departmental policy which by its own terms does not apply in any criminal or civil proceeding and for which violations form the basis only of departmental administrative sanctions; and

**WHEREAS**, materials presented to the Assembly in connection with that contract identified automated license plate readers, unmanned aircraft detection technology, and two additional unspecified tools as being provided at no additional cost, demonstrating that surveillance capability may be acquired by the Municipality without additional independent procurement review nor require Assembly deliberation and approval directed to that capability; and

**WHEREAS**, in preparing for deployment of the new technology, the Chief of Police adopted three Policy and Procedures effective February 20, 2026 governing the use and operations of the Real Time Crime Center (Policy Number 7.08), Drone as First Responder (Policy Number 7.10), and Automated License Plate Readers (Policy Number 7.11)<sup>5</sup>; and

**WHEREAS**, a real-time crime center serves a legitimate and valuable public safety function when it provides responding officers with immediate situational awareness, and that function is distinct from, and does not require, the retention of a searchable historical record of the movements of persons who are not suspected of any offense; and

**WHEREAS**, restrictions on recording and retention alone do not prevent continuous human viewing, virtual patrol, remote camera control, or camera-to-camera tracking, and meaningful protection of privacy therefore requires incident-based limits, technical access controls, audit logs, and enforceable limits on live monitoring; and

**WHEREAS**, residents and businesses that voluntarily choose to share a camera feed with the Municipality serve the public interest, and the Assembly intends to preserve that voluntary program while ensuring that the Municipality does not convert it into a means of continuous observation of the public; and

**WHEREAS**, in jurisdictions throughout the United States, automated license plate reader data collected by municipal agencies has been queried by out-of-state and federal agencies without local authorization, has been used to identify persons attending lawful political demonstrations, and has been used to investigate conduct that is lawful in the jurisdiction where the data was collected; and

**WHEREAS**, in each such instance the harm resulted from retrospective queries of retained data rather than from real-time alerts, and in several such jurisdictions the governing agency had adopted a written policy prohibiting the conduct that

---

<sup>4</sup> Assembly Resolution No. 2025-283(S); *see also* Assembly Information Memorandum No. 185-2025.

<sup>5</sup> Available at <https://public.powerdms.com/ANCHOR/tree/documents/4076478>

nonetheless occurred, demonstrating that an administrative policy alone, absent independent audit and enforceable limits, is insufficient to protect the constitutionally protected privacy rights of residents; and

**WHEREAS**, the Anchorage Assembly finds that the acquisition of new or additional surveillance capability should be preceded by public deliberation, that surveillance data collected from persons not suspected of an offense should not be retained beyond the period necessary for real-time public safety operations, and that limits on the use of surveillance technology should be established in Code rather than in administrative policy subject to unilateral revision; now, therefore,

## **THE ANCHORAGE ASSEMBLY ORDAINS:**

**Section 1.** Anchorage Municipal Code chapter 3.102 is hereby repealed in its entirety and replaced with the following: *(requiring no legislative formatting)*

### **CHAPTER 3.102 MUNICIPAL USE OF SURVEILLANCE TECHNOLOGIES**

#### **Sections**

|           |                                            |
|-----------|--------------------------------------------|
| 3.102.010 | Definitions.                               |
| 3.102.020 | General Provisions                         |
| 3.102.030 | Data collection, protection, and retention |
| 3.102.040 | Annual surveillance technologies report.   |
| 3.102.050 | Audit and enforcement.                     |
| 3.102.060 | Automated license plate reader systems.    |
| 3.102.070 | Body-worn cameras.                         |
| 3.102.080 | Facial recognition technology.             |
| 3.102.090 | Unmanned aircraft systems.                 |
| 3.102.100 | Real-time crime center operations.         |

#### **3.102.010 Definitions.**

*Automated license plate reader (ALPR) system* means any system, device, software, algorithm, or combination thereof, whether fixed, mobile, semi-stationary, aerial, or handheld, that captures images of vehicles or vehicle license plates and converts, analyzes, classifies, or processes those images into machine-readable or searchable data. The term includes any system that identifies, classifies, or enables the search of vehicles by characteristics other than license plate number.

*Body-worn camera system* means a body-worn audio/video recording system primarily consisting of a camera and an internal battery pack.

*Captured plate data* means any data captured by, derived from, or inferred from an ALPR system, including license plate number, photographic images, geographic coordinates, date and time of capture, the identity of the capturing device, and any vehicle characteristic data including but not limited to make, model, body type, color, markings, decals, stickers, damage, modifications, cargo, or attached equipment.

1        *Cell-site simulator* means any device that functions as or simulates a base  
2 station for commercial mobile services or private mobile services in order to  
3 identify, locate, or intercept transmissions from cellular devices for purposes  
4 other than providing ordinary commercial mobile services or private mobile  
5 services.

6  
7        *Digital multimedia evidence (DME)* means all digital recordings, including  
8 but not limited to audio, video, photographs, and their associated metadata.  
9 Metadata includes any digital identifiers that are captured as part of the actual  
10 recording, such as date/time, GPS coordinates, labeling, and similar  
11 information.

12  
13        *External surveillance data network* means any database, platform,  
14 network, consortium, or data-sharing arrangement, whether operated by a  
15 private vendor, a governmental entity, or any combination thereof, through  
16 which surveillance data collected by or on behalf of a jurisdiction other than  
17 the municipality is made available to the municipality for query, or through  
18 which surveillance data collected by or on behalf of the municipality is made  
19 available to a jurisdiction other than the municipality. The term does not  
20 include a specific, case-related exchange of records between law  
21 enforcement agencies conducted in accordance with this chapter.

22  
23        *Facial recognition* means an automated or semi-automated process that  
24 assists in identifying or verifying an individual, or capturing information about  
25 an individual, based upon analysis of the individual's face.

26  
27        *Facial recognition technology* means any computer software or application  
28 that performs facial recognition.

29  
30        *Hot list* means a list of specific license plates or specific vehicles that a law  
31 enforcement agency has determined are relevant and material to a specific,  
32 documented, and ongoing criminal investigation or missing-persons  
33 investigation, and that is maintained so as to remain accurate, current, and  
34 complete.

35  
36        *Integrated camera feed* means a video or audio feed from a camera not  
37 owned by the municipality that is made available to the municipality on a  
38 continuous or on-demand basis with the consent of the owner.

39  
40        *Live monitoring session* means any intentional viewing, observation,  
41 selection, switching among, or control of one or more live camera feeds  
42 through a real-time crime center or other municipal system by a municipal  
43 employee. The term includes use of pan, tilt, or zoom controls; map-based  
44 camera selection; camera-to-camera following; and automated presentation  
45 of a live feed. The term does not include a system health check that does not  
46 display images or audio of identifiable persons or vehicles.

47  
48        *Real-time* describes the operation or execution of an action or process, by  
49 either human or technological means, contemporaneous with an identified  
50 event.  
51

1        *Real-time crime center* means any centralized municipal element,  
2 platform, or system that aggregates live or recorded video, audio, location,  
3 sensor, or dispatch data from multiple sources for the purpose of providing  
4 operational information to public safety personnel.

5  
6        *Registered camera* means a camera not owned by the municipality whose  
7 location and owner contact information have been provided to the  
8 municipality by the owner, and to which the municipality has no direct access.

9  
10        *Surveillance* or *surveil* means to observe or analyze the movements,  
11 behavior, data, or actions of individuals. Individuals include those whose  
12 identity can be determined through use of information maintained by the  
13 Department of Motor Vehicles either independently or when combined with  
14 any other record.

15  
16        *Surveillance data* means any data collected, generated, or derived by  
17 surveillance technology, including captured plate data, video, audio, location  
18 data, sensor data, and associated metadata.

19  
20        *Surveillance technology* means any software, electronic device, or system  
21 used, designed, or primarily intended to collect, retain, analyze, process, or  
22 share audio, electronic, visual, location, thermal, olfactory, biometric, or  
23 similar information specifically associated with, or capable of being  
24 associated with, any individual, vehicle, or group. Surveillance technology  
25 does not include:

- 26  
27            1.        Operational IT systems not used for surveillance;  
28  
29            2.        Evidence-processing tools used only for case-specific  
30 investigations; or  
31  
32            3.        Infrastructure-monitoring systems with strict retention limits.

33  
34        *Unmanned aircraft (UA)* means an aircraft that is intended to navigate in  
35 the air without an onboard pilot. Also alternatively called a remotely piloted  
36 aircraft (RPA), remotely operated vehicle (ROV), or drone.

37  
38        *Unmanned aircraft system (UAS)* means a system that includes the  
39 necessary equipment, network, and personnel to control an unmanned  
40 aircraft.

41  
42        (AO No. 2018-5, § 1, 2-13-2018; AO No. 2023-35(S-1), § 1, 4-18-2023)

### 43        **3.102.020    General provisions.**

44  
45  
46        A.        *Prohibited uses.* In order to protect the constitutional right to privacy  
47 of persons in the Municipality of Anchorage, and to ensure their safety,  
48 no municipal agency shall possess or use surveillance technology or  
49 data derived therefrom except as provided in this chapter.

- 50  
51            1.        No surveillance technology or surveillance data shall be used

to monitor, track, or identify persons based upon their actual or perceived participation in activity protected by the First Amendment to the Constitution of the United States or Article I, Sections 5 or 6 of the Constitution of the State of Alaska, or based solely upon race, ethnicity, national origin, immigration status, religion, sex, sexual orientation, gender identity, disability, or age. This subsection does not prevent response to a specific and credible threat to public safety, or the provision of public safety services requested by an event organizer.

2. *External surveillance data networks.* No municipal agency shall join, subscribe to, participate in, contribute surveillance data to, query, receive surveillance data from, or enable interoperability with any external surveillance data network.

3. *Purchase of data.* No municipal agency shall purchase, lease, subscribe to, or otherwise obtain captured plate data or historical location data from any private vendor, data broker, or commercial database, except pursuant to a warrant issued upon probable cause.

B. *Authorized uses.* The following surveillance technologies are approved for use by agencies of the municipality, subject to the limitations of this chapter and any other provisions of code:

1. Automated license plate readers
2. Body cameras
3. Facial recognition technology
4. Privately owned registered cameras
5. Unmanned aircraft systems

C. *Acquisition of surveillance technology.*

1. *Assembly approval required.* No municipal agency shall acquire or otherwise obtain or use any surveillance technology, or materially expand the deployment capability of any surveillance technology already in use, without prior approval of the assembly. This prohibition shall apply to any free trial, demonstration, beta test, or other temporary acquisition, as well as to any amendment, renewal, extension, or other change to an existing contract, regardless of whether the underlying contract was previously approved by the assembly, and regardless of dollar value.

a. Any municipal agency that requests an exception to the restrictions of this section shall include in its request to the assembly a written surveillance impact report, made available to the public not fewer than fourteen days before the public hearing, containing:

i. A description of the technology and each of its

- capabilities, including any capability the agency does not intend to use;
- ii. The categories of data collected, generated, retained, or accessed;
- iii. The proposed retention period for each category and the technical mechanism by which deletion will occur;
- iv. Each category of person authorized to access the data and the access controls applied;
- v. Every entity with which data will or may be shared, the legal basis for each such sharing, and whether the technology is capable of connecting to any external surveillance data network;
- vi. Total fiscal impact including acquisition, subscription, storage, personnel, training, and maintenance costs, projected for the full contract term and for five years, and the funding source;
- vii. An assessment of the effect upon privacy rights under Article I, Sections 14 and 22 of the Constitution of the State of Alaska;
- viii. Available evidence regarding effectiveness, including peer-reviewed research and published outcome data from comparable jurisdictions;
- ix. Whether any comparable jurisdiction has terminated, suspended, or declined to renew use of the same technology or the same vendor within the preceding three years, and the stated reasons; and
- x. For technology capable of live monitoring, the proposed authorized uses, maximum session duration, geographic limits, supervisory approval requirements, audio and remote-control capabilities, cross-camera tracking capability, and the technical mechanisms that will enforce access, logging, and automatic termination requirements.
- b. The assembly may approve the proposed acquisition by resolution after a public hearing, with or without revisions and conditions, for a period of no longer than 90 days, if it finds that the exception is consistent with the stated goals of preventing discrimination and promoting

privacy, transparency, and the public trust.

c. Upon conclusion of the period of temporary approval, the agency shall submit a report of its uses of the technology or information to the assembly. The agency may at that time or subsequently request the extension of the approval for another 90 days or that the assembly make the exception a permanent authorized use by ordinance adding it under subsection A.

d. A agency that has obtained a permanent authorization shall submit an annual summary of its uses of the technology or information as part of the Annual Surveillance Report to the assembly. This summary shall not include personally identifiable information.

2. *Bundled and unused capability.* Where surveillance technology is acquired that includes a capability the acquiring agency does not intend to use, the agency shall disclose that capability to the assembly at the time of the request, disable that capability by technical configuration where technically possible, and certify the Annual Surveillance Report that the capability remains unused and, where applicable, disabled. A municipal agency that intends to activate and use such disabled capability shall first obtain assembly approval in accordance with this subsection.

D. *Vendor-initiated changes.* No municipal agency shall enable, activate, or permit to remain enabled any vendor-provided feature, update, or default configuration that would share surveillance data outside the municipality; connect a municipal system to an external surveillance data network; enable persistent live display, live audio, remote camera control, automated camera selection, cross-camera tracking, person or vehicle reidentification, appearance search, or other automated analysis; or otherwise materially expand surveillance capability without the approval required by this section. A municipal agency receiving notice from a vendor of the availability or activation of such a feature shall disable the feature where technically possible and notify the Assembly in writing within ten days.

E. *Notice of solicitation.* A municipal agency receiving a solicitation, offer, demonstration, or proposal from a vendor of surveillance technology shall report that contact to the Assembly in writing within thirty days. This subsection creates no obligation to decline such contact.

(AO No. 2023-35(S-1), § 1, 4-18-2023; AO No. 2024-69, § 3, 7-30-2024)

### **3.102.030 Data collection, protection, and retention.**

A. *Collection of data.* Any and all data gathered by municipal surveillance technology, to include meta-data, shall be the exclusive property of



the Municipality of Anchorage and shall be stored and preserved within the municipality's custody until destroyed in accordance with this code and/or agency retention schedules.

1. No vendor shall acquire ownership, intellectual property rights, or perpetual license interests in municipal data, including derivative or aggregated forms, except as expressly authorized by ordinance.
2. Any contract provision purporting to grant a vendor irrevocable, perpetual, royalty-free, transferable, or sublicensable rights in municipal data or its derivatives is void as against public policy unless expressly approved by the Assembly.

B. *Protection and sharing of data.* Except as permitted by an expressed provision in code, no agent or agency of the municipality may disclose data or meta data collected through the use of surveillance technology to a third party, without the approval of the assembly in the form of a resolution.

1. Surveillance data shall not be shared with, disclosed to, or made accessible to any agency of another state, any federal agency, or any private person or entity, except pursuant to a warrant issued upon probable cause, other valid court order, or as required by the Alaska Public Records Act.
2. Surveillance data shall not be sold, leased, traded, or transferred for any commercial purpose.
3. No municipal employee shall query, cause to be queried, or request that another person query any surveillance system or database, whether operated by the municipality or by any other entity, on behalf of or for the benefit of an agency of another state, a federal agency, or a private person or entity, except pursuant to a warrant issued upon probable cause or other valid court order. This paragraph applies to municipal employees assigned to multi-agency task forces.
4. Surveillance data shall not be used for, or shared for the purpose of, the enforcement of civil immigration law, or the enforcement of the law of another jurisdiction with respect to conduct that is lawful in the State of Alaska.
5. Nothing in this subsection prevents the municipality from complying with the National Child Search Assistance Act, 34 U.S.C. §§ 41307 and 41308, or other federal statute requiring cooperation in the search for missing or exploited children.

C. *Retention.*

1. Captured plate data shall be permanently deleted no later than

- 14 fourteen days after capture, unless otherwise specified in this  
15 section.
- 16 2. Video, audio, and sensor data collected by, routed through, or  
17 recorded by a real-time crime center, a camera owned or  
18 operated by the municipality, or an integrated camera feed shall  
19 be permanently deleted no later than fourteen days after  
20 capture.
- 21 3. Captured plate data may be retained beyond fourteen days  
22 only where, before the expiration of the fourteen-day period, the  
23 data has been:
- 24 a. Determined to be relevant and material to an  
25 investigation of a vehicle identified on a hotlist;
  - 26 b. Designated as evidence in a specific criminal  
27 investigation identified by case number, by a named  
28 municipal employee, with the designation, the case  
29 number, the identity of the designating employee, and  
30 the date and time of designation recorded in an audit log;
  - 31 c. Preserved pursuant to a written preservation request,  
32 litigation hold, court order, or discovery obligation;
  - 33 d. Preserved pursuant to a pending public records request;  
34 or
  - 35 e. Preserved pursuant to a warrant, subpoena, or other  
36 judicial order.
- 37 4. Bulk, categorical, automatic, or default designation of  
38 surveillance as relevant to an investigation is prohibited. Each  
39 designation shall be individually made and individually  
40 recorded.
- 41 5. Deletion required by this subsection shall be accomplished by  
42 automated technical configuration of the applicable system and  
43 shall not rely upon manual or procedural action alone. The chief  
44 of police shall certify in the Annual Surveillance Report that  
45 automated deletion is configured and functioning and shall  
46 disclose any period during which it was not.
- 47 6. The retention periods established by this subsection may be  
48 extended only by ordinance. They shall not be extended by  
49 administrative policy, departmental procedure, vendor  
50 agreement, contract term, memorandum of understanding, or  
51 vendor default configuration.

**3.102.040 Annual surveillance technologies report.**

No later than June 1 of each year, the mayor or a designee shall submit to the assembly in the form of an information memorandum the Annual Surveillance Report with all the information required by this section.

A. Each municipal department or agency using ALPR technology under as authorized under this chapter shall provide a general description of the type and purpose of each instance that sufficiently explains how the use was not prohibited by this chapter, and, if applicable, whether the use was pursuant to a search warrant, a court order, or a judicially recognized exception to the warrant requirement, and the final disposition of evidence resulting from each instance, to include:

1. The total number of license plates or vehicles captured;
2. The number of hot list matches, disaggregated by category;
3. The number of matches confirmed accurate and the number determined to be inaccurate; and
4. The number of warrants sought, obtained, and denied for queries.

B. Each municipal department and agency that used a UAS in the preceding calendar year shall report:

1. The number of instances in which a UAS was used;
2. A general description of the type and purpose of each instance that sufficiently explains how the use was not prohibited by this chapter, and, if applicable, whether the use was pursuant to a search warrant, a court order, or a judicially recognized exception to the warrant requirement, and the final disposition of evidence resulting from each instance; and
3. Any new policy, or change in department or agency policy, related to the use of UAS technology.

C. Each municipal department or agency using facial recognition technology under an exception provided in this chapter shall report:

1. The number of instances in which facial recognition technology was used or information derived from facial recognition technology was received or used under exceptions provided in this chapter;
2. A general description of the type and purpose of each instance that sufficiently explains how the use was not prohibited by this chapter, and, if applicable, whether the use was pursuant to a search warrant, a court order, or a judicially recognized

exception to the warrant requirement, and the final disposition of evidence resulting from each instance; and

3. Any new policy, or change in department or agency policy, related to the use of facial recognition technology.

D. The annual report shall also include the following information with respect to real-time crime center operations and the use of any other surveillance technology:

1. The number of instances in which a cell-site simulator or similar technology was used, and whether the use was permitted by a search warrant, court order, or judicially recognized exception to the warrant requirement;
2. The duration of time used, amount and nature of data collected in each instance, to include the amount and nature of data inadvertently collected from devices or individuals who were not the intended target of the search or subject of the warrant;
3. The number of live monitoring sessions, total and average session duration, and the number of sessions involving integrated camera feeds, disaggregated by authorized purpose, to include:
  - a. The number of supervisory renewals, emergency sessions initiated without prior approval, cross-camera tracking sessions, uses of remote pan, tilt, or zoom controls, and instances in which live audio was accessed;
  - b. The average and maximum number of camera feeds accessed during a live monitoring session; and
  - c. Each substantiated instance of unauthorized live access or violation of this chapter., and the corrective action taken;
4. The number of arrests made by APD where surveillance technology was utilized in a related incident response or investigation, regardless of whether the information gathered from the technology was used to establish probable cause;
5. The number of instances in which surveillance data was designated as evidence, reported in aggregate by case type;
6. The detailed log of every unauthorized receipt, access, or use of surveillance technology or information derived from surveillance technology. The log shall denote how the unauthorized access occurred, what corrective steps have been taken, and the final disposition of any evidence or

information improperly received;

7. Each instance of surveillance data sharing outside the municipality, identifying the receiving entity, the legal basis, and the volume of data;
8. The total number of queries of retained surveillance data, disaggregated by justification category to include:
  - a. The number of queries resulting in arrest, and the number resulting in referral for prosecution; and
  - b. The number of queries conducted under the imminent-threat exception provided in this chapter;
9. The certification of automated deletion and any period of non-compliance;
10. The certification of unused and disabled capability;
11. Each solicitation and each vendor feature reported as required by this chapter; and
12. All audit exceptions identified and their disposition.

(AO No. 2023-35(S-1), § 1, 4-18-2023)

### **3.102.050 Audit and enforcement.**

- A. *Independent audit.* The municipal ombudsman, or internal audit at the direction of the Assembly, shall conduct an annual audit of compliance with this chapter. The audit shall include direct examination of system audit logs, retention configuration, sharing configuration, consent records, user access records, and a risk-based sample of live monitoring sessions sufficient to test the incident or case nexus, authorized purpose, camera and geographic scope, duration, supervisory approvals, renewals, audio access, remote camera control, cross-camera tracking, and automatic termination controls. The audit report shall be submitted in the form of an information memorandum to the assembly.
- B. *Violations.* Any municipal employee who violates a provision of this chapter may be subject to discipline in accordance with the municipality's disciplinary policies and procedures and applicable collective bargaining agreements. Violation of this chapter by any official or employee of the municipal is grounds for remedial training, suspension, termination, and/or criminal prosecution.
  1. *Suspension.* Upon a finding by the Assembly, after public hearing, that a municipal agency has materially violated this chapter, the assembly may by resolution suspend that agency's

1 use of the surveillance technology at issue until the assembly  
2 finds the violation cured.

3  
4 2. *Unlawful destruction and unlawful retention.* Intentional  
5 destruction of records required to be retained under this  
6 chapter, and intentional retention of surveillance data required  
7 to be deleted under this chapter, may be prosecutable as a  
8 criminal offense.

9  
10 3. *Inadmissibility.* Surveillance data obtained, accessed, viewed,  
11 monitored, retained, queried, or shared in violation of this  
12 chapter, and any evidence derived therefrom, shall not be  
13 offered into evidence in any proceeding brought by the  
14 municipality, except where the evidence is exculpatory.

15  
16 C. *Private cause of action.*

17  
18 1. Any violation of this chapter constitutes an injury, and any  
19 person so injured may institute proceedings in the Superior  
20 Court in a civil action seeking injunctive relief, declaratory relief,  
21 damages, and attorney's fees. Any action instituted under this  
22 paragraph shall be brought against the municipality. If  
23 applicable, any third party with whom the municipality  
24 contracted or entered into an agreement may be joined as a  
25 third party to such action.

26  
27 2. Any person who has instituted proceedings under the previous  
28 paragraph and is found to have been subjected to face  
29 surveillance in violation of this chapter, or about whom data or  
30 information is found to have been obtained, retained, stored,  
31 possessed, accessed, used, or collected in violation of this  
32 chapter, shall be entitled to recover actual damages of not less  
33 than the greater of:

34  
35 a. \$1,000.00 for each violation of this chapter; or

36  
37 b. \$10,000.00.

38  
39 3. Any prevailing plaintiff in any action brought under this  
40 subsection shall be entitled to the award of costs and  
41 reasonable attorney's fees.

42  
43 (AO No. 2023-35(S-1), § 1, 4-18-2023)

44  
45 **3.102.060 Automated license plate reader systems.**

46  
47 A. *Use of ALPR systems.* It shall be unlawful for any municipal agency to  
48 operate or use an ALPR system, or use captured plate data, except  
49 as authorized by this section.

50  
51 B. *Permitted real-time comparison.* An ALPR system may compare

captured plate data in real time against a hot list limited to vehicles that are:

1. Reported stolen, or that bear license plates reported stolen;
2. The subject of an active AMBER Alert, Silver Alert, or comparable emergency alert concerning a missing or endangered person;
3. Registered to a person for whom an outstanding felony warrant has been issued;
4. Specifically identified in an active, documented investigation of a felony offense; or
5. Specifically identified in an active, documented investigation of a missing or endangered person.

An ALPR system shall not be used for investigation or enforcement of any suspected misdemeanor or minor offense, infraction, or civil violation.

- C. The provisions of this section shall be repealed by operation of law effective January 1, 2031 unless affirmatively continued by the assembly by ordinance.

### **3.102.070 Body-worn cameras.**

- A. There shall be a body-worn camera policy governing the employment and use of body-worn cameras, including the standards for the storage, preservation, review, release and disposition of digital multimedia evidence by the Anchorage Police Department.
1. The policy shall contain a mandatory procedure and timeline for the review and release of body-worn camera footage of critical incidents. The policy may provide for footage to be edited or redacted, but shall ensure that the footage released is a fair, accurate, and thorough depiction of the critical incident. A delay beyond the established release date shall constitute a denial of any pending public records request, upon which the requester may, notwithstanding the provisions of section 3.90.060, immediately seek appropriate relief from the superior court.
  2. The policy shall be reviewed by the municipal attorney and approved by the chief of police.
- B. Any use of body-worn cameras or digital multimedia evidence shall be in accordance with the approved body-worn camera policy. Failure to adhere to the policy may be considered grounds for corrective action or discipline under established police department policies and

procedures.

### **3.102.080 Facial recognition technology.**

- A. The use of facial recognition technology in conjunction with, or as a component of, any real-time surveillance or surveillance technology by the municipality or any municipal staff shall be unlawful.
- B. Unless provided otherwise within this section, it shall be unlawful for the municipality or any municipal staff to obtain, retain, request, access, or use:
  - 1. Facial recognition technology; or
  - 2. Information obtained from facial recognition technology.
- C. Municipal staff's inadvertent or unintentional receipt, access to, or use of any information obtained from facial recognition technology shall not be a violation of this section, provided that:
  - 1. Municipal staff did not request or solicit the receipt, access to, or use of such information; and
  - 2. Municipal staff logs such receipt, access, or use in its Annual Surveillance Report. Such report shall not include any personally identifiable information or other information the release of which is prohibited by law.
- D. Any evidence or information obtained through facial recognition technology, regardless of whether it was obtained lawfully, shall not be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant.
- E. Exceptions.
  - 1. Nothing in this chapter shall prevent the municipality from:
    - a. Acquiring, obtaining, retaining, or accessing facial recognition technology on an electronic device intended for a single user, such as a mobile communication device, cellular phone or tablet, when the facial recognition technology is used solely for the purpose of the user;
    - b. Acquiring, obtaining, retaining, or accessing social media or communications software or applications intended for communication with the general public that include facial recognition technology, as long as the municipality does not intentionally use the facial recognition technology;



- c. Having custody or control of electronic devices that include facial recognition technology when such electronic devices are held by the municipality solely for evidentiary purposes;
  - d. Acquiring, obtaining, retaining, or accessing facial recognition technology solely for the purpose of using automated or semi-automated redaction software;
  - e. Complying with the National Child Search Assistance Act, 34 U.S.C. §§ 41307—41308, or other federal statutes requiring cooperation in the search for missing or exploited children; or
  - f. Participating in, coordinating with, or otherwise being involved with multi-agency law enforcement investigations, working groups or task forces. Specifically, municipal law enforcement may intentionally work with third-party agencies using Facial Recognition Technology to identify:
    - i. Human remains or suspected missing persons;
    - ii. Suspected victims of human trafficking; or
    - iii. Suspected victims of child abuse or exploitation.
2. It shall not be a violation of this chapter for the municipality to acquire, obtain, or retain facial recognition technology when all the following conditions exist:
  - a. The facial recognition technology is an integrated, off-the-shelf capability, bundled with software or stored on a product or device;
  - b. Other functions of the software, product, or device are necessary or beneficial to the performance of municipal functions;
  - c. The software, product, or device is not acquired for the purpose of performing facial recognition;
  - d. The facial recognition technology cannot be deleted from the software, product, or device;
  - e. The municipality does not use the facial recognition technology; and
  - f. The municipal department, agency, or official seeking to acquire the software, product, or device discloses the integrated, off-the-shelf facial recognition technology

that cannot be deleted to the assembly when seeking to acquire the software, product, or device.

### **3.102.090 Unmanned aircraft systems.**

A. The use of Unmanned Aircraft Systems (UAS) by departments, agencies, and contractors of the Municipality of Anchorage is restricted as follows:

1. A UAS shall not be used in violation of AS 18.65.900—18.65.909 Law Enforcement Use of Unmanned Aircraft Systems;
2. A UAS shall not be used for routine patrol activities;
3. A UAS shall not be used for warrantless searches that are specifically seeking evidence as part of a criminal investigation;
4. A UAS shall not be used in a manner that violates a person's reasonable expectation of privacy unless supported by a warrant, or in accordance with a judicially recognized exception to the warrant requirement;
5. A UAS shall not be weaponized, nor shall it be used as a weapon;
6. A UAS shall not be used for any surveillance of persons or groups involved in constitutionally protected activities;
7. A UAS shall not be used for traffic enforcement activities, except to the extent that such use relates to an accident investigation; and
8. A municipality-owned UAS shall not be permitted to be used by any non-municipality of Anchorage agency, including, but not limited to, agencies of the State of Alaska or agencies of the United States of America.

### **3.102.100 Real-time crime center operations.**

A. *Purpose.* A real-time crime center exists to provide public safety personnel with immediate situational awareness in response to a specific incident. It shall not be used as a repository of the historical movements of members of the public, a system for continuous observation or virtual patrol, or a means to track persons or vehicles across cameras without an incident-specific law enforcement basis.

B. *Prohibitions.* Unless otherwise authorized in code, no facial recognition, person or vehicle reidentification, appearance search, gait analysis, behavior or emotion inference, demographic inference, anomaly detection, automated crowd analysis, route reconstruction,

1 or automated camera-to-camera tracking shall be applied to a live  
2 camera feed.

3  
4 C. *Registered cameras, integrated camera feeds, and live monitoring.*

- 5  
6 1. The municipality may maintain a program under which owners  
7 of cameras not owned by the municipality may voluntarily  
8 register the location of those cameras, or may voluntarily  
9 provide the municipality with an integrated camera feed.  
10 Participation shall be voluntary in all respects.
- 11  
12 2. Registration of a camera under this subsection does not  
13 authorize the municipality to access that camera. The  
14 municipality may obtain recorded footage from a registered  
15 camera only by voluntary provision by the owner or owner's  
16 authorized agent, or pursuant to a warrant, court order, or  
17 subpoena.
- 18  
19 3. An integrated camera feed shall be established only upon the  
20 written, informed, and revocable, clear and unmistakable  
21 consent of the camera owner. The consent shall state the  
22 cameras included, the hours of availability, whether the feed  
23 includes audio or permits remote pan, tilt, or zoom control, the  
24 live-monitoring limitations established by this section, and the  
25 owner's right to withdraw consent at any time and for any  
26 reason. Withdrawal of consent shall take effect within twenty-  
27 four hours.
- 28  
29 4. The municipality shall not continuously record, copy, buffer, or  
30 store any integrated camera feed. The municipality may record  
31 a discrete segment of an integrated camera feed only where  
32 the segment relates to a specific incident, and any such  
33 recording is subject to protection and retention requirements of  
34 this chapter.
- 35  
36 5. The municipality shall not accept, register, integrate, or receive  
37 data from any privately owned or privately operated ALPR  
38 system, and shall not accept an integrated camera feed from  
39 any camera that incorporates ALPR capability unless that  
40 capability is disabled with respect to the feed provided to the  
41 municipality.
- 42  
43 6. Participation or non-participation in a program under this  
44 subsection shall not be a condition of, and shall not affect, the  
45 provision of any municipal service, permit, license, or law  
46 enforcement response.
- 47  
48 7. The municipality shall not disclose the identity, address, or  
49 contact information of a participant except as required by law.
- 50  
51 8. A municipal employee may initiate or participate in a live

monitoring session only for one or more of the following purposes:

- a. Responding to a specific reported incident, emergency call, or computer-aided dispatch event that is in progress or for which an immediate law enforcement response remains active;
- b. Addressing a specific and articulable imminent threat of death or serious physical injury;
- c. Locating a specific missing or endangered person;
- d. Supporting an active, documented investigation of a felony offense where a supervisor has approved a written statement of specific facts establishing a reasonable nexus between the investigation and the camera or geographic area to be viewed; or
- e. Conducting monitoring authorized by a warrant or other valid court order.

9. A live monitoring session shall not be used for continuous, random, generalized, or location-based observation; routine patrol; deterrence; crowd scanning; monitoring of a route, neighborhood, residence, business, gathering place, or category of persons; or observation of persons for whom no authorized purpose exists. Integrated camera feeds shall not be displayed on a persistent wallboard, automatically cycled, or left open between authorized live monitoring sessions.

10. Before initiating a live monitoring session, the user shall enter into the system the user's identity, the applicable incident, dispatch, or case number, the authorized purpose, the specific camera or narrowly defined geographic area to be viewed, and the date and time. Supervisory approval shall be recorded before monitoring begins. Where delay would create a substantial risk of death or serious physical injury, monitoring may begin without prior supervisory approval, but the user shall record the required information as soon as practicable and a supervisor shall review and approve or disapprove the session within twenty-four hours.

11. Each live monitoring session shall be limited to cameras and a geographic area reasonably likely to provide information material to the authorized purpose. The session shall end promptly when the operational need ends. The system shall automatically terminate live access after sixty minutes unless a supervisor records a specific written justification for renewal. Each renewal shall be limited to thirty minutes. A renewal may not rely solely upon a pre-set or categorical justification.

12. The system shall automatically log each camera feed accessed, the start and end time of access, each user with access, each use of pan, tilt, or zoom controls, each recording or export, each expansion of the geographic area, and each supervisory approval or renewal. Audit logs required by this paragraph shall be retained for not less than four years and shall not contain the video or audio content of the feed.
13. No municipal employee shall use live camera feeds to follow, reidentify, or reconstruct the movements of a person or vehicle across two or more cameras, except to address an imminent threat of death or serious physical injury, to locate a missing or endangered person, during an active pursuit of a person reasonably suspected of a felony offense, or pursuant to a warrant or other valid court order. Any such cross-camera tracking shall be specifically documented and separately identified in the audit log.
14. The municipality shall not remotely pan, tilt, zoom, reposition, or otherwise control a privately owned camera unless the owner has separately and expressly consented in writing to remote control. Remote control may be used only during an authorized live monitoring session and only to view an area reasonably related to the authorized purpose. Absent a warrant or an imminent threat of death or serious physical injury, no camera shall be manipulated to view into a dwelling or an area not ordinarily visible from the camera's normal position.
15. Audio from an integrated camera feed shall be disabled by default and shall not be accessed, monitored, recorded, or analyzed unless authorized by a warrant or other valid court order, necessary to address an imminent threat of death or serious physical injury, or separately authorized through incident-specific consent that complies with applicable law.
16. Access to live camera feeds shall be limited through role-based permissions to trained employees whose assigned duties require such access. The municipality shall require unique user credentials, multi-factor authentication, automatic screen locking, and prompt revocation of access upon reassignment, separation, or loss of operational need. Shared user accounts are prohibited.

C. *Query controls.*

1. Every query of retained surveillance data shall record the identity of the querying user, the date and time of the query, a valid case number, and a specific written justification. Selection from a menu of pre-set justifications shall not by itself satisfy this requirement.

2. A query of captured plate data more than fourteen days old shall additionally require a warrant issued upon probable cause, except where necessary to address an imminent threat to human life, in which case a written report shall be filed with the chief of police within twenty-four hours and disclosed in the Annual Surveillance Report to the assembly.

D. *Predictive analytics prohibited.* No municipal agency shall use predictive analytics to forecast the location of future criminal activity or to assign a risk score to an identified individual. All action taken on the basis of surveillance data shall be predicated on observed and verified information.

E. *Audit logs.* Audit, query, access, consent, and system configuration logs generated under this section are public records subject to disclosure under chapter 3.90. Individual license plate numbers, vehicle images, and vehicle-identifying characteristics shall be redacted before release.

**Section 2.** Anchorage Municipal Code section 7.15.040 is hereby amended to read as follows (*the remainder of the section is not affected and therefore not set out*):

**7.15.040 Assembly approval of contracts and grants.**

A. Assembly approval of contracts. In addition to a contract described in subsections F and G, no contract for supplies, services, professional services or construction whereby the municipality is obligated to pay more than \$500,000.00 pursuant to a contract awarded through competitive procedures (which are described in sections 7.20.020 through 7.20.040 (bids) and section 7.20.060 (proposals)) or more than \$500,000.00 pursuant to a contract awarded pursuant to section 7.20.080A.1 (intergovernmental, utility, and post-secondary educational agreements) or section 7.20.080A.2 (cooperative purchases; piggybacking), or more than \$250,000.00 pursuant to a contract for legal services awarded pursuant to section 7.20.100A, or more than \$50,000.00 pursuant to a contract awarded through other authorized procedures, including any amendment pursuant to awards under section 7.20.080A.5, may be executed unless the assembly has approved a memorandum setting forth the essential terms of the contract and information required by this section.

\*\*\* \*\*\* \*\*\*

F. Lobbying contracts. Regardless of the amount involved, all contracts for professional lobbying services must be approved in advance by the assembly.

G. Surveillance contracts. Regardless of the amount involved, all contracts for the procurement of surveillance technology or services, as that term is defined in chapter 3.102, must be approved in advance

by the assembly.

H. CM/GC and compensation-from-revenue-generated-from-use-of municipal-property contracts. Notwithstanding the dollar amount thresholds for procurement methods or contract types stated in subsection A, the following types of contracts are subject to the requirements of assembly approval prior to execution, in addition to reporting requirements, as stated herein:

\*\*\* \*\*

(AO No. 79-203; AO No. 82-168; AO No. 93-217, § 1, 2-26-1994; AO No. 94-123(S), § 1, 8-25-1994; AO No. 2001-122(S-1), § 2, 7-24-2001; AO No. 2007-22, § 1, 2-27-2007; AO No. 2018-74, § 1, 9-25-2018; AO No. 2015-39, § 1, 5-14-2015; AO No. 2019-24, § 3, 4-1-2019; AO No. 2023-23(S), § 1, 3-21-2023;[1] AO No. 2023-108, § 1, 11-21-2023; AO No. 2025-37, § 4, 5-16-2025; AO No. 2025-139(S) Amended, 1-13-2026)

**Section 3.** Within one hundred twenty days after the effective date of this ordinance, the Mayor is directed to cause each municipal agency to submit to the Assembly an inventory of all surveillance technology currently in use, acquired, or under contract, together with a surveillance impact report for each. Surveillance technology in use as of the effective date may continue in use during Assembly review.

**Section 4.** The existing text of Anchorage Municipal Code chapter 3.102 being repealed under this ordinance is attached as Exhibit A, in accordance with Anchorage Municipal Code subsection 1.05.050B.

**Section 5.** This ordinance shall be effective ninety days after passage and approval by the Assembly, except the requirements of AMC subsection 3.102.020C. shall be effective immediately upon passage and approval by the Assembly.

PASSED AND APPROVED by the Anchorage Assembly this \_\_\_\_\_ day of \_\_\_\_\_, 2026.

Chair

ATTEST:

Municipal Clerk