

ORDINANCE O-2026-XX

AN ORDINANCE ENACTING, IN PERTINENT PART, THE DURANGO CODE OF ORDINANCES CHAPTER 2 - ADMINISTRATION - ARTICLE VIII – MASS SURVEILLANCE TECHNOLOGY REGULATION, TO READ AS FOLLOWS:

(Red type indicates addition of text, strike through indicates original text removed,
empty brackets [] indicate omitted and unchanged text)

WHEREAS, surveillance technologies may assist legitimate law enforcement investigations, emergency response, public safety operations, and municipal administration;

WHEREAS, the unchecked acquisition, use, retention, or sharing of surveillance technologies and Surveillance Data may infringe upon constitutional rights, civil liberties, privacy interests, and freedom of association and expression;

WHEREAS, public transparency and democratic oversight regarding surveillance technologies increase public trust and accountability;

WHEREAS, clear standards, data minimization practices, independent oversight, and procedural safeguards improve compliance with the United States Constitution, Colorado law, and principles of due process;

WHEREAS, the purpose of this Ordinance is to establish narrowly tailored safeguards governing the acquisition, use, retention, sharing, and oversight of surveillance technologies while preserving lawful and necessary public safety functions.

ARTICLE VIII – Mass Surveillance Technology Regulation

Section 2-301. Definitions

Agency means any department, office, division, board, commission, or other unit of the City of Durango, including the Durango Police Department, that acquires, uses, accesses, shares, or manages Surveillance Technology or Surveillance Data.

Biometric data means one or more biometric identifiers that are used or intended to be used, singly or in combination with each other or with other personal identifying information, for identification purposes. *Biometric data* does not include the following unless the biometric data is used for identification purposes:

1. A digital or physical photograph;
2. An audio or voice recording; or
3. Any data generated from a digital or physical photograph or an audio or video recording.¹

Biometric identifier means data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. "Biometric identifier" includes:

1. A fingerprint;

¹ C.R.S. § 6-1-1303

2. A voiceprint;
3. A scan or record of an eye retina or iris;
4. A facial map, facial geometry, or facial template; or
5. Other unique biological, physical, or behavioral patterns or characteristics.²

Bulk Collection means the indiscriminate or large-scale collection of Surveillance Data concerning multiple persons, devices, or vehicles where individualized suspicion is absent.

Exigent circumstances means a situation that poses an imminent threat to public safety requiring urgent action to prevent harm. This includes, but is not limited to, situations involving an imminent threat of death or serious bodily harm or other critical incidents necessitating immediate response.

Personal Identifying Information means information that may be used, along or in conjunction with any other information, to identify a specific individual, including but not limited to a name; a date of birth; a place of birth; a social security number or tax identification number; a password or pass code; an official government-issued driver's license or identification card number; information contained in an employment authorization document; information contained in a permanent resident card; vehicle registration information; a license plate number; a photograph, electronically stored photograph, or digitized image; a fingerprint; a record of a physical feature, a physical characteristic, a behavioral characteristic, or handwriting; a government passport number; a health insurance identification number; an employer, student, or military identification number; a financial transaction device; a school or educational institution attended; a source of income; medical information; biometric data; financial and tax records; home or work addresses or other contact information; family or emergency contact information; status as a recipient of public assistance or as a crime victim; race; ethnicity; national origin; immigration or citizenship status; sexual orientation; gender identity; physical disability; intellectual and developmental disability; or religion.³

Point-in-time means the observation or recording of activities exposed to public view, without prolonged monitoring, individualized tracking, behavioral analysis, or movement reconstruction. Point-in-time observation or recording, alone, does not constitute surveillance under this Ordinance, unless it operates without an individualized or incident-based trigger, as described in Section 2-302(b).

Privacy and Civil Liberties Officer or *PCLO* means the individual or City Official designated to perform the duties under 2-306(c).

Share or *Sharing* means to disclose, transfer, provide access to, sell, license, or otherwise make available Surveillance Data, including Personal Identifying Information, to any person or entity outside the possessing Agency.

Surveillance Data means any information, record, image, audio, video, metadata, biometric data, biometric identifier, location information, or derivative analysis collected, generated, or obtained by or through the use of Surveillance Technology, including Personal Identifying Information acquired from third parties for surveillance purposes.

Surveillance Technology means any software, hardware, system, device, or process that is designed or primarily intended to observe, collect, retain, infer, analyze, or share information about persons or groups, their activities, locations, movements, or associations. Surveillance Technology includes, but is not limited to, automated license

² *Id.*

³ C.R.S. § 24-74-102

plate readers; video cameras with analytics; cellular site simulators; drones or unmanned aircraft systems; facial recognition or other biometric identification technologies; social media monitoring tools; predictive analytics; gunshot detection; and real-time location tracking systems. Exclusions: routinely used City information technology that does not collect or analyze data for surveillance purposes (e.g., standard IT security tools, building access systems limited to authorized employees) is not Surveillance Technology unless configured or used to surveil members of the public.

Third Party means any private entity, non-City governmental entity, or individual that is not an Agency.

Warrant means a search warrant issued by a court of competent jurisdiction upon a showing of probable cause, as required by law.

Section 2-302. Scope; Applicability; Construction

- a) **Applicability.** This Ordinance applies to all Agencies' acquisition, use, operation, procurement and contracting for, data practices relating to, and Sharing of Surveillance Technology and Surveillance Data, regardless of funding source.
- b) **Scope of Covered Surveillance Technology.** This Ordinance applies only to Surveillance Technology that, by design or deployment, continuously or routinely captures, collects, monitors, or analyzes information concerning persons, vehicles, devices, or locations without requiring an individualized or incident-based trigger.
 - (1) This Ordinance does not apply to technologies that record or collect information only in response to a discrete event, violation, emergency, lawful enforcement action, or manual activation, including body-worn cameras, dashboard cameras, interview room recording systems, or traffic safety cameras that capture images only upon detection of a specific violation.
 - (2) This Ordinance does not apply to ordinary law enforcement records, administrative records, evidence systems, or information management systems that store, maintain, or process information collected through other means and that do not independently capture, collect, monitor, or analyze information concerning persons, vehicles, devices, or locations.
- c) **Contracts and Grants.** No contract, grant, intergovernmental agreement, memorandum of understanding, or nondisclosure agreement may be used to circumvent any requirement of this Ordinance.
- d) **Construction.** Where this Ordinance imposes greater protections or stricter standards than otherwise required by law, Agencies shall comply with this Ordinance to the fullest extent consistent with applicable state and federal law.

Section 2-303. Warrant Triggers and Legal Process

- a) **Warrant Required.** Absent an applicable exception under subsection (c) of this section, a Warrant is required for:
 - (1) targeted, or prolonged tracking of a person's movements, communications content, or location information not exposed to public view;
 - (2) access to Personal Identifying Information from a device or account where a reasonable expectation of privacy exists;
 - (3) acquisition or use of Biometric Data for identification or verification of a specific person; and

- (4) bulk collection or analysis that could reasonably raise individualized constitutional concerns.
- b) Warrant Guidelines. When seeking a Warrant, the Agency or Third-Party shall:
 - (1) articulate probable cause and particularity to limit scope, duration, and data types;
 - (2) minimize acquisition of non-pertinent data;
 - (3) include deletion protocols for the surveillance data sought; and
 - (4) include a return and reporting mechanism consistent with court rules.
- c) Exceptions to Warrant Requirement.
 - (1) Consent. Valid, informed, and voluntary consent by the data subject, documented in writing or recorded; or
 - (2) Exigent circumstances. The Agency or Third-Party shall seek a Warrant or other lawful process as soon as practicable and, in any event, within 72 hours, where required by law. Access of surveillance data shall cease once the Exigent Circumstances end if no legal process is obtained.
 - (3) Plain View/Public Exposure. Observation of activities or information knowingly exposed to the public, consistent with applicable law.

Section 2-304. Data Sharing

- a) Conditions for Sharing. An Agency may Share Surveillance Data only when:
 - (1) Sharing is necessary for a legitimate law enforcement, public safety, or City operational purpose consistent with an approved Surveillance Use Policy under Section 306; and
 - (2) Sharing is supported by one or more of the following:
 - i. A valid Warrant;
 - ii. A court order or other lawful process which compels disclosure;
 - iii. A written, case-specific request citing applicable legal authority; or
 - iv. A documented Exigent circumstance, with post hoc court authorization or other authorization obtained as required by law.
- b) Prohibitions and Restrictions.
 - (1) No Sharing for civil immigration enforcement, civil debt collection, or discrimination based on protected characteristics or First Amendment activity, except as required by law.
 - (2) No sale, licensing for consideration, or monetization of Surveillance Data.
 - (3) No Sharing of Biometric Data or location data obtained through Bulk Collection absent a Warrant or explicit statutory authorization, except in an Exigent Circumstance with post ad hoc court authorization.
 - (4) No Sharing subject to an agreement that prevents compliance with this Ordinance, City records obligations, state or federal law, or court orders.
- c) Minimum Safeguards for Recipients. Prior to Sharing, the Agency shall execute a written agreement with the recipient that:
 - (1) limits use to the stated purpose and prohibits secondary use;
 - (2) requires data security measures, access controls, and audit logging;
 - (3) imposes retention and destruction requirements consistent with Section 2-305;
 - (4) prohibits further disclosure without the City's written consent or court order;
 - (5) requires breach notification to the Agency and Private Civil Liberties Officer (PCLO) within forty-eight (48) hours of discovery;
 - (6) permits City audit of Surveillance Technology and Surveillance Data; and
 - (7) mandates return or destruction of Surveillance Data upon completion of the stated purpose.

- d) Transparency. The Agency shall document each Sharing event, including legal basis, recipient, purpose, data categories, and date, and include aggregated reporting under Section 2-306.

Section 2-305. Privacy Protections; Data Management

(a) Data Minimization.

- (1) Agencies shall collect only the minimum Surveillance Data necessary to achieve an approved, lawful purpose and shall avoid collection of extraneous Personal Identifying Information wherever feasible.
- (2) Prior to implementation, the implementing Agency shall adopt a written policy for each Surveillance Technology establishing clear minimum data collection standards and limitations.

(b) Access Controls. Agencies shall implement role-based access controls, unique user authentication, least privileged access, and audit logging. Access to Biometric Data and any Warrant-derived data shall be limited to personnel with a documented legitimate law enforcement, public safety, or City operational purposes.

(c) Retention Limits.

- (1) Default Retention. Surveillance Data shall be retained no longer than twenty-one (21) days unless associated with a specific case, enforcement action, incident report, summons, or other legal obligation requiring longer retention. Prior to implementation, the implementing Agency shall establish policies governing retention and deletion timeframes.
- (2) Biometric and Highly Sensitive Data. Retention shall not exceed one ten (10) days except as otherwise provided in subsection (3) below. Prior to implementation, the implementing Agency shall establish policies governing retention limits for biometric and other highly sensitive data.
- (3) Extended Retention. Data tied to an ongoing investigation, prosecution, or claim shall be retained until final disposition and expiration of applicable legal holds, after which it shall be deleted. Prior to implementation, the implementing Agency shall establish policies governing extended retention and disposition timeframes.

(d) Destruction and Purging.

Agencies shall implement automated and auditable destruction processes aligned with subsections 305(a) – (c). Implementing Agency shall adopt a written policy for length of time destruction logs shall be maintained.

(e) Accuracy; Provenance.

Agencies shall maintain reasonable measures to ensure accuracy of Surveillance Data and its provenance. Analytical outputs shall be labeled as such and not treated as fact without corroboration.

(f) Security.

Agencies shall implement administrative, technical, and physical safeguards reasonably designed to protect Surveillance Data against unauthorized access, disclosure, alteration, or destruction, including encryption in transit and at rest where feasible.

(g) Use Limitations.

Surveillance Data shall not be used to infer or track protected characteristics and activities except where strictly necessary to investigate or prevent a specific criminal act and consistent with applicable law and approved policies.

(h) Training.

Personnel with access to Surveillance Technology or Surveillance Data must complete City-approved training on privacy, civil rights, data security, and this Ordinance before access and at least annually thereafter.

Section 2-306. Oversight and Accountability

(a) Agency Policies.

Each Agency shall adopt and publish a Surveillance Use Policy consistent with this Ordinance, approved by the PCLO, addressing permissible uses, prohibited uses, access controls, data management, Warrant procedures, training, audits, and complaint handling.

(b) Audits.

Agencies shall conduct internal audits annually and independent audits every three years to assess compliance with this Ordinance, approved policies, and data security standards. Findings and corrective actions shall be provided to the PCLO, City Council and, to the extent permissible, made public.

(c) Privacy and Civil Liberties Officer.

The PCLO shall: (1) review and make recommendations on Surveillance Impact Reports and Use Policies; (2) monitor compliance and oversee audits; (3) receive and investigate complaints; (4) provide technical assistance and training; and (5) publish annual reports.

(d) Complaint Mechanism.

The City shall maintain a public process to receive complaints concerning Surveillance Technology or Surveillance Data practices. Complaints shall be acknowledged within five (5) business days and reported on within thirty (30) days, subject to legal constraints.

(e) Public Reporting.

The City shall publish an annual report including: (1) inventory of approved Surveillance Technology; (2) aggregate usage statistics and purposes; (3) aggregate Sharing events by recipient type and legal basis; (4) retention and destruction metrics; (5) audit findings and corrective actions; (6) incidents of non-compliance and remedial measures; and (7) any verified impacts on civil rights or civil liberties.

Section 2-307. Contracting; Vendors

(a) Contract Requirements.

Contracts for Surveillance Technology or data services shall require compliance with this Ordinance and any applicable Colorado and federal law, and incorporate data security, privacy, transparency, audit, retention, and deletion obligations consistent with this Ordinance.

(b) Prohibited Terms. No vendor agreement shall include terms that:

(1) prevent compliance with this Ordinance, applicable Colorado and federal law, or court orders;

(2) compel the City to conceal the existence or capabilities of Surveillance Technology; or

(3) transfer ownership of City Surveillance Data to the vendor.

(c) Vendor Audits.

Vendors handling Surveillance Data shall submit to audits and provide timely breach notices within forty-eight (48) hours as specified in Section 2-304(c) and City standards.

Section 2-308. Penalties; Remedies; Enforcement

(a) Administrative Penalties.

Any Agency or City employee who knowingly or recklessly violates this Ordinance may be subject to disciplinary action up to and including termination, and the Agency may be subject to administrative sanctions imposed by the City Manager, including suspension of technology use.

(b) Penalties.

A violation by a vendor or Third Party may result in penalties as set forth in City Code Sec. 1-16, assessed per violation per day, and may also result in injunctive relief, contract suspension or suspension of services, or termination for cause.

(c) Suppression and Exclusion.

Nothing in this Ordinance limits any party's ability to seek suppression or exclusion of evidence as provided by applicable law.

(d) Cure and Mitigation.

Where feasible, the City may require remedial measures, including data destruction, retraining, policy revision, and enhanced monitoring.

(e) No Waiver of Immunities.

Nothing herein waives any immunities or defenses available to the City or its employees under applicable Colorado or federal law.

Section 2-309. Exceptions; Savings

(a) Exigent Circumstances.

In Exigent Circumstances an Agency may deviate from procedural requirements of Sections 303 and 304 only to the minimum extent necessary. The Agency shall document the facts, duration, and data collected; notify the PCLO within forty-eight (48) hours; and complete required processes post hoc as soon as practicable.

(b) Preexisting Technologies.

Within 180 days of the effective date, Agencies shall submit Surveillance Impact Reports and Use Policies for all preexisting Surveillance Technology to the PCLO. Continued use after that period without approval is prohibited.

(c) Conflict with Law.

If any provision of this Ordinance conflicts with state or federal law, the latter controls, and the conflicting provision shall be severed or construed to preserve the remainder. Nothing in this Ordinance shall be interpreted to limit rights of access under the Colorado Open Records Act or the Colorado Criminal Justice Records Act except where records are lawfully exempt from disclosure. Agencies shall maintain records sufficient to permit auditing, oversight, and public accountability consistent with applicable law.

This ordinance shall become effective ten (10) days after its passage and final publication as provided by law.

THE CITY OF DURANGO

Attest:

CITY COUNCIL OF

City Clerk

Mayor

STATE OF COLORADO

)

) ss.

COUNTY OF LA PLATA

)

I, Faye Harmer, City Clerk of the City of Durango, La Plata County, Colorado, do hereby certify that Ordinance No. O-2026- was regularly introduced and read at a regular meeting of the City Council of the City of Durango, Colorado on the ____ day of _____, 2026, and was ordered published in accordance with the terms and conditions of the statutes in such cases made and provided, in the Durango Herald, a newspaper of general circulation, on the ____ day of _____, 2026, prior to its final consideration by the City Council

City Clerk

I further certify that said Ordinance No. O-2026- was duly adopted by the Durango City Council on the ____ day of _____ 2026, and that in accordance with instructions received from the Durango City Council, said ordinance was published by title only in the Durango Herald on the ____ day of _____ 2026.

City Clerk