

# New Braunfels Surveillance Ordinance

Draft for legal and policy review

## Review note

The proposed ordinance prohibits City use of historical license plate reader systems and specified surveillance practices, including facial detection and recognition except for the narrow exclusions in Section 74-46. It permits hit-only readers at approved City entry points and on moving law enforcement vehicles during ordinary patrol, limits voluntary interagency sharing to eligible Texas agencies, and requires public reporting of recipients and sharing activity.

**State-law review is required before introduction.** Texas Business & Commerce Code Section 552.003 broadly preempts local regulations regarding artificial intelligence use. That could affect both the biometric provisions and AI-enabled ALPR restrictions. Limiting the ordinance to City operations does not establish that it avoids preemption. The City Attorney must resolve that question.

## HB 149 enacted text

Fixed and stationary readers are limited to approved City entry points. Hit-only readers on moving law enforcement vehicles are permitted during ordinary patrol under Section 74-41(i). Facial detection is permitted for privacy redaction. A separate, narrow exception permits court-authorized facial recognition of specified, previously obtained evidence in a specific criminal investigation; it does not authorize historical ALPR systems or live public scanning. Numerical deadlines are proposed policy choices, not existing legal requirements. Exhibit A must be completed and adopted before any fixed or stationary reader location is authorized. Section numbering, technical feasibility, mandatory retention and disclosure duties, initiative requirements, and Texas Business & Commerce Code Section 552.003 concerning local artificial-intelligence regulation require legal review before adoption. This draft is not approved for petition circulation.

Records-management reference: Texas State Library Local Schedule PS

*This review note is separate from the proposed ordinance text.*

## ORDINANCE NO. 2026-\_\_\_

**AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF NEW BRAUNFELS, TEXAS, AMENDING CHAPTER 74, “LAW ENFORCEMENT,” BY ADDING ARTICLE III, “SURVEILLANCE TECHNOLOGY AND PERSONAL DATA”; PROHIBITING SPECIFIED SURVEILLANCE TECHNOLOGIES AND PRACTICES; AUTHORIZING LIMITED HIT-ONLY AUTOMATED LICENSE PLATE RECOGNITION AT APPROVED CITY ENTRY POINTS AND ON MOVING LAW ENFORCEMENT VEHICLES DURING ORDINARY PATROL; RESTRICTING DATA COLLECTION, RETENTION, ACCESS, AND DISCLOSURE; LIMITING VOLUNTARY INTERAGENCY SHARING TO ELIGIBLE TEXAS AGENCIES; REQUIRING PUBLIC DISCLOSURE OF DATA RECIPIENTS AND SHARING ACTIVITY; ESTABLISHING CONTRACTING, AUDITING, COMPLIANCE, AND IMPLEMENTATION REQUIREMENTS; PROVIDING FOR REPEALER AND SEVERABILITY; AND ESTABLISHING AN EFFECTIVE DATE.**

WHEREAS, the City Council seeks to protect public safety while limiting unnecessary collection and use of information concerning the public’s identities, movements, associations, and activities; and

WHEREAS, contemporaneous comparison of a vehicle’s license plate against a narrowly authorized Hotlist presents different privacy concerns from retaining observations of vehicles that do not match that Hotlist; and

WHEREAS, facial detection, facial recognition, biometric identification, device tracking, and aggregation of personal information can enable identification and monitoring of individuals across locations, activities, and databases; and

WHEREAS, the City Council intends to establish enforceable limits on the City’s acquisition, operation, funding, and use of surveillance capabilities and information obtained through those capabilities; and

WHEREAS, the public should be able to determine which entities receive or can access City surveillance information, the purposes of that access, and the safeguards governing it; and

WHEREAS, the City Council intends that this Ordinance operate within the authority granted to the City and consistently with controlling state and federal law;

**NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF NEW BRAUNFELS, TEXAS:**

### **SECTION 1. AMENDMENT.**

Chapter 74, “Law Enforcement,” of the New Braunfels Code of Ordinances is amended by adding Article III to read as follows:

### **ARTICLE III. SURVEILLANCE TECHNOLOGY AND PERSONAL DATA**

#### **Sec. 74-37. Purpose and applicability.**

- (a) This article limits the City’s collection, acquisition, retention, use, and disclosure of personal surveillance information. It authorizes narrowly defined Hit-Only ALPR Systems at approved City Entry Points and on moving law enforcement vehicles during ordinary patrol under Section 74-41(i), and prohibits the surveillance practices identified in this article.
- (b) This article applies to every City department and to each officer, employee, contractor, vendor, volunteer, or other person acting on behalf of or at the direction of the City.
- (c) These restrictions apply regardless of:
  - (1) ownership of the equipment, software, account, or information;

- (2) the source of funding;
  - (3) whether a service is purchased, donated, borrowed, provided through a grant, or offered without charge;
  - (4) whether processing occurs locally, remotely, or through another entity; or
  - (5) whether a person acts through an individual account, shared account, interlocal agreement, or task-force assignment while performing City duties.
- (d) This article governs the City’s conduct and contractual relationships. It does not independently regulate an unaffiliated private person’s activities or direct another governmental entity’s operations.
- (e) The restrictions in this article are subject to the specific requirements of controlling law as addressed in Section 74-50.

## **Sec. 74-38. Definitions.**

For purposes of this article:

**ALPR System** means equipment or software configured or used to automatically extract, interpret, or compare motor vehicle license plate information from images or other sensor observations.

**Biometric Surveillance** means automated identification, verification, reidentification, or tracking of a person using biological or behavioral characteristics, including face geometry, iris or retinal patterns, voiceprints, gait, or comparable characteristics. Narrowly permitted forensic activities are addressed in Section 74-46.

**Candidate Alert** means an automated match between an observed complete license plate and an eligible Hotlist entry existing before the observation, pending human verification. A Candidate Alert is not a Verified Hit.

**City Entry Point** means a location where an existing public roadway crosses the incorporated municipal boundary of New Braunfels between the City and territory outside the City, as specifically identified in Exhibit A. The term does not include a county boundary, an extraterritorial-jurisdiction boundary, or an interstate ramp merely because traffic uses that location to reach the City.

**Covered Data** means Vehicle Observation Data and personal information generated, obtained, or derived through a technology or surveillance practice regulated by this article, including alerts, reports, analytical products, and copies containing that information.

**Eligible Texas Agency** means a governmental agency of the State of Texas or of a Texas political subdivision. The term excludes federal agencies, agencies of another state or country, and a task force, network, or other arrangement through which excluded entities receive access.

**Facial Detection** means automated analysis that locates or detects the presence of a human face in an image, recording, or live feed, whether or not the person is named, identified, or matched to another image. Permitted uses are limited by Section 74-46(h) and (i).

**Facial Recognition** means automated analysis of facial features to identify, verify, distinguish, reidentify, or track a person. It includes one-to-one verification, one-to-many identification, and matching across images or recordings without determining a person’s name.

**Fixed or Stationary ALPR** means an ALPR System installed or operated from a fixed or temporarily stationary platform, including a pole, structure, trailer, portable stand, parked vehicle, or similar platform.

**Historical ALPR System** means an ALPR System that retains or makes subsequently retrievable Vehicle Observation Data from a Non-Hit Observation beyond the processing expressly permitted by Section 74-40.

**Hit-Only ALPR System** means an ALPR System that satisfies every requirement of Section 74-40 and retains observation information only as expressly authorized for Candidate Alerts and Verified Hits.

**Hotlist** means a list containing only individually eligible vehicle entries meeting Section 74-42.

**Non-Hit Observation** means an observation that does not produce a Candidate Alert within the processing interval permitted by Section 74-40. An observation for which a comparison fails or cannot be completed is a Non-Hit Observation.

**Personal Information** means information that identifies, distinguishes, or can reasonably be linked to a person, household, personal device, or vehicle, alone or in combination with other reasonably available information. It includes:

- (1) names and government-issued identifiers;
- (2) biometric measurements, templates, and embeddings;
- (3) license plates and other vehicle identifiers;
- (4) device identifiers, advertising identifiers, network identifiers, and persistent online identifiers;
- (5) precise locations and movement histories;
- (6) identified communications, relationships, associations, or activities; and
- (7) inferred sensitive characteristics or individualized profiles derived from such information.

Information does not cease to be Personal Information merely because it is publicly available, encrypted, hashed, pseudonymized, or assigned an identifier instead of a name.

**Verified Hit** means a Candidate Alert for which an authorized person has confirmed the observed plate, its issuing jurisdiction, and the continuing validity and eligibility of the underlying Hotlist entry.

**Vehicle Observation Data** means information identifying or reasonably linkable to an observed vehicle, including its plate, image, location, observation time, travel direction, distinguishing characteristics, device or lane identifier, and any derivative capable of identifying the vehicle or reconstructing its observation.

#### **Sec. 74-39. Prohibited technologies and practices.**

- (a) The City shall not purchase, acquire, lease, subscribe to, install, operate, maintain, fund, or obtain services providing:
  - (1) a Historical ALPR System;
  - (2) Facial Detection, Facial Recognition, or Biometric Surveillance, except activities expressly preserved by Section 74-46;
  - (3) automated tracking or reidentification of individuals across cameras, recordings, or sensor observations;
  - (4) collection of personal-device identifiers from cellular, wireless, Bluetooth, or comparable signals to identify persons or reconstruct their movements;
  - (5) commercial personal-location histories or equivalent tracking information obtained from data brokers, advertising networks, applications, connected vehicles, or other commercial sources; or
  - (6) automated aggregation of unrelated administrative, commercial, online, or surveillance records into generalized dossiers concerning individuals' movements, associations, lawful activities, or sensitive personal characteristics.
- (b) The City shall not use automated surveillance analysis to infer a person's race, ethnicity, religion, political affiliation, health condition, sexual orientation, or comparable sensitive characteristic, or to assign a generalized suspicion or risk score based on lawful activities or associations.
- (c) The City shall not access, request, purchase, knowingly receive, or use Non-Hit Observation histories to determine whether, when, or where a vehicle was previously observed.
- (d) The City shall not process previously recorded video or other archived information to obtain a capability prohibited by this section.

- (e) These prohibitions apply to live operation and retrospective analysis. Immediate deletion does not authorize Facial Detection, Facial Recognition, or another independently prohibited practice.
- (f) Consent, public availability of information, a vendor's characterization of its product, or the existence of an active investigation does not independently create an exception to this section.
- (g) Historical ALPR Systems are prohibited at every location and on every platform used by or on behalf of the City, including City Entry Points, moving or parked law enforcement vehicles, trailers, and portable equipment. No deployment authorization in Section 74-41 permits a Historical ALPR System.
- (h) These prohibitions apply whether a function uses artificial intelligence, machine learning, computer vision, conventional software, or a combination of methods. Use of artificial intelligence to perform plate reading and Hotlist comparison is permitted only within a compliant Hit-Only ALPR System and does not authorize facial analysis, personal tracking, profiling, prohibited aggregation, or retention of Non-Hit Observations.

**Sec. 74-40. Requirements for Hit-Only ALPR Systems.**

- (a) An authorized ALPR System shall compare observations against an eligible Hotlist locally, within the City-controlled capture device or dedicated local processing equipment.
- (b) Non-Hit Observation data shall:
  - (1) remain only in volatile memory necessary for the comparison;
  - (2) be discarded immediately upon completion or failure of the comparison, and no later than one second after initial capture;
  - (3) never be written to persistent storage; and
  - (4) never be transmitted outside that local processing environment.
- (c) The requirements of subsection (b) apply to images, extracted plate information, derivatives, buffers, diagnostic records, swap files, crash dumps, telemetry, backups, and other recoverable representations.
- (d) Network interruption, an unavailable or outdated Hotlist, software failure, or an incomplete comparison shall not authorize storage or queuing for later processing. A system unable to comply shall cease capturing observations.
- (e) Non-Hit Observation data shall not be used for analytics, product development, advertising, model training, testing, or other secondary purposes.
- (f) The system may retain operational totals and equipment-health information only if they cannot reasonably identify a person or vehicle or reconstruct an individual observation.
- (g) Live interfaces, screenshots, exports, or operator notes shall not be used to preserve Non-Hit Observation data that the system itself is prohibited from retaining.
- (h) Candidate Alerts and Verified Hits shall be handled exclusively under Section 74-43.

**Sec. 74-41. Deployment at City Entry Points and mobile patrol use.**

- (a) Except for mobile patrol use expressly authorized by subsection (i), the City shall operate an ALPR System only at a City Entry Point expressly authorized in Exhibit A. Every authorized deployment shall use a Hit-Only ALPR System.
- (b) The entry-point restriction applies to fixed, stationary, portable, trailer-mounted, and parked vehicle-mounted systems. A vehicle-mounted system is exempt from that placement restriction only while operated in compliance with subsection (i).
- (c) Each authorized site shall identify:
  - (1) the public roadway and municipal-boundary crossing;

- (2) installation coordinates;
  - (3) the authorized capture area, lanes, and direction of observation;
  - (4) the maximum number of devices; and
  - (5) the necessary property, roadway, and right-of-way permissions.
- (d) Equipment operated at a City Entry Point shall be positioned and configured to observe vehicles crossing the municipal boundary. It shall not capture unrelated neighborhood traffic, parking activity, or traffic traveling solely within the City.
  - (e) An Interstate Highway 35 entrance ramp, exit ramp, frontage road, or other roadway qualifies only if it independently satisfies this section and is listed in Exhibit A.
  - (f) Addition of a site, expansion of its capture area, an increase in its authorized device count, or a material relocation requires amendment of Exhibit A by ordinance.
  - (g) A boundary change does not automatically authorize a new site. A site that no longer qualifies as a City Entry Point shall cease operation.
  - (h) No location is authorized merely because the City has permission to install equipment there.
  - (i) A Hit-Only ALPR System installed on a moving law enforcement vehicle may operate during ordinary lawful patrol within the City without designation in Exhibit A. Brief stops required by traffic signals, congestion, or safe driving do not convert ordinary patrol into stationary deployment. Scanning shall cease when the vehicle is parked or stationed, unless it is operating at an authorized City Entry Point in compliance with subsections (a) through (h). A vehicle shall not be parked, staged, repeatedly circled, or otherwise deployed to maintain a substantially fixed observation point or circumvent the entry-point restriction. This subsection does not authorize continuous following of a particular vehicle solely to record its movements.
  - (j) Mobile patrol systems remain subject to every applicable Hotlist, processing, deletion, access, sharing, vendor, audit, and prohibited-use requirement of this article. Mobile operation creates no exception for historical retention or prohibited facial, biometric, or other personal-data surveillance.

#### **Sec. 74-42. Hotlist eligibility and administration.**

- (a) A vehicle may be included on a Hotlist only if it is:
  - (1) currently reported stolen;
  - (2) supported by documented facts establishing a current connection to a person subject to an active criminal arrest warrant;
  - (3) specifically identified in an active missing-person or endangered-person alert;
  - (4) specifically identified for prospective observation in a valid warrant or court order issued under independently applicable law; or
  - (5) supported by specific, articulable facts establishing its material connection to a specified criminal offense and the necessity of a prospective alert in an active investigation.
- (b) Each entry shall identify the complete plate number, issuing jurisdiction, applicable eligibility category, source, supporting facts, case or incident number, responsible officer, activation time, and expiration time.
- (c) A case number, generalized investigative interest, presence in a particular area, or association with another person does not alone establish eligibility.
- (d) A locally initiated entry requires documented supervisory approval before activation. An imported entry requires confirmation that its source and category satisfy this article.

- (e) Wildcard entries, bulk registration lists, and entries based solely on vehicle color, make, model, or other general characteristics are prohibited.
- (f) Each entry shall expire within 30 days unless renewed following documented review. Entries shall be removed earlier when their qualifying basis ends.
- (g) An entry under subsection (a)(5) shall not remain active for more than 90 cumulative days concerning substantially the same investigation unless continued observation is specifically authorized by a valid warrant or court order issued under independently applicable law.
- (h) Changing a case number, temporarily removing an entry, or transferring responsibility does not restart the cumulative period.
- (i) Hotlist sources shall be refreshed at least once every 24 hours. A cancellation or disqualifying change received by the City shall be implemented within one hour. Entries whose required validation is unavailable shall be disabled.
- (j) No entry shall be based on protected characteristics, lawful expression, lawful association, or the exercise of constitutional rights. Those characteristics and activities shall not substitute for independently documented eligibility.
- (k) Hotlist authorization operates prospectively. It does not authorize retrieval of observations made before activation.

#### **Sec. 74-43. Candidate Alerts and Verified Hits.**

- (a) Candidate Alerts may be retained temporarily for verification, but no longer than 60 minutes unless preservation is required under Section 74-50.
- (b) Verification shall confirm:
  - (1) the plate characters and issuing jurisdiction;
  - (2) that the entry existed before capture;
  - (3) that the underlying warrant, report, alert, or investigative basis remains active; and
  - (4) that the entry satisfies Section 74-42.
- (c) A false or unverified alert shall be deleted upon that determination or expiration of the verification period, subject to Section 74-50.
- (d) An automated alert does not independently authorize a stop, search, detention, arrest, or other enforcement action. Personnel shall confirm the alert and establish the legal basis applicable to the proposed action.
- (e) A Verified Hit shall be deleted within 72 hours unless a supervisor documents its specific evidentiary or operational necessity and assigns it to an identified case or incident. Further retention shall comply with the applicable records schedule and Section 74-50.
- (f) Retained Verified Hits shall be accessible only to personnel assigned an authorized case, supervisory, audit, records-management, or legal function. Each access and export shall be logged.
- (g) A retained hit shall not be placed in a generally searchable movement-history database or searched across unrelated cases. Use in another case requires separately documented relevance and supervisory approval.
- (h) Retention shall be limited to information necessary to document the qualifying observation. Images and derivatives shall exclude or mask unrelated vehicles and persons before persistent storage, except to the extent preservation is legally required.
- (i) Records preserved under this section shall not be used for commercial purposes, advertising, product development, or model training.

#### **Sec. 74-44. Texas-only voluntary interagency sharing.**

- (a) Except as required by Section 74-50, the City shall disclose identifiable Covered Data to another governmental entity only if that entity is an Eligible Texas Agency and all requirements of this section are met.
- (b) The City shall not voluntarily provide Covered Data, direct access, search access, alerts, reports, or information derived from Covered Data to:
  - (1) an agency of another state or country;
  - (2) a federal agency, including a federal office physically located in Texas;
  - (3) a nationwide, multistate, or international sharing network; or
  - (4) a task force, fusion center, contractor, or intermediary that provides access to an entity excluded by this subsection.
- (c) Each permitted disclosure shall:
  - (1) concern a specified incident or investigation;
  - (2) be limited to relevant Verified Hit information lawfully retained;
  - (3) receive documented supervisory approval; and
  - (4) be governed by an executed agreement satisfying this article.
- (d) Standing access to the City's observation records, unrestricted database access, automatic interagency feeds, and bulk transfers are prohibited.
- (e) Each recipient agreement shall prohibit:
  - (1) disclosure or access outside the permitted recipient agency;
  - (2) contribution to a federal, national, multistate, commercial, or otherwise prohibited database;
  - (3) use for an unrelated purpose;
  - (4) model training or product development; and
  - (5) retention beyond the agreed period, except where controlling law requires otherwise.
- (f) Further disclosure to another Eligible Texas Agency requires separate City approval and an agreement with the additional recipient. Voluntary onward disclosure to an excluded entity is prohibited.
- (g) The recipient shall maintain access records, permit compliance review, report unauthorized access or disclosure within 24 hours after discovery, and provide disposition certifications.
- (h) The City shall not make a voluntary disclosure when it knows or reasonably should know that the recipient cannot comply with these restrictions.
- (i) Use of a Texas agency as an intermediary does not authorize prohibited disclosure. Participation in a network is prohibited if it automatically transmits City observations or derived alerts to excluded entities.
- (j) Receipt of an otherwise eligible Hotlist does not authorize returning City observation information to its source. Any return transmission remains subject to this section.
- (k) Necessary vendor processing is governed by Section 74-47 and does not authorize the vendor to use the information independently or disclose it to another customer or agency.

#### **Sec. 74-45. Public disclosure of recipients and sharing activity.**

- (a) The City shall maintain a publicly accessible **Surveillance Data Sharing Register** on its official website. Access shall not require registration, payment, or a public-information request.

- (b) Before voluntarily disclosing Covered Data to an agency or granting a vendor or subcontractor access, the City shall publish:
  - (1) the recipient's full legal name;
  - (2) its governmental jurisdiction, if applicable;
  - (3) its role as recipient agency, contractor, hosting provider, or subcontractor;
  - (4) the categories of information it may receive or access;
  - (5) the specific authorized purposes;
  - (6) the method and scope of access;
  - (7) the applicable retention and deletion requirements;
  - (8) restrictions on onward disclosure;
  - (9) the agreement's approval, commencement, and expiration dates; and
  - (10) a copy of the governing agreement and material amendments, subject to subsection (h).
- (c) Descriptions such as "law enforcement partners," "authorized agencies," "Texas agencies," or "service providers" shall not substitute for naming the actual recipient.
- (d) Publication and an agreement do not independently authorize disclosure prohibited elsewhere in this article.
- (e) No later than the fifteenth day of each month, the City shall publish an activity report for the preceding month identifying:
  - (1) every entity that actually received or accessed Covered Data;
  - (2) the date of each disclosure or access event;
  - (3) the categories and quantity of records disclosed or accessed;
  - (4) the general purpose and authorizing City office;
  - (5) whether disclosure was voluntary or legally compelled;
  - (6) any known onward disclosure and the identity of the subsequent recipient, when disclosure of that identity is lawful; and
  - (7) any suspension, termination, violation, or corrective action affecting the recipient.
- (f) When no sharing or external access occurred, the City shall publish an affirmative statement to that effect.
- (g) Additions, suspensions, terminations, and material changes to recipient arrangements shall be posted within seven calendar days. New recipients shall nevertheless be listed before voluntary disclosure or access begins.
- (h) The register shall not publish vehicle plates, biometric information, precise individual movements, or other underlying personal surveillance information. The City shall redact information that controlling law prohibits it from disclosing and identify the legal basis for each redaction when legally permissible. Contractual confidentiality alone does not justify withholding information required by this section.
- (i) If a binding legal requirement temporarily prohibits identifying a recipient or disclosure, the City shall publish the otherwise required information when that restriction expires. It shall disclose the existence and legal basis of the restriction earlier when lawful.
- (j) The register shall include legally compelled disclosures to otherwise excluded recipients, subject to subsection (i). Such reporting does not characterize those disclosures as voluntarily authorized.
- (k) The register shall be available in an accessible web format and a downloadable, machine-readable format. Prior versions and monthly reports shall remain publicly available for at least five years, or longer when required by law.

## **Sec. 74-46. Ordinary municipal functions and narrow exceptions.**

- (a) This article does not prohibit collection and maintenance of information reasonably necessary for ordinary municipal services, including utility billing, payroll, purchasing, permitting, emergency response, and case or incident administration.
- (b) Ordinary administrative collection shall be limited to information reasonably necessary for the identified service or legal duty. It shall not be repurposed to perform a practice prohibited by Section 74-39.
- (c) This article does not prohibit ordinary photographs, body-camera recordings, dash-camera recordings, facility-security recordings, or human review of particular evidence lawfully obtained. It does prohibit applying a prohibited identification, tracking, or aggregation function to those materials.
- (d) This article does not prohibit legally required booking or identification records, or lawful fingerprint and DNA examination of evidence associated with a specified investigation. This subsection does not authorize Facial Detection, Facial Recognition, or generalized biometric monitoring of the public.
- (e) Cybersecurity logs reasonably necessary to protect City systems may be maintained for that purpose. They shall not be used to construct unrelated records of the public's movements or associations.
- (f) None of these exclusions authorizes acquisition of a prohibited commercial tracking product, a prohibited surveillance database, or information produced through a prohibited search.
- (g) The exclusions in this section do not create independent authority to collect, search, retain, or disclose information otherwise restricted by law.
- (h) Facial Detection may be used solely to locate faces for blurring or redaction in material otherwise lawfully held or processed, including compliance with Section 74-43(h). This exclusion permits no identification, matching, reidentification, tracking, demographic or behavioral inference, or separate record of a person's presence. Processing shall remain local, retain no biometric template or reusable identifier, and discard face-location coordinates immediately after redaction. The exclusion authorizes neither additional collection nor retention, and does not permit a retained face-detection index or log.
- (i) Notwithstanding subsection (h) and Section 74-39(a)(2), (a)(3), and (d), solely to perform the particularized comparison authorized by this subsection, Facial Detection necessary for Facial Recognition, and Facial Recognition itself, may be used only when every following condition is satisfied. This subsection supplies no independent authority to obtain a warrant, compel assistance, collect evidence, or access reference material.
  - (1) The use concerns a specified criminal investigation and is expressly authorized in advance by a valid, particularized search warrant or court order issued under independently applicable law by a court of competent jurisdiction. The judicial authorization shall identify the investigation, the specified images or recordings, the bounded reference collection, the investigative purpose, the authorized comparisons, and the period of use. A general authorization to investigate or use technology is insufficient.
  - (2) The images or recordings shall have been lawfully obtained before the request for judicial authorization. The reference collection shall be lawfully accessible for the specified comparison and identified in the authorization. The City shall not create or expand a generalized facial gallery, use a commercial collection assembled by indiscriminate scraping, or acquire material prohibited elsewhere in this article.
  - (3) The City Attorney shall confirm the legal authority and scope, and a supervisor shall approve a written execution plan stating the case number, authorized personnel, comparison limits, and deletion schedule before processing begins. Authorization under this article expires when the judicial authorization expires or 30 days after issuance, whichever occurs first. Further processing requires a new or renewed particularized judicial authorization and renewed written approval.
  - (4) Processing shall be confined to the authorized comparison of specified existing evidence. It shall not include live or prospective public scanning, crowd monitoring, ongoing tracking, searches to identify

persons engaged in lawful political or religious activity as such, inference of sensitive characteristics, or generalized profiling. The exception to Section 74-39(a)(3) extends only to the specified facial comparison and does not authorize linking successive location observations or following a person across recordings. Section 74-39(a)(4) through (6) and (b) remain controlling.

- (5) An authorized, trained person shall review each proposed match and document independent corroboration. An automated result shall not alone establish identity or supply the sole basis for a stop, search, arrest, or other adverse action. The City shall record the software and version, threshold settings, reference source, operator, time, purpose, and verification outcome for audit, without creating a searchable index of nonmatching persons.
- (6) Nonmatching templates, derived face coordinates, and other transient comparison artifacts shall be discarded immediately after the authorized comparison. Copies of underlying source evidence and material legally required for disclosure, preservation, or review shall be handled under Section 74-50. Confirmed results may be retained only as necessary for the identified case and applicable records duties; they shall not be repurposed into a general biometric or movement database.
- (7) Every use shall comply with the access, Texas-agency sharing, public recipient register, vendor, audit, and enforcement requirements of this article. The public annual report shall identify the number of applications, authorizations, uses, verified matches, known false matches, and compliance failures, withholding only information lawfully confidential. Vendors shall have no independent reuse or model-training rights.
- (8) This subsection creates no exception for Historical ALPR Systems, retention or retrieval of Non-Hit Observations, prohibited personal tracking or dossiers, or voluntary sharing with an ineligible recipient. A judicial authorization that merely permits a broader activity does not expand this exception. Compelled legal duties are addressed separately in Section 74-50.

#### **Sec. 74-47. Contracts, vendors, and technical controls.**

- (a) Before operation, each regulated system shall be governed by enforceable written terms requiring compliance with this article.
- (b) Those terms shall bind the vendor and all subcontractors and shall require:
  - (1) collection, processing, access, and retention limited to expressly authorized functions;
  - (2) prohibition of independent use, sale, licensing, advertising, and model training using Covered Data;
  - (3) prohibition of access by other customers or unauthorized agencies;
  - (4) technical separation sufficient to prevent cross-customer searches and prohibited sharing;
  - (5) disclosure and approval of subcontractors before access;
  - (6) City and independent-auditor access sufficient to verify compliance;
  - (7) notice within 24 hours after discovery of unauthorized retention, access, or disclosure;
  - (8) approval and verification before material changes to data flows or regulated functionality;
  - (9) return or lawful disposition of information when service ends; and
  - (10) suspension and termination rights for material noncompliance.
- (c) Vendor support, troubleshooting, security monitoring, and product improvement shall not create exceptions to non-hit deletion or prohibited-use requirements.
- (d) A service shall not be used if the vendor cannot demonstrate compliance. A contractual promise alone does not establish technical compliance.

- (e) A vendor shall not disclose Covered Data to an excluded agency voluntarily. The contract shall require notice of legally compelled disclosure and an opportunity for lawful review or objection when legally permitted.
- (f) The City shall not transfer a noncompliant deployment to another entity while continuing to fund, direct, access, or obtain its prohibited outputs.

**Sec. 74-48. Verification, auditing, and reporting.**

- (a) Before activation, and after a material change affecting compliance, an independent qualified reviewer shall verify the system's relevant functions, data flows, storage behavior, access controls, and sharing configuration.
- (b) Testing shall include:
  - (1) normal operation;
  - (2) network interruption and unavailable Hotlists;
  - (3) logs, caches, backups, and remote services;
  - (4) Candidate Alert expiration and false-positive handling;
  - (5) recipient and subcontractor access;
  - (6) geographic capture restrictions and compliance of mobile patrol deployments with Section 74-41(i); and
  - (7) the absence of prohibited facial-detection, facial-recognition, biometric, AI profiling, or personal-tracking functions in operation, and documented compliance of every use under Section 74-46(i) with its judicial authorization and all limiting conditions.
- (c) The City shall conduct monthly compliance reviews and obtain independent quarterly audits. At least one quarterly audit each year shall include technical testing under subsection (b).
- (d) Audit records shall document Hotlist additions, approvals, renewals, removals, retained-hit access, exports, disclosures, configuration changes, and compliance incidents. They shall not create records of Non-Hit Observations.
- (e) Within 30 days after completion of each independent audit, the City shall publish its findings, identified deficiencies, and corrective-action status, subject to legally required redactions.
- (f) The City Manager and Chief of Police shall submit an annual compliance report to City Council identifying equipment, authorized sites, mobile patrol systems, expenditures, recipients, verified outcomes, false alerts, complaints, violations, and corrective actions.
- (g) Compliance audits and reports shall address each requirement separately. A general certification that a system is "privacy compliant" is insufficient.

**Sec. 74-49. Enforcement and prohibition on circumvention.**

- (a) Upon substantiation of prohibited collection, retention, access, disclosure, or deployment, the City Manager shall immediately suspend the affected function. If it cannot be reliably isolated, the affected system shall be suspended.
- (b) Operation shall not resume until corrective action is completed and independently verified. The City shall publish the suspension and resumption status subject to legally required redactions.
- (c) The City shall maintain a public complaint process. Complaints shall be reviewed by an official or reviewer who did not participate in the challenged conduct.
- (d) Intentional or negligent violations shall be addressed under applicable personnel rules, contractual remedies, and law. This article does not displace required employment procedures.

- (e) No person acting for the City shall obtain indirectly a capability, search, or disclosure prohibited directly. This prohibition includes requests through another agency, account, task force, vendor, data broker, or private person.
- (f) Prohibited information remains prohibited when delivered as a tip, narrative, screenshot, analytical conclusion, or other derivative instead of its underlying records.
- (g) Upon recognizing unsolicited information as the product of a prohibited practice, personnel shall discontinue operational use, restrict access, and refer it for legal and records-management review under Section 74-50.
- (h) Product renaming, artificial separation of system components, rotation of equipment, deletion after a short retention period, or use of temporary or free services does not excuse noncompliance.
- (i) No City official may waive these restrictions by administrative policy, grant acceptance, contract, or interlocal agreement.
- (j) This article creates administrative and contractual requirements. It does not create a new criminal offense, independently determine admissibility of evidence, or alter remedies established by controlling law.

**Sec. 74-50. Controlling law and required preservation or disclosure.**

- (a) Nothing in this article requires destruction of information that controlling law requires the City to preserve, or refusal to comply with a binding legal duty or enforceable court order.
- (b) An exception under this section shall extend only to the information and conduct actually required. A law or order that merely permits an activity does not independently exempt that activity from this article.
- (c) The City Attorney shall document the specific authority, affected information, required conduct, scope, and duration of an exception. If immediate compliance is legally required, documentation shall follow within three business days.
- (d) Information preserved solely because of a legal hold or other preservation duty shall be segregated from ordinary operational searches. Access shall be limited to fulfilling the legal obligation, responding to authorized proceedings, and necessary records administration.
- (e) Preservation of existing information does not independently authorize continued collection, renewed tracking, broader searches, or voluntary disclosure.
- (f) Required preservation shall be reviewed at least every 90 days. Information shall be disposed of when lawful and required by the applicable schedule.
- (g) A vendor preference, grant condition, general cooperation request, or voluntary sharing agreement does not alone establish legal compulsion.
- (h) Before a compelled disclosure outside the recipients permitted by Section 74-44, the City Attorney shall review its validity and scope when legally and practically possible. The City shall disclose only what is required and seek available protective measures when appropriate.
- (i) Required disclosures shall be reported under Section 74-45 to the extent publication is lawful.

**SECTION 2. EXISTING SYSTEMS AND IMPLEMENTATION.**

- (a) Beginning on the effective date, the City shall not enter into a new agreement, renewal, expansion, or trial authorizing a practice prohibited by this Ordinance.
- (b) Beginning on the effective date, the City shall suspend prohibited functions and unauthorized sharing. Equipment may remain installed temporarily while inactive.

- (c) Within 30 days, the City Manager shall inventory:
  - (1) regulated devices, software, subscriptions, and accounts;
  - (2) Facial Detection, Facial Recognition, other biometric capabilities, and artificial-intelligence functions used for surveillance;
  - (3) personal-device tracking and commercial personal-data services;
  - (4) data holdings, integrations, and search capabilities;
  - (5) vendors, subcontractors, recipient agencies, and sharing networks; and
  - (6) applicable contracts, grants, legal holds, and retention obligations.
- (d) Within 30 days, the City shall establish the public register required by Section 74-45, identifying existing arrangements and their active, suspended, or terminated status.
- (e) Existing data shall be reviewed for lawful disposition. Records subject to mandatory retention or preservation shall be handled under Section 74-50. The City shall seek deletion or return of previously shared copies to the extent legally and contractually available and document the results.
- (f) Within 90 days, noncompliant equipment shall be removed from service or converted and independently verified before reactivation. No fixed or stationary ALPR shall operate unless its site is authorized in Exhibit A. A mobile patrol ALPR may operate only in compliance with Section 74-41(i) and (j).
- (g) The City shall pursue lawful modification, termination, or nonrenewal of inconsistent contracts. Contract-administration or equipment-removal deadlines do not extend the suspension requirement.
- (h) Within 120 days, the City Manager shall provide City Council with a public implementation report identifying completed actions, remaining legal or contractual issues, and the operational status of each regulated system.

### **SECTION 3. REPEALER.**

Conflicting ordinances and portions of ordinances are repealed to the extent of the conflict. City administrative policies and agreements shall be brought into conformity with this Ordinance, subject to controlling law.

### **SECTION 4. SEVERABILITY.**

If a court of competent jurisdiction holds a provision or application of this Ordinance invalid or unenforceable, the remaining provisions and applications shall remain effective to the extent they can operate independently. The City Council declares that it would have adopted those independently operative provisions.

### **SECTION 5. OPEN MEETINGS.**

For action taken by the City Council concerning this Ordinance, the Council finds that each meeting at which it took such action was open to the public and noticed as required by the Texas Open Meetings Act. Adoption by initiative election shall be documented through the applicable election and canvass procedures.

### **SECTION 6. EFFECTIVE DATE.**

If adopted by the City Council, this Ordinance takes effect upon completion of the adoption, execution, filing, recording, and publication requirements applicable under the City Charter and controlling law. If adopted by the qualified voters through the initiative process, it takes effect as provided by Article VI, Section 6.07 of the City Charter and controlling law. The implementation periods in Section 2 run from the applicable effective date. The execution and certification blocks shall be conformed to the method of adoption before final petition circulation or Council introduction.

**PASSED AND APPROVED** on first reading this \_\_\_\_ day of \_\_\_\_\_, 2026.

**PASSED AND APPROVED** on second and final reading this \_\_\_\_ day of \_\_\_\_\_, 2026.

**CITY OF NEW BRAUNFELS, TEXAS**

\_\_\_\_\_  
Mayor

**ATTEST:**

\_\_\_\_\_  
City Secretary

**APPROVED AS TO FORM:**

\_\_\_\_\_  
City Attorney

## EXHIBIT A — AUTHORIZED CITY ENTRY POINTS

Each approved site shall be accompanied by a map showing the incorporated municipal boundary and the permitted capture area.

| Site ID | Roadway and boundary crossing | Installation coordinates | Authorized lanes and directions | Maximum devices | Permissions |
|---------|-------------------------------|--------------------------|---------------------------------|-----------------|-------------|
| —       | To be adopted by City Council | —                        | —                               | —               | —           |

**No fixed or stationary site is authorized until its entry and corresponding map are adopted by ordinance. Mobile patrol use under Section 74-41(i) does not require a site entry in this exhibit.**