TOWN OF APEX, NORTH CAROLINA

ORDINANCE NO. _____

AUTOMATED LICENSE PLATE READER GOVERNANCE ORDINANCE

An Ordinance Establishing Civilian Governance, Privacy Protections, Transparency Requirements, Operational Restrictions, and Enforceable Accountability Standards for Automated License Plate Reader Systems Within the Town of Apex

Enacted pursuant to N.C. Gen. Stat. §§ 160A-174, 160A-175, and Chapter 20, Article 3D of the North Carolina General Statutes

Prepared by DeFlock Apex
deflockapex.org

Draft: June 2026

Article I — Legislative Findings and Purpose

Section 1.01 — Statutory Authority

This ordinance is enacted pursuant to the general police power of the Town of Apex under N.C. Gen. Stat. § 160A-174, the ordinance-making authority under N.C. Gen. Stat. § 160A-175, and the regulatory framework for automatic license plate reader systems established by N.C. Gen. Stat. Chapter 20, Article 3D (§§ 20-183.30 through 20-183.33). Nothing in this ordinance shall be construed to conflict with state law. Where this ordinance imposes stricter requirements than state law within the scope of local authority, the stricter local requirement shall govern.

Section 1.02 — Findings

The Town Council finds that:

(1) Automated License Plate Reader ("ALPR") systems create searchable historical records of vehicle movement and therefore implicate privacy, civil liberties, and constitutional concerns distinct from ordinary public observation. The Supreme Court of the United States recognized in *Carpenter v. United States*, 585 U.S. 296 (2018), that comprehensive records of a person's movements implicate expectations of privacy, even when generated from information exposed to third parties.

(2) ALPR systems possess capabilities extending beyond simple image capture, including: historical searchability of vehicle movement across time and geography; metadata analysis including vehicle make, model, color, body type, and distinguishing characteristics; network-based sharing with hundreds or thousands of agencies through vendor-operated platforms; real-time alerting on designated watch lists; AI-assisted identification functions including "Vehicle Fingerprint" matching; and integration into broader surveillance ecosystems through federated search and cross-jurisdictional data pooling.

(3) Public records obtained by Town residents in 2026 reveal that the Apex Police Department's Flock Safety system maintained active data-sharing relationships with 994 organizations as of March 2026 (186 in-state, 808 out-of-state, and 2 federal), growing to 1,070 organizations by April 2026 (195 in-state, 875 out-of-state). These sharing relationships were established without public notice, public hearing, or recorded Council vote.

(4) The same public records reveal a discrepancy between the Chief of Police's January 29, 2025 statement to Council that Apex does not share data with federal entities ("no federal entities, hard stop") and the March 2026 sharing snapshot showing two federal sharing relationships. This discrepancy remains unexplained as of the date of this ordinance.

(5) Public records further show that Apex PD received and maintained access to private surveillance camera networks (including MacGregor Downs) and outside hot lists (including from WakeMed Campus PD, Whitestown IN PD, and Brevard County FL SO), without public disclosure or Council authorization.

(6) Flock Safety's vendor platform architecture enables sharing through a nationwide network of over 80,000 connected cameras. On May 14, 2026, the Federal Bureau of Investigation published a Request for Proposals seeking up to $36 million for nationwide access to ALPR data, with Flock Safety identified as one of the few vendors capable of fulfilling the contract. This federal procurement underscores the risk that locally collected ALPR data may become accessible to federal agencies through vendor-mediated channels without direct local consent.

(7) Neighboring North Carolina jurisdictions, including Chatham County (April 2026) and Pittsboro (May 2026), have ended their Flock Safety contracts following sustained resident advocacy and governance concerns.

(8) N.C. Gen. Stat. § 20-183.31(a) requires law enforcement agencies using ALPR systems to adopt written policies governing their use, including data retention, sharing, training, access, auditing, and oversight. The Town Council finds that the policy requirements of state law are necessary but insufficient, and that local governance standards must provide additional transparency, accountability, and civilian oversight.

(9) The Town recognizes the risk of surveillance expansion, function creep, indefinite data retention within statutory limits, regional or federal sharing through vendor platforms, and hybrid public-private surveillance systems that blur public accountability.

(10) Investigative usefulness alone is insufficient justification for unrestricted or inadequately governed mass collection of vehicle movement data. Independent research published in the Journal of Experimental Criminology has found no significant deterrent effect from ALPR systems. In Piedmont, California, less than 0.3% of ALPR "hits" translated into an actionable investigative lead.

Section 1.03 — Purpose

The purpose of this ordinance is to:

(a) Establish strict civilian control over ALPR systems operated by or on behalf of the Town;

(b) Ensure compliance with North Carolina law while imposing stricter local safeguards where authorized under the Town's police power;

(c) Prevent unauthorized surveillance expansion and function creep;

(d) Restrict data retention, sharing, and external access below state-law maximums;

(e) Ensure public transparency, meaningful oversight, and enforceable accountability;

(f) Preserve constitutional protections and civil liberties, including Fourth Amendment rights as interpreted in *Carpenter v. United States*;

(g) Require democratic authorization before any new surveillance technology is deployed, expanded, or renewed;

(h) Establish enforceable operational restrictions, violation consequences, and citizen redress mechanisms.

Article II — Definitions

Section 2.01 — Automated License Plate Reader ("ALPR")

Any system capable of capturing, processing, storing, searching, analyzing, matching, alerting upon, or sharing license plate data or associated vehicle metadata, whether fixed, mobile, or portable, and whether operated by law enforcement, a vendor, a private entity, or any combination thereof. This definition includes but is not limited to systems marketed as "license plate recognition," "vehicle intelligence," or "public safety operating systems" that incorporate ALPR functionality.

Section 2.02 — Vehicle Metadata

Any data associated with or derived from an ALPR capture, including: license plate number and state of registration; vehicle make, model, color, year, and body type; timestamp and geolocation of capture; direction of travel; vehicle distinguishing characteristics (including damage, accessories, decals, or modifications); and any analytical or inferential metadata generated by AI or algorithmic processing, including but not limited to "Vehicle Fingerprint" data or similar vehicle-identification technologies.

[NEW] "Vehicle Fingerprint" or equivalent vehicle-identification technology that identifies or tracks a specific vehicle by physical characteristics independent of its license plate number is not authorized as standard vehicle metadata. Passive or continuous operation of Vehicle Fingerprint is governed by Section 8.01. Limited investigative use of Vehicle Fingerprint is governed by Section 6.01(g).

Section 2.03 — Surveillance Expansion Features

Any functionality beyond license plate capture and database comparison, including but not limited to: facial recognition; biometric analysis; behavioral analytics; predictive policing algorithms; live video monitoring or streaming (including "LiveView" or equivalent functionality); audio detection (including gunshot detection integrated with ALPR infrastructure); AI-based identity inference; persistent tracking or movement reconstruction; cross-jurisdiction search federation; real-time integrated surveillance platforms; and any feature that enables identification of individuals (as distinct from vehicles) or prediction of future behavior.

Section 2.04 — Sharing

Any arrangement, whether active or passive, direct or indirect, manual or automated, by which ALPR data collected by or on behalf of the Town is made searchable, accessible, queryable, viewable, exportable, downloadable, or otherwise available to any entity other than authorized Town personnel. This includes but is not limited to: vendor-operated nationwide or statewide search networks; federated search systems; data pooling or mirroring arrangements; API access; standing interagency access agreements; hot list sharing; camera sharing (including receiving search access to privately owned cameras); and any configuration of vendor platform settings that enables external access.

Section 2.05 — Hot List

Any list of license plates designated for automated alerting, whether created by the Town, received from another agency, received from a vendor, or compiled from any external source. Hot lists include but are not limited to stolen vehicle lists, wanted person lists, missing person lists, custom watch lists, and any list that triggers real-time notification when a matching plate is captured.

Section 2.06 — Private Camera Network

Any ALPR or surveillance camera system owned, operated, or maintained by a private entity (including homeowners' associations, businesses, property management companies, or private security firms) that is

connected to, shared with, or made searchable by law enforcement through a vendor platform or direct integration.

Section 2.07 — Authorized Governing Bodies

The only entities authorized to establish, amend, renew, suspend, or terminate ALPR policy are the Apex Town Council, the Mayor of Apex, and the Citizen ALPR Oversight Committee established herein. The Apex Police Department ("APD") shall possess no independent policymaking authority regarding ALPR governance. APD retains authority to establish internal operational procedures consistent with this ordinance, subject to Committee review and audit.

Article III — Governance and Oversight

Section 3.01 — Civilian Governance

ALPR systems shall remain under civilian authority at all times. APD shall function solely as a system operator, investigative user, and compliance participant. APD shall not independently establish policy, expand capabilities, authorize sharing, alter retention rules, modify deployment scope, accept or approve share requests from other agencies, or configure vendor platform settings that affect data access, sharing, or retention.

Section 3.02 — Citizen ALPR Oversight Committee

(a) Establishment and Composition

A permanent Citizen ALPR Oversight Committee (the "Committee") shall be established consisting of seven (7) members appointed by the Town Council. Members shall serve staggered three-year terms. No member shall serve more than two consecutive terms. At least one member shall possess expertise in privacy law, civil liberties, or data governance. At least one member shall possess expertise in information security or technology. No member shall be a current employee of the Town, any law enforcement agency, or any ALPR vendor. No member shall have a financial interest in any surveillance technology vendor.

(b) Powers and Duties

The Committee shall: review all quarterly and annual compliance reports; review all audit findings, including independent annual audits; review all disciplinary findings related to ALPR misuse; conduct or commission public hearings on ALPR policy matters; review and make recommendations on all proposed policy amendments, contract renewals, and deployment changes; review and approve or reject all proposed sharing arrangements before they take effect; monitor operational compliance on an ongoing basis; issue public recommendations to Council; receive and investigate citizen complaints; and maintain a public record of all proceedings.

(c) Immediate Suspension Authority

The Committee may recommend immediate operational suspension to the Town Council upon evidence of misuse, material noncompliance, unauthorized sharing, or any violation described in Article IX. Upon such recommendation, Council shall convene within fourteen (14) calendar days to consider suspension.

(d) Access and Resources

The Committee shall have access to all ALPR audit logs, system configuration records, sharing settings, vendor communications, and compliance documentation. The Committee shall have independent access to legal counsel, funded by the Town. The Town shall provide reasonable staff support and an annual operating budget sufficient for the Committee to fulfill its duties, including the cost of independent audits.

Section 3.03 — Independent Privacy Advocate

The Town shall appoint an Independent Privacy Advocate or retain outside privacy counsel. The Privacy Advocate shall be selected by the Committee from a shortlist of qualified candidates and may only be removed for cause by a two-thirds vote of the Committee. The Privacy Advocate shall: review compliance with this ordinance and applicable state and federal law; evaluate surveillance risks, including risks of function creep and civil liberties impact; issue annual findings to the Committee and Council; advise Council regarding privacy implications, legal exposure, and constitutional considerations; and review all proposed vendor contracts, renewals, and amendments for privacy and civil liberties implications before Council action.

Section 3.04 — Surveillance Impact Report

Before the Town Council votes on any ALPR deployment, expansion, renewal, vendor change, or functional upgrade, the Committee and Privacy Advocate shall prepare and publish a Surveillance Impact Report. The report shall include: a description of the proposed technology and all of its capabilities, including capabilities not proposed for activation; an analysis of the privacy and civil liberties implications, including any disparate impact on communities of color, immigrant communities, low-income communities, or other vulnerable populations; an analysis of the proposed data retention, sharing, and access arrangements; an assessment of alternative approaches that could achieve the stated public safety objective with less surveillance; the total cost of the proposed technology, including direct costs, staff time, oversight costs, and legal exposure; and a recommendation for or against approval, with stated reasoning. The Surveillance Impact Report shall be published at least thirty (30) days before any Council vote.

Article IV — Deployment Restrictions

Section 4.01 — Permitted Locations

ALPR systems may only be installed at major roadway intersections, designated ingress/egress corridors, or traffic-flow locations explicitly approved by Council through recorded vote. No ALPR system shall be installed on state-maintained highways except as authorized by N.C. Gen. Stat. § 20-183.31 and any applicable NCDOT agreements.

Section 4.02 — Prohibited Locations

ALPR systems shall not be installed: inside residential neighborhoods or on streets primarily serving residential traffic; adjacent to or within 500 feet of schools (K-12) unless separately approved by Council following a Surveillance Impact Report; within 500 feet of hospitals or medical campuses; within 500 feet of houses of worship; within 500 feet of designated protest or assembly areas; within parks or recreational facilities; within pedestrian-focused civic areas, including downtown walking districts; or at any location where placement would enable comprehensive surveillance of constitutionally protected activities including religious practice, medical care, political assembly, or association. The distance requirements in this section shall be measured from the nearest property line of the protected location to the ALPR installation point.

Section 4.03 — Public Hearing Requirement

The following actions require public notice (at least thirty (30) days), public hearing, a published Surveillance Impact Report, and a recorded Council vote: new ALPR deployment; relocation of existing ALPR cameras; expansion of camera count or coverage area; functional upgrades (including software capabilities not previously authorized); vendor replacement; any policy modification; any new or modified sharing arrangement; and any contract renewal.

Section 4.04 — Vendor Restrictions

No ALPR vendor shall possess authority to independently determine camera placement, modify deployment architecture, alter retention settings, establish or modify sharing arrangements, expand operational scope, activate features not explicitly authorized by Council, communicate directly with outside agencies regarding Apex data access, or change platform configurations that affect data governance without prior written authorization from the Town Manager and notification to the Committee. Any vendor contract inconsistent with this ordinance shall be deemed void and unenforceable within the Town's jurisdiction. Vendor default platform settings shall not govern; all settings affecting data retention, sharing, access, and feature activation shall be explicitly configured to match this ordinance and documented in writing.

Article V — Data Governance

Section 5.01 — Maximum Retention

All ALPR data shall be permanently and irreversibly deleted within ten (10) calendar days after the date of capture unless: (a) the data is subject to a valid judicial preservation order or search warrant issued pursuant to N.C. Gen. Stat. § 20-183.32(b) or (c); (b) the data is attached to an active, documented felony or violent crime investigation with a case number and assigned investigator; or (c) retention is otherwise required by a specific provision of state or federal law. No blanket preservation of ALPR data is permitted. Each retention exception must be individually documented with the case number, authorizing officer, legal basis, and expected duration. The Committee shall review all active retention exceptions quarterly.

> *Note: N.C. Gen. Stat. § 20-183.32(a) establishes a maximum retention period of 90 days. This ordinance sets a stricter local standard of 10 days, which is within the Town's authority under § 160A-174 as the state statute establishes a ceiling, not a floor. Flock Safety's current Apex contract specifies a 30-day retention period. This ordinance reduces that to 10 days.*

Section 5.02 — Local Data Sovereignty

ALPR data collected by or on behalf of the Town shall remain exclusively under Town control. ALPR data shall not be exported, shared, federated, mirrored, pooled, or made searchable outside Apex jurisdiction except as specifically authorized by this ordinance. The vendor's nationwide network, statewide network, and any similar data-pooling mechanism shall be disabled for all Apex cameras and data. The Town shall require the vendor to certify in writing, at contract execution and annually thereafter, that no entity other than authorized Town personnel can search, access, or receive Apex ALPR data through any vendor platform feature, API, data feed, or network configuration.

Section 5.03 — Sharing Restrictions

The Town shall not participate in national ALPR sharing systems, regional federated search systems, vendor-operated search ecosystems or nationwide lookup tools, passive sharing networks (where data is searchable without an affirmative per-query authorization), standing interagency access arrangements, or automated federal query systems. This section expressly supersedes any vendor-sharing functionality included in prior or current agreements.

(a) Permitted Case-by-Case Sharing

ALPR data may be disclosed to another law enforcement agency only if all of the following conditions are met: (i) the requesting agency submits a written request as required by N.C. Gen. Stat. § 20-183.32(e), specifying the legitimate law enforcement purpose; (ii) the request is for data related to a specific, active investigation involving a felony, violent crime, missing or endangered person, or stolen vehicle; (iii) the request is reviewed and approved by a supervisor at the rank of Captain or above; (iv) the disclosure is logged with the requesting agency, the request date, the approving officer, the case number, and the specific data disclosed; and (v) the Committee is notified of the disclosure within seven (7) calendar days.

(b) Federal Access Restrictions

No federal agency shall receive direct access, standing access, mirrored access, API access, federated search access, or shared retention access to Town ALPR data. Federal agencies may request specific, case-by-case data disclosure only through the process described in Section 5.03(a), and only pursuant to a federal search warrant issued in compliance with the Federal Rules of Criminal Procedure as authorized by N.C. Gen. Stat. § 20-183.32(b)(3), or pursuant to a written request for a legitimate law enforcement purpose under § 20-183.32(e). No federal data request related to civil immigration enforcement shall be honored. Any violation of this section triggers automatic suspension under Article IX.

Note: N.C. Gen. Stat. § 20-183.32(e) permits disclosure to federal law enforcement for a legitimate law enforcement purpose pursuant to a written request. This ordinance does not prohibit all federal disclosure (which would conflict with state law) but restricts it to case-by-case written requests with local supervisory approval and Committee notification, and categorically excludes immigration enforcement.

Section 5.04 — Private Camera Network Restrictions

APD shall not receive search access to, accept camera shares from, or integrate data from any private camera network without: (a) prior written authorization from the Town Council following a public hearing; (b) a published Surveillance Impact Report addressing the specific private cameras at issue; and (c) a written agreement specifying the scope of access, retention of data obtained from private cameras, and audit requirements. Any existing private camera access arrangements that have not been authorized by Council shall be terminated within thirty (30) days of this ordinance's effective date.

Section 5.05 — Hot List Governance

APD shall maintain a written policy governing all hot lists used with the ALPR system. The policy shall specify: which hot lists are authorized (limited to NCIC stolen vehicle files, state BOLO databases for felony warrants, and Amber/Silver/Blue alert systems unless otherwise approved by Council); the criteria for adding plates to any locally created hot list; the maximum duration a plate may remain on a locally created hot list; the process for receiving, reviewing, and approving or rejecting hot lists from outside agencies; and the audit and oversight procedures for all hot list activity. Hot lists from outside agencies shall not be accepted without review and written approval by a supervisor at the rank of Captain or above. The Committee shall review all active hot list arrangements annually.

Section 5.06 — Storage Security Standards

ALPR systems shall utilize FedRAMP-authorized cloud infrastructure or Town-controlled on-premises storage; encryption at rest (AES-256 or equivalent); encryption in transit (TLS 1.2 or higher); multi-factor authentication for all user accounts; immutable, tamper-evident audit logs; role-based access controls with principle of least privilege; and automated deletion mechanisms that execute the retention limits in Section 5.01 without manual intervention.

Section 5.07 — Data Breach Notification

In the event of any unauthorized access to, disclosure of, or compromise of ALPR data or the ALPR system (including vendor system breaches affecting Apex data), the Town shall: (a) notify the Committee, Council, and Privacy Advocate within forty-eight (48) hours of discovery; (b) publish a public notice within seven (7) calendar days describing the nature and scope of the breach; (c) suspend all ALPR operations until the breach is remediated and an independent security assessment confirms restoration of compliant operations; and (d) retain an independent forensic investigator if the breach involves unauthorized external access.

Section 5.08 — Vendor Response to Legal Process

The vendor contract shall require that if the vendor receives any subpoena, court order, national security letter, or other legal process from any federal, state, or local government entity seeking access to Apex ALPR data, the vendor shall: (a) notify the Town Manager, Town Attorney, Committee Chair, and Privacy Advocate within twenty-four (24) hours of receipt, unless prohibited by law from doing so; (b) not disclose any Apex data in response to such process without first providing the Town a reasonable opportunity to intervene, move to quash, or otherwise challenge the legal process in court; and (c) if legally prohibited from notifying the Town (such as by a gag order accompanying a national security letter), seek judicial relief from the nondisclosure requirement at the earliest opportunity. The vendor's failure to comply with this section constitutes a material breach of the vendor contract.

Section 5.09 — Interoperability Restriction

ALPR data, systems, and infrastructure shall not be integrated with, cross-referenced against, or made interoperable with any other surveillance system operated by or on behalf of the Town, including but not limited to closed-circuit television (CCTV), body-worn cameras, gunshot detection systems, drone surveillance, social media monitoring tools, or any other data collection system, unless such integration is separately authorized by ordinance following the process described in Section 8.02.

[NEW]

Section 5.10 — Occupant Image Minimization

(a) The ALPR system shall be configured to capture the minimum data necessary to perform authorized functions. To the extent the system captures images of vehicle occupants, passengers, or pedestrians incidental to plate capture, such images shall not be stored, indexed, searched, analyzed, shared, or used for any purpose.

(b) The vendor shall implement automated technical measures to prevent the retention of occupant imagery, including but not limited to: masking, blurring, or cropping occupant-identifiable portions of captured images before storage; or configuring the system to retain only the extracted plate data, vehicle metadata as defined in Section 2.02, and a cropped image of the license plate area.

(c) If the vendor's system architecture does not permit automated occupant image suppression, the full captured image shall be subject to the same ten (10) day deletion requirement as all other ALPR data under Section 5.01, and no occupant-identifiable image shall be disclosed, shared, or provided to any requesting agency under Section 5.03.

(d) The independent annual audit required by Section 7.03 shall include a specific evaluation of whether the system is capturing, retaining, or making available occupant imagery in violation of this section.

(e) No ALPR image shall be used as the basis for identifying any individual (as distinct from a vehicle), regardless of whether the image was captured incidentally or intentionally.

> *Note: This section addresses the fact that Flock Safety cameras capture contextual images extending well beyond the license plate, creating a de facto photographic record of vehicle occupants at surveilled locations. Without explicit restriction, this imagery is unregulated by the remainder of this ordinance.*

[NEW]

Section 5.11 — Protection Against Civil Process Disclosure

(a) ALPR data collected by or on behalf of the Town shall not be disclosed in response to any civil subpoena, discovery request, Freedom of Information request to the extent exempt under applicable law, or other non-criminal legal process.

(b) Upon receipt of any civil subpoena or discovery request seeking ALPR data, the Town Attorney shall move to quash or otherwise resist disclosure. The Committee and Privacy Advocate shall be notified within five (5) business days of receipt.

(c) This section does not limit the authority of a court of competent jurisdiction to order disclosure pursuant to a criminal search warrant or preservation order as described in Section 5.01, or to order disclosure in a civil action brought under Section 10.05 of this ordinance to enforce its provisions.

> *Note: North Carolina public records law (N.C. Gen. Stat. § 132-1.4) exempts criminal investigation records from public disclosure. This section extends protection against civil-process access to all ALPR data, consistent with the ordinance's privacy-protective construction and the sensitive nature of location data as recognized in Carpenter v. United States.*

Article VI — Operational Restrictions

Section 6.01 — Authorized Uses

ALPR systems may only be used for: (a) felony investigations; (b) violent crime investigations; (c) missing or endangered person investigations (as defined in N.C. Gen. Stat. § 20-183.30(8)); (d) stolen vehicle investigations; (e) active felony warrant apprehension (as authorized by N.C. Gen. Stat. § 20-183.30(5)(b)); and (f) judicially authorized investigations supported by a warrant or preservation order.

[NEW] (g) Single-query use of "Vehicle Fingerprint" or equivalent vehicle-identification technology to identify a specific suspect vehicle in an active felony or violent crime investigation, subject to all of the following conditions: (i) the query is tied to a documented case with an assigned case number and investigating officer; (ii) the query is approved in advance and in writing by a supervisor at the rank of Captain or above; (iii) the query is logged in full compliance with Section 6.03; and (iv) the Vehicle Fingerprint function is activated only for the duration of the specific query and is not maintained in continuous or passive operation. This subsection authorizes individual investigative queries only and does not authorize always-on, passive, or continuous Vehicle Fingerprint matching.

Section 6.02 — Prohibited Uses

ALPR systems shall not be used for: traffic enforcement (consistent with N.C. Gen. Stat. § 20-183.31(b)); civil immigration enforcement or any investigation where the primary purpose is enforcement of federal immigration law; monitoring, tracking, or identifying participants in protests, demonstrations, marches, rallies, or any constitutionally protected assembly; monitoring, tracking, or identifying individuals based on political affiliation, religious practice, association, or expression; generalized intelligence gathering unconnected to a specific investigation; civil code enforcement including parking, zoning, or municipal ordinance violations; predictive policing or any algorithmic risk assessment of future criminal activity; continuous surveillance or persistent tracking of any individual absent a judicial order; behavioral analysis or pattern-of-life reconstruction; monitoring of constitutionally protected activities including visits to medical facilities, houses of worship, legal counsel, or political organizations; or any purpose not expressly authorized by Section 6.01 and consistent with N.C. Gen. Stat. § 20-183.30(5).

Section 6.03 — Query Documentation

Every ALPR query shall be documented with: the case number or incident number to which the query relates; the identity of the officer or authorized user conducting the query; the investigative purpose and factual basis for the query; the specific search parameters used; the timestamp of the query; the results returned; and any subsequent action taken based on the query results. All query logs shall be retained for a minimum of three (3) years and shall be auditable by the Committee, Privacy Advocate, and independent auditors.

Section 6.04 — Search Threshold Requirement

No ALPR search shall occur absent articulable investigative relevance tied to a documented, active case. Speculative searches, fishing expeditions, pattern-of-life analysis, and bulk queries unconnected to a specific investigation are prohibited. Any search covering more than a single license plate or a single twenty-four (24) hour time window shall require written supervisory approval at the rank of Lieutenant or above, documented in the query log.

Section 6.05 — Warrant Preference

For any ALPR query seeking historical location data spanning more than forty-eight (48) hours for a single vehicle, APD shall obtain a search warrant from a court of competent jurisdiction before executing the query,

except in exigent circumstances involving an imminent threat to life. This provision reflects the privacy principles recognized in *Carpenter v. United States*, 585 U.S. 296 (2018), and ensures that comprehensive historical movement data is treated with the constitutional gravity it warrants.

Section 6.06 — Geofence and Location-Based Query Restrictions

No ALPR query shall be structured to identify all vehicles present at or near a specific location during a specified time period (a "geofence-style query") without a search warrant issued by a court of competent jurisdiction upon a showing of probable cause. A geofence-style query is any query that uses geographic coordinates, camera location, or area-based parameters as the primary search criteria rather than a specific license plate number. This restriction applies regardless of the time window involved.

Section 6.07 — Training Requirements

Consistent with N.C. Gen. Stat. § 20-183.31(a)(4), all personnel authorized to operate, search, administer, or access the ALPR system shall complete documented training before receiving access. Training shall cover: the provisions of this ordinance and all applicable state law; authorized and prohibited uses; query documentation requirements; search threshold and warrant requirements; data retention and deletion obligations; sharing restrictions; hot list governance; audit and oversight procedures; constitutional considerations including Fourth Amendment principles as interpreted in *Carpenter v. United States*; civil liberties implications of ALPR technology; and procedures for reporting suspected misuse. Refresher training shall be completed annually. Training records shall be maintained and made available to the Committee upon request.

Section 6.08 — Misidentification and Wrongful Action Remediation

If any person is stopped, detained, arrested, searched, or otherwise subjected to law enforcement action based in whole or in part on an ALPR alert or query result that is later determined to have been erroneous (due to misread plates, stale data, database errors, or any other cause), APD shall: (a) document the incident, including the cause of the error, within twenty-four (24) hours; (b) notify the affected individual in writing within seventy-two (72) hours of the determination that the action was based on erroneous ALPR data; (c) report the incident to the Committee at its next meeting; (d) include the incident in the quarterly report; and (e) cooperate with any claim or complaint filed by the affected individual. The Committee shall track misidentification incidents and report trends to Council annually. Patterns of misidentification shall be considered grounds for operational review or suspension.

Article VII — Transparency and Public Reporting

Section 7.01 — Quarterly Reports

APD shall publish quarterly reports, reviewed by the Committee before publication, including: total plate reads during the quarter; total searches conducted, categorized by authorized use type; total alerts generated and resulting law enforcement actions; felony case associations, with case disposition where available; all retention exceptions with case numbers and legal basis; all data preservation events; all sharing disclosures made under Section 5.03(a), with requesting agency and case type; all violations identified, investigations initiated, and disciplinary actions taken; all external sharing requests received, whether approved or denied; all hot list additions, modifications, and removals; all audit findings; and a summary of Committee proceedings and recommendations.

Section 7.02 — Public Transparency Portal

The Town shall maintain a continuously accessible public web portal displaying: all current ALPR camera locations, depicted on a map; the full text of this ordinance and all governing policies; all audit summaries and independent audit reports; all Committee meeting agendas, minutes, and recommendations; all quarterly and annual reports; all current and historical vendor contracts, order forms, and amendments (with pricing); renewal and expiration timelines; all Surveillance Impact Reports; all sharing arrangements (with the name and jurisdiction of each sharing partner, the permissions granted, and the date of Council authorization); all hot list policies and current hot list sources; and all citizen complaints and their disposition (with personally identifiable information redacted as required by law). The portal shall be updated within fourteen (14) days of any change.

Section 7.03 — Annual Independent Audit

An independent third-party audit shall occur annually, funded by the Town, commissioned by the Committee, and conducted by an auditor with no financial relationship to any ALPR vendor. The audit shall evaluate: compliance with this ordinance and N.C. Gen. Stat. Chapter 20, Article 3D; retention enforcement, including verification of automated deletion; query legitimacy, including a random sample review of at least 10% of all queries; access control enforcement, including role-based permissions and multi-factor authentication; security compliance, including encryption, logging, and penetration testing results; unauthorized access attempts and any system compromises; all sharing activity, including vendor platform configuration review to verify that nationwide/statewide network participation is disabled; all hot list activity; and comparison of vendor-reported system configuration against this ordinance's requirements.

[NEW] The audit shall include infrastructure-level deletion verification, conducted at the vendor's data storage environment, confirming that ALPR data subject to the ten (10) day retention limit in Section 5.01 has been irreversibly destroyed from all storage layers, including primary databases, backup systems, disaster recovery replicas, content delivery caches, and any intermediate processing storage. The auditor shall have direct access to the vendor's storage systems for purposes of this verification, or the vendor shall provide a sworn certification from an independent forensic examiner confirming deletion at all storage layers. A vendor's refusal to permit infrastructure-level deletion verification or to provide the sworn forensic certification constitutes a material audit finding and shall be reported to Council as a compliance failure.

Audit results shall be published in full on the transparency portal within thirty (30) days of completion.

Section 7.04 — Annual Effectiveness Report

In addition to the independent compliance audit, APD shall publish an annual effectiveness report evaluating whether the ALPR system is achieving its stated public safety objectives. The report shall include: the total number of ALPR-assisted arrests, categorized by offense type; the total number of ALPR-assisted case

clearances; the total number of alerts generated versus the number that resulted in a law enforcement action; the false positive rate (alerts that did not match the intended vehicle); the number of misidentification incidents reported under Section 6.08; a comparison of crime rates in ALPR-covered areas before and after deployment; total system cost (including hardware, software, maintenance, staff time, oversight, and audit costs) expressed as a cost-per-case-clearance figure; and any other metrics the Committee deems relevant. The effectiveness report shall be published on the transparency portal and presented to Council before any contract renewal vote. The Committee may commission an independent evaluation of system effectiveness if it determines the APD-prepared report is insufficient.

Article VIII — Surveillance Expansion Prohibition

Section 8.01 — Prohibited Features

The Town shall not deploy, activate, or permit the activation of: facial recognition (including any integration between ALPR and facial recognition systems); biometric analysis of any kind; AI-assisted identity systems that identify or infer the identity of individuals (as distinct from vehicles); live video monitoring or streaming, including "LiveView" or equivalent vendor features; predictive policing systems or algorithms; behavioral analytics; audio detection systems integrated with ALPR infrastructure; persistent movement reconstruction systems; **[NEW]** continuous, passive, or always-on vehicle-identification systems that track or identify specific vehicles by physical characteristics (including damage, accessories, decals, modifications, or other distinguishing features) independent of license plate number, including but not limited to "Vehicle Fingerprint" or equivalent vendor features operated in any mode other than the limited single-query investigative use authorized by Section 6.01(g); or any feature that converts ALPR infrastructure into a general-purpose surveillance or intelligence platform.

Section 8.02 — Expansion Approval Requirement

Any future surveillance technology deployment or expansion of ALPR capabilities beyond those authorized in this ordinance shall require: a separate ordinance enacted through the full legislative process; an independent Surveillance Impact Report prepared by the Privacy Advocate; a public hearing with at least forty-five (45) days' advance notice; a majority vote of the full Town Council; and a disparate impact analysis evaluating the technology's effects on communities of color, immigrant communities, low-income communities, and other vulnerable populations.

Article IX — Violations, Suspension, and Enforcement

Section 9.01 — Automatic Suspension

The ALPR system shall be automatically suspended for a minimum of sixty (60) days upon confirmed occurrence of any of the following: unauthorized sharing of ALPR data (including via vendor platform misconfiguration); retention violation (data held beyond authorized period); prohibited search (query without documented investigative basis); unauthorized access (access by any person or entity not authorized under this ordinance); data breach or system compromise; audit noncompliance or obstruction; quarterly or annual reporting failure exceeding thirty (30) days past due; activation of any prohibited feature listed in Section 8.01; or unauthorized acceptance of external share requests or hot lists. Suspension shall be effective immediately upon confirmation by the Committee, Privacy Advocate, or Town Manager.

Section 9.02 — Mandatory Investigation

Any suspension event shall trigger: an independent investigation conducted by a party with no reporting relationship to APD; a public report of findings, redacted only as required by law; review and recommendations by the Committee; a public Council hearing; and a recorded Council vote to resume operations, which shall not occur until all identified deficiencies have been remediated and verified by the independent auditor.

Section 9.03 — Personnel Discipline

Confirmed intentional misuse of the ALPR system by any Town employee shall trigger: disciplinary review pursuant to Town personnel policies; potential termination of employment; referral for criminal review under N.C. Gen. Stat. § 20-183.33, which makes unauthorized access, preservation, or disclosure of ALPR data a Class 1 misdemeanor; and mandatory disclosure of the incident to Council and the Committee.

Article X — Citizen Appeals and Redress

Section 10.01 — Complaint Process

Any person may file a complaint alleging: a privacy violation related to ALPR operation; misuse of the ALPR system; noncompliance with this ordinance; a request for audit or investigation; or a policy concern. Complaints may be filed with the Committee, the Town Clerk, or through the transparency portal. The Committee shall acknowledge receipt within five (5) business days and provide a substantive response or investigation timeline within thirty (30) days.

Section 10.02 — Independent Review

Complaints shall be reviewed by the Committee with assistance from the Privacy Advocate or outside counsel as necessary. Complaints alleging criminal misuse shall be referred to the appropriate prosecutorial authority. The complainant shall be notified of the outcome in writing.

Section 10.03 — Public Findings

Final findings on all complaints shall be publicly released on the transparency portal, with personally identifiable information redacted as required by law.

Section 10.04 — Non-Retaliation

No person shall be subject to retaliation, harassment, or adverse action for filing a complaint under this article, testifying before the Committee, or participating in any proceeding under this ordinance.

Section 10.05 — Private Right of Action

Any person who has been harmed by a violation of this ordinance may bring a civil action in the General Court of Justice of North Carolina to enforce its provisions. A court may award declaratory relief, injunctive relief (including an order to suspend ALPR operations), and reasonable attorneys' fees and costs to a prevailing plaintiff. This private right of action supplements, and does not replace, any other remedy available under state or federal law, including claims under 42 U.S.C. § 1983 for constitutional violations. For purposes of this section, "harm" includes but is not limited to: being subjected to an unauthorized search or query; being stopped, detained, or arrested based on erroneous ALPR data; having one's ALPR data shared in violation of this ordinance; or being subjected to surveillance in a manner prohibited by this ordinance.

> *Note: North Carolina municipalities may create civil causes of action through ordinance under their general police power (G.S. § 160A-174). The private right of action ensures that enforcement does not depend solely on the willingness of Town officials to act, consistent with the EFF's recommendation for CCOPS ordinances and Washington State's approach in SB 6002.*

[NEW]

Section 10.06 — Individual Data Inquiry

(a) Any person may submit a written inquiry to the Committee requesting confirmation of whether their vehicle's license plate data was captured, searched, or shared by the ALPR system during a specified time period not exceeding ninety (90) days.

(b) The Committee shall respond in writing within thirty (30) calendar days. The response shall confirm or deny that the individual's plate data was captured during the specified period, confirm or deny that the individual's plate data was the subject of any search or query, and confirm or deny that the individual's plate data was shared with any external entity under Section 5.03(a).

(c) If the individual's data was searched or shared, the response shall include the date and general category of the search or disclosure (felony investigation, stolen vehicle, etc.) but shall not include information that would compromise an active investigation. The Committee may defer disclosure of search or sharing details for up to one hundred eighty (180) days if disclosure would jeopardize an active felony investigation, provided the Committee documents the basis for deferral.

(d) No fee shall be charged for an individual data inquiry. The Committee shall process inquiries in the order received.

(e) The non-retaliation protections of Section 10.04 apply to any person who submits a data inquiry under this section.

Note: This provision is modeled on data subject access rights common in privacy frameworks including GDPR (Article 15) and CCPA (§ 1798.110). Because ALPR data is deleted after ten (10) days under Section 5.01, the Committee's response regarding capture data will be limited to the current retention window. Query and sharing logs, retained for three (3) years under Section 6.03, support responses regarding searches and disclosures over the full ninety (90) day lookback period.

Article XI — Contracting and Procurement

Section 11.01 — Contract Limits

No ALPR contract shall exceed two (2) years in duration. Automatic renewals are prohibited. Each renewal requires a public hearing, Committee recommendation, Surveillance Impact Report, and recorded Council vote.

Section 11.02 — Mandatory Competitive Review

After two consecutive contract terms with the same vendor, the Town shall conduct a competitive Request for Proposals process open to all qualified vendors before entering into a subsequent contract.

Section 11.03 — Vendor Override Clause

No vendor contract, master services agreement, order form, terms of service, privacy policy, or other agreement may: override any provision of this ordinance or Town policy; expand sharing authority beyond what this ordinance permits; alter retention limits; authorize external access not permitted by this ordinance; permit vendor-controlled policy changes; grant the vendor authority to change platform settings affecting Apex data governance without written Town authorization; or enable any feature or capability not explicitly approved by Council. Any clause in any vendor agreement that conflicts with this ordinance is void and unenforceable within Town jurisdiction. In the event of conflict between vendor terms and this ordinance, this ordinance controls.

Section 11.04 — Prohibition on Commercialization

No ALPR vendor shall commercialize, anonymize for resale, aggregate for commercial products, monetize, or repurpose any data collected by or on behalf of the Town, including anonymized, de-identified, or derivative data. This section expressly rejects any vendor contract provision purporting to authorize commercialization of anonymized or derivative data.

Section 11.05 — Vendor Certification Requirements

As a condition of any ALPR contract, the vendor shall certify in writing at contract execution and annually thereafter: (a) that the vendor's platform configuration for Apex cameras and data matches the requirements of this ordinance, including disabled nationwide/statewide network participation and sharing restrictions; (b) that no entity other than authorized Town personnel can access Apex data through any vendor feature, API, network, or backdoor; (c) that the vendor has not provided, and will not provide, any federal agency with direct or indirect access to Apex ALPR data except through a request processed by the Town under Section 5.03; (d) that the vendor will notify the Town within twenty-four (24) hours of any data breach, unauthorized access, or legal process (including subpoenas or national security letters) affecting Apex data; and (e) that the vendor will cooperate fully with independent audits commissioned under this ordinance. A vendor's material breach of any certification constitutes grounds for immediate contract termination.

[NEW]

Section 11.06 — Minimum Accuracy Standard

(a) Any ALPR system operated by or on behalf of the Town shall demonstrate a plate-read accuracy rate of ninety-nine percent (99%) or higher under representative operational conditions, including nighttime, adverse weather, and variable vehicle speeds.

(b) The vendor shall provide independent third-party accuracy testing results at contract execution and at each renewal. Testing shall be conducted by a laboratory or testing organization with no financial relationship

to the vendor. The testing methodology, sample size, and conditions shall be disclosed in full.

(c) APD shall conduct or commission a local field-accuracy validation within one hundred eighty (180) days of initial deployment and annually thereafter. The validation shall compare a random sample of at least one thousand (1,000) ALPR reads against manual verification and shall report: the true positive rate (correct plate reads); the false positive rate (incorrect plate reads, including partial misreads); and the false negative rate (plates present but not captured). This validation timeline runs independently of the ninety (90) day transition period in Section 14.02.

(d) If any accuracy test or validation yields a result below ninety-nine percent (99%), the Town shall notify the vendor in writing and require corrective action within thirty (30) days. If accuracy remains below ninety-nine percent (99%) after the corrective period, the affected cameras shall be taken offline until compliance is restored and verified by independent retest.

(e) All accuracy testing results, methodology, and corrective actions shall be published on the transparency portal and included in the annual effectiveness report required by Section 7.04.

Note: There is no North Carolina statute establishing an ALPR accuracy threshold. This section exercises the Town's authority under N.C. Gen. Stat. § 160A-174 to impose local operational standards.

Article XII — Sunset and Reauthorization

Section 12.01 — Automatic Sunset

Authorization to operate any ALPR system under this ordinance shall automatically expire four (4) years after its effective date unless reauthorized. Upon expiration, all ALPR operations shall cease and all data shall be deleted within ten (10) calendar days, unless subject to a valid preservation order or active investigation retention exception.

Section 12.02 — Reauthorization Requirements

Reauthorization requires: a public hearing with at least forty-five (45) days' advance notice; review of the most recent independent audit; a Surveillance Impact Report addressing whether continued ALPR use is justified in light of the system's actual effectiveness, privacy costs, and available alternatives; a Committee recommendation for or against reauthorization; and a recorded vote of the full Town Council. APD shall possess no independent renewal authority.

Article XIII — Severability and Construction

Section 13.01 — Severability

If any section, subsection, sentence, clause, or phrase of this ordinance is for any reason held to be invalid or unconstitutional by a court of competent jurisdiction, such holding shall not affect the validity of the remaining portions of this ordinance. The Town Council declares that it would have adopted this ordinance and each section, subsection, sentence, clause, and phrase thereof irrespective of the fact that any one or more sections, subsections, sentences, clauses, or phrases may be declared invalid.

Section 13.02 — Construction

This ordinance shall be liberally construed to effectuate its purposes of protecting privacy, civil liberties, and democratic oversight of surveillance technology. Any ambiguity in the scope of a restriction, prohibition, or limitation in this ordinance shall be resolved in favor of greater privacy protection and narrower surveillance authority. Nothing in this ordinance shall be construed to authorize any surveillance activity not expressly permitted herein. The omission of a specific surveillance technique, technology, or practice from the prohibited lists in this ordinance shall not be construed as authorization for its use; rather, any activity not expressly authorized by Section 6.01 is prohibited.

Article XIV — Effective Date and Transition

Section 14.01 — Effective Date

This ordinance shall take effect upon adoption by the Town Council.

Section 14.02 — Transition Period

Within ninety (90) days of the effective date: (a) APD shall bring all ALPR operations into compliance with this ordinance, including retention limits, sharing restrictions, and vendor platform configuration; (b) all unauthorized sharing arrangements shall be terminated; (c) all unauthorized private camera network access shall be terminated; (d) the vendor shall provide the certifications required by Section 11.05; (e) the Town shall publish the transparency portal required by Section 7.02; and (f) the Town Council shall appoint the initial members of the Citizen ALPR Oversight Committee.

Section 14.03 — Existing Contracts

Any existing ALPR vendor contract shall be modified to comply with this ordinance within sixty (60) days of the effective date. If the vendor refuses to accept modifications necessary for compliance, the contract shall be terminated at the earliest date permitted by its terms, and all ALPR operations shall cease upon termination.

Appendix A — Legal and Policy References

North Carolina Statutes

N.C. Gen. Stat. §§ 20-183.30 through 20-183.33 (Automatic License Plate Reader Systems)

N.C. Gen. Stat. § 160A-174 (General Police Power)

N.C. Gen. Stat. § 160A-175 (Ordinance-Making Authority)

N.C. Gen. Stat. § 132-1 (Public Records)

Federal Law and Case Law

Carpenter v. United States, 585 U.S. 296 (2018) (Fourth Amendment requires a warrant for historical cell-site location information; analogous privacy principles apply to comprehensive vehicle movement records)

United States v. Jones, 565 U.S. 400 (2012) (GPS tracking constitutes a search under the Fourth Amendment)

United States v. Yang, No. 18-50440 (9th Cir. 2020) (standing requirements for challenging ALPR database queries)

42 U.S.C. § 1983 (Civil action for deprivation of rights under color of law)

Model Legislation and Comparable Ordinances

ACLU Community Control Over Police Surveillance (CCOPS) Model Bill (April 2021)

San Diego Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance

San Diego Privacy Advisory Board: Final Recommendation on ALPR, May 2026

Washington State SB 6002 (effective March 30, 2026): ALPR registration with Attorney General, 72-hour retention, prohibited uses including immigration enforcement and location-based restrictions, private right of action, annual audits, gross misdemeanor penalties

California SB 274 (2025): 60-day retention for non-hot-list data, supervisory approval for access, audit trail requirements, prohibition on default vendor database access

South Carolina Community Data Protection and Responsible Surveillance Act, H.B. 4675 (2025)

Oakland, CA Privacy Commission and Surveillance Oversight Ordinance

San Francisco Surveillance Technology Ordinance

Research and Reporting

Brennan Center for Justice: Automatic License Plate Readers: Legal Status and Policy Recommendations (2020)

Electronic Frontier Foundation: Street-Level Surveillance project and CCOPS framework

TRUST SD: People's Surveillance Impact Report for ALPR (March 2025)

Journal of Experimental Criminology: Independent research finding no significant deterrent effect from ALPR deployment

Major Cities Chiefs Association: ALPR Technology in Law Enforcement best practices (February 2023)

Apex-Specific Evidence

Town of Apex public records (2025-2026): Flock Safety sharing snapshots, pending share requests, contract documents, and internal correspondence obtained pursuant to the North Carolina Public Records Act (N.C. Gen. Stat. § 132-1 et seq.)

Flock Safety Order Form, Exhibit A (2025): Retention Period 30 days; Nationwide Network Enabled; Statewide Network: North Carolina Enabled

March 2026 Sharing Snapshot: 994 organizations (186 in-state, 808 out-of-state, 2 federal)

April 2026 Sharing Snapshot: 1,070 organizations (195 in-state, 875 out-of-state, "No Federal")

Pending share requests (16 documents, 2025-2026): agencies from Georgia, Indiana, Florida, Mississippi, Texas, Tennessee, Kansas, Oklahoma, Louisiana, Kentucky, Ohio, Nebraska, South Carolina, Missouri, Utah, Alabama, and Virginia requesting search, hot list, VMS, and analytics access

Federal Developments

FBI Request for Proposals: Nationwide ALPR data access ($36 million), published May 14, 2026, Directorate of Intelligence. Six geographic regions covering all 50 states and territories. Single-vendor preference. Flock Safety and Motorola Solutions identified as likely bidders.

404 Media reporting (2025-2026): local police performing Flock nationwide database lookups on behalf of ICE; Homeland Security Investigations, Secret Service, and Navy criminal investigation arm pilot access to Flock's nationwide network

Flock Safety login credentials found for sale on Russian hacking forums (November 2025)