STATEMENT AND RECOMMENDED POLICY FRAMEWORK

Automated License Plate Readers (ALPR), Flock Cameras, Artificial Intelligence & Emerging Surveillance Technology

Presented to

Judge Lloyd Lane
Freestone County Commissioners Court
Sheriff Jeremy Shipley

September 2, 2026

Public safety and constitutional liberty are not competing responsibilities. Good government protects both.

Submitted by

Robert P. Sharpe - RancherRob
Simsboro, Texas

Submitted as a private citizen for deliberation and the public record.

Prepared Statement

Judge Lane, Commissioners, and Sheriff Shipley:

I want to begin by making my position clear. I support our Sheriff, our deputies, our constables, and the men and women charged with protecting Freestone County. I support giving law enforcement effective tools to locate a missing child, recover a stolen vehicle, identify a wanted fugitive, investigate serious crime, and protect officers.

This is not a choice between law enforcement and liberty. We should protect both.

Automated license-plate readers can be extremely useful investigative tools. But the technology has evolved beyond simply taking a photograph of a license plate. Modern systems can connect cameras, databases, artificial intelligence, vehicle characteristics, location histories, and information-sharing networks across jurisdictions. That creates tremendous investigative capability. It also creates tremendous governmental power.

My concern is not that anyone in Freestone County has abused that power. I have found no basis for making such an accusation, and I am not making one.

Judge Lane has publicly stated that Freestone County does not own or operate Flock cameras. If that remains the case, then Freestone County has an opportunity some communities did not have: we can establish good policy before there is a controversy instead of writing policy after something goes wrong.

Texas public-safety guidance and law-enforcement best practices recognize the importance of written rules governing ALPR deployment, use, access, retention, information sharing, auditability, and accountability. Recent controversies in Texas and other states demonstrate why those safeguards matter.

A good policy should never depend entirely upon whether we trust the people currently holding office. We may have confidence in the Sheriff, Judge, Commissioners, or other officials serving today. But the policies we establish can outlast every one of us.

Recent history should remind us how quickly circumstances can change. During the COVID-19 emergency, Americans experienced extraordinary governmental restrictions affecting businesses, churches, schools, gatherings, travel, and ordinary daily life. Whatever one thinks about individual decisions made during that period, the institutional lesson is that emergency conditions can cause governmental authority to expand very quickly.

Most of us are also old enough to remember the images from Tiananmen Square in 1989 - the tanks and the lone man standing before them. I am not comparing Freestone County or American law enforcement to the Chinese Communist government. The lesson is more fundamental: technology and governmental power can protect people under constitutional restraints, or they can be used by authoritarian governments to identify, locate, track, and suppress people.

There is a fine line between protection and abuse, and good policy helps us draw that line before anyone crosses it.

We should build safeguards not only for the administration we trust, but for the administration we cannot foresee. We should never grant government a power merely because we trust the people who possess it today. We should ask whether we would be comfortable with that same power in the hands of an administration we did not trust.

The fact that technology can do something does not automatically mean government should do it. Likewise, a new capability added by a vendor should not automatically become an authorized governmental use.

I am not asking this Court to dictate how Sheriff Shipley conducts criminal investigations. Operational law-enforcement decisions properly belong with our elected law-enforcement officials. I am recommending that any county department that acquires, operates, accesses, contracts for, or participates in ALPR or comparable surveillance technology maintain clear written policies governing that power.

Those policies should answer basic questions: Who may use the system? For what purposes? What justification is required for a search? How long is information retained? Who may receive it? Which outside systems may county personnel search? Which outside agencies may search ours? Is every search logged? Who reviews those logs? What happens if the system is misused? And who decides whether a new AI, facial-recognition, biometric, predictive, or tracking capability will be used?

An ALPR alert should ordinarily be treated as an investigative lead and appropriately verified before enforcement action whenever circumstances permit. Every authorized user should be individually accountable. Searches should have legitimate documented purposes. Retention should be defined rather than indefinite. Sharing should be controlled rather than automatic. Misuse should have consequences.

The existence of an emergency should not, standing alone, erase those protections. Nor should surveillance technology be used merely to identify or monitor citizens because they are attending church, participating in lawful political activity, exercising free speech, assembling peacefully, working as journalists, or otherwise exercising constitutionally protected rights.

We do not need to fear technology. We need to govern it.

The difference between technology that protects liberty and technology that threatens liberty is often not the technology itself. It is the law, policy, accountability, and constitutional restraints governing the people who control it.

Give law enforcement the tools necessary to protect this county. Give our officers clear rules governing those tools. Protect legitimate investigations. Protect taxpayer-funded information. Protect the Constitution. And protect the liberty of the citizens whom county government exists to serve.

Those goals are not in conflict. Good government requires us to do all of them.

I am not asking Freestone County to choose between law enforcement and liberty; I am asking us to establish the rules that allow us to protect both.

Recommended Policy Framework

For consideration by the Freestone County Commissioners Court and Sheriff. This is a policy framework, not an attempt to prescribe investigative tactics or supersede the lawful authority of an independently elected official.

1. Purpose and scope

Apply written safeguards to county acquisition, operation, access, contracting, or participation involving ALPR/Flock systems and materially similar AI-enabled, biometric, facial-recognition, or location-tracking surveillance technology.

2. Lawful and defined uses

Limit use to legitimate public-safety and law-enforcement purposes authorized by law and departmental policy, including bona fide criminal investigations, stolen vehicles, wanted persons, missing persons, Amber/Silver Alerts, officer safety, and comparable lawful purposes.

3. Protected constitutional activity

Do not use surveillance technology solely to identify, catalog, or monitor persons because of lawful religious worship, political activity, peaceful assembly, speech, journalism, association, or other constitutionally protected activity.

4. Authorized users and training

Require individual user credentials, role-based access, appropriate authentication, and documented training before access. Shared user accounts should be prohibited.

5. Documented search justification

Require a case number, incident number, dispatch number, intelligence reference, or other documented legitimate purpose for searches whenever practicable. Emergency searches should be documented promptly afterward.

6. Verification before enforcement

Treat an ALPR alert as an investigative lead. When circumstances permit, verify the plate, vehicle, wanted status, and other relevant information through an authoritative source before enforcement action.

7. Audit trail and supervisory review

Maintain logs showing the user, date/time, query, and documented purpose. Require periodic supervisory review and investigation of anomalous or suspected unauthorized searches.

8. Data retention and destruction

Adopt a specific, defensible retention period for routine data. Information lawfully preserved as evidence may be retained separately under applicable evidence and records-retention requirements. Avoid indefinite retention merely because storage is available.

9. Interagency and network sharing

Define which agencies may receive county-originated data and under what circumstances. Define when county personnel may search outside networks. Do not make broad or nationwide sharing automatic merely because a vendor offers it.

10. No automatic mission creep

Acquisition or possession of hardware, software, a subscription, database access, or a vendor-added capability shall not by itself constitute authorization to use a materially new surveillance capability. New AI, facial-recognition, biometric, predictive, or expanded location-tracking functions should undergo legal and policy review before operational use.

11. Vendor and contract protections

Address ownership and control of county data, cybersecurity, breach notification, subcontractors, secondary/commercial use, compliance with retention requirements, access upon termination, and verified deletion when appropriate.

12. Emergency safeguards

A declared emergency shall not, standing alone, authorize a use otherwise prohibited by policy. Extraordinary use should require specific lawful authority, documented justification, appropriate supervision, and auditability.

13. Misuse and consequences

Unauthorized searches, disclosure, or use should result in immediate review, possible suspension or revocation of access, appropriate departmental discipline, and referral for criminal or other investigation when warranted.

14. Citizen complaints and incident response

Provide a clear process for reporting suspected misuse, data breaches, or improper disclosure, and establish responsibility for investigating and documenting those complaints.

15. Public transparency with operational security

Once developed and adopted, post the policy publicly on the Freestone County website, preferably under the Sheriff's Office page and under the page of any other county agency that uses or accesses the technology. The public posting should make the basic rules governing governmental use easy to find while protecting information that lawfully must remain confidential, including investigative techniques, security vulnerabilities, credentials, and sensitive operational details.

16. Records management

Address retention, preservation, disclosure, and destruction in accordance with applicable Texas records law, evidentiary requirements, court orders, and lawful public-information exceptions.

17. Periodic review

Review the policy at least annually and whenever material changes occur in law, vendor capability, interoperability, artificial intelligence, data-sharing networks, or departmental practice.

18. Governance principle

Policy should remain effective regardless of who holds office. Safeguards should be designed for future administrations as well as the officials whom citizens trust today.

Guiding principle: Give law enforcement effective tools, but place durable constitutional guardrails around governmental power.

Suggested Next Steps

- Ask the Sheriff and any affected county department to identify whether it currently owns, operates, accesses, or receives information from any ALPR or comparable network.
- If access exists, inventory current written policies, contracts, MOUs, retention settings, sharing settings, authorized users, audit controls, and training requirements.
- Compare existing policy against this framework and applicable Texas law, DPS requirements, records-retention rules, and current law-enforcement best practices.
- Have the appropriate elected official or department develop operational procedures, with legal review as appropriate, while the Court addresses matters within its own authority such as funding, contracts, county data, records, and countywide governance.
- Return any proposed policy or material contract to the appropriate public process for consideration, while protecting confidential law-enforcement information as required by law.

Research Basis

This framework is informed by Texas public-safety guidance and records-retention requirements, law-enforcement policy best practices, and recent state/local debates over ALPR use. It is intentionally written as an administration-neutral governance framework rather than as a partisan platform document. Specific legal requirements should be reviewed by the County Attorney or other appropriate counsel before formal adoption.

- Texas Department of Public Safety - License Plate Reader Program guidance.
- Texas State Library and Archives Commission - Local Schedule PS (Public Safety Records), including ALPR-related records.
- International Association of Chiefs of Police - guidance on responsible automated license plate recognition use.
- Texas legislative materials concerning ALPR safeguards and catalytic-converter-theft grant funding.
- Recent state and local actions concerning Flock/ALPR systems, including Texas and Florida developments, used as comparative policy examples rather than as evidence of Freestone County conduct.

Respectfully submitted,

Robert P. Sharpe - RancherRob
Simsboro, Texas