

Securing Public Trust in LPR



Why Flock Safety is the privacy-protecting license plate recognition (LPR) choice for cities – legally, technically, and reputationally.

As communities demand both safety and accountability, city leaders must **ensure that any LPR program is designed to protect civil liberties and remain in compliance** with local laws and policies. The Flock LPR system is built with Privacy by Design: we collect only what is visible from public roadways, enforce strict retention, and hard-code safeguards that limit inappropriate access.

The Flock Standard: Four Ways Communities Can Improve Public Trust Around LPR

Flock's LPR ensures community safety doesn't come at the expense of community values.



Federal Sharing Safeguards

Flock does not contract with ICE or DHS.



No Data Resale

Flock does not sell or share LPR data and is not a data broker.



Breach and Security Risk

Flock uses CJIS-aligned controls (including encryption at rest and in transit) and our cloud has never been compromised.



Built In Transparency

Flock offers permanent audit trails, automatic data deletion, and transparency portals

What Flock LPRs Collect (and What We Don't)



Collected:

License Plate Text, Date/Time, Camera Location, and Basic Vehicle Attributes (Make/Model/Color) - All Observable From Public Roadways.



Not Collected:

Names, Addresses, Phone Numbers, Driver Identity, Biometric Identifiers, or Other Confidential Personal Information.

Bottom line: Flock's LPR is **not connected** to DMV records and does not build a database of people, only vehicle attributes already visible in public



Safeguards That Limit Federal Access



No national or statewide lookups for federal agencies: federal agencies are excluded from the nationwide and statewide network search capabilities.



Compliance with state-level restrictions: in states such as California and Virginia, legal restrictions that govern federal or out-of-state access to LPR data are coded directly in the platform to help customers with compliance.

Council FAQ

Q: How do we know this won't be used for unauthorized immigration enforcement?

A: There is no backdoor access into Flock. Flock does not contract with ICE or DHS, and federal agencies are excluded from national and statewide network search capabilities. In states such as California and Virginia, legal restrictions that may limit federal or out-of-state access to publicly funded LPR data are supported within the platform to help agencies comply.

Q: Does LPR capture confidential personal information?

A: No. Flock captures plates and vehicle characteristics that are visible from public roadways. It does not capture names, addresses, phone numbers, or driver identity.

Q: What happens to the data after 30 days?

A: By default, it is permanently deleted via a 30-day hard delete, supporting investigations while limiting long-term surveillance risk.

Q: If a citizen complains about misuse, can we audit access?

A: Yes. Every search requires a justification, and agencies can access a comprehensive audit trail for their organization showing who searched, when, and why.



The Executive Takeaway

If your city is considering LPR, the critical question is not whether LPR works, it's whether your vendor minimizes legal, security, and reputational risk. Flock's Privacy-by-Design model, hard-coded safeguards limiting federal access, strict default retention, and CJIS-aligned security controls make it the **lowest-risk LPR option to defend in public.**

