

Frequently Asked Questions

FLOCK Cameras, Public Safety, and Privacy

(Informed by recent community and media coverage)

Q1: There's a lot of concern online that these cameras are an invasion of privacy. How do you respond?

A:

We understand why people are asking questions—any new technology should be scrutinized. These cameras are not designed to monitor people. They capture license plates and basic vehicle characteristics **after a crime occurs**, not individuals going about their daily lives. They do not identify drivers or passengers, and they do not use facial recognition.

Q2: Some posts claim data from FLOCK cameras “goes places it doesn’t belong.” Is that true?

A:

No. The City owns 100 percent of the data collected. The vendor does not own it, cannot sell it, and cannot use it for any other purpose. Data is only accessed by authorized personnel for legitimate investigations, and sharing requires specific City approval. There is no commercial use and no uncontrolled sharing.

Q3: A commenter mentioned a video claiming FLOCK cameras can be easily intercepted or hacked. How secure is the system?

A:

The system uses encrypted data transmission and secure government-grade cloud infrastructure. Once data uploads, it is removed from the physical camera itself. Like all technology, security is taken seriously, which is why access is limited, activity is audited, and the City maintains oversight and contractual security requirements. There is no evidence of unauthorized access to City data.

Q4: Why are FLOCK cameras installed at places like shopping centers or home improvement stores?

A:

Those locations are frequent targets for vehicle theft and organized retail crime. Cameras are positioned to capture vehicles entering and exiting high-risk areas—not to monitor shoppers. The focus is on identifying suspect vehicles connected to crimes, not on recording where people shop.

Q5: Several articles point out that other cities, like Flagstaff, have canceled their contracts. Why is El Paso continuing?

A:

Every city makes decisions based on its own policies, oversight, and community expectations. El Paso has used license plate reader technology since 2006, under multiple City Councils, without privacy violations. Our program includes strict retention limits, ownership protections, and oversight measures that may differ from other jurisdictions.

Q6: Are these traffic cameras or revenue-generating tools?

A:

No. These are not traffic enforcement cameras. They do not issue tickets, do not monitor speed, and do not generate revenue. They are investigative tools used after crimes occur.

Q7: How does this technology help the City do more with existing public safety resources?

A:

This technology helps investigators identify suspect vehicles and develop leads more quickly. It helps officers use their time more efficiently, while the City continues to hire and invest in sworn personnel, and it supports a faster response across investigations, including vehicle theft and violent crime.

Q8: Does this help keep car insurance costs down for residents?

A:

The cameras were supported through a state grant focused on reducing motor vehicle theft. While insurance rates are set by insurers and depend on many factors; reducing auto theft can reduce claims over time, which can help ease cost pressure for residents and businesses.

Q9: Do these cameras track people over time or build profiles of residents?

A:

No. The system does not track people, does not build profiles, and does not follow vehicles for general monitoring. Searches require a specific investigative purpose and are tied to case numbers. Data is automatically deleted after 30 days unless it is evidence in an active case.

Q10: Are these cameras being used to watch protests, religious services, or political activity?

A:

No. City policy explicitly prohibits using this technology to monitor First Amendment–protected activities, including protests, religious gatherings, or political events. Any such use would violate policy and result in discipline.

Q11: Can this data be used for immigration enforcement or civil code enforcement?

A:

No. The system is not used for immigration enforcement, civil code enforcement, or parking enforcement. Its use is limited to serious criminal investigations and public safety emergencies.

Q12: Who inside the Police Department can access the system?

A:

Only trained, authorized personnel. Every search is logged, audited, and subject to supervisory review. Misuse is not tolerated and results in disciplinary action.

Q13: How long is data kept?

A:

Data is automatically deleted after 30 days. This is a long-standing standard in El Paso. Data is retained longer only if it is formally tied to an active criminal investigation.

Q14: Is this technology new for El Paso?

A:

No. El Paso has responsibly used license plate reader technology for nearly two decades. What's different today is our emphasis on transparency, public-facing policies, and modernized security standards.

Q15: What cybersecurity safeguards are in place to protect the system and the data?

A:

Protecting City data is a core requirement of this program. The City's information security team has reviewed the technology and associated controls. Access is restricted to authorized users and requires multi-factor authentication. All activity is logged and auditable, and contractual requirements prohibit the vendor from selling or monetizing City data. Data is retained for a limited period unless formally preserved as evidence in an active criminal investigation.

Q16: How is the City responding to public concern raised online and in the media?

A:

We take public concern seriously. That's why we publish our policies, provide transparency portals and continue to review how the technology is used. Community trust matters, and we will adjust if expectations or best practices evolve.

Q17: What should residents take away from all of this?

A:

This is a carefully controlled investigative tool—not mass surveillance. It is designed to solve crimes, protect victims, and improve public safety while respecting privacy and constitutional rights.