



Thornton Police Education & Engagement Series, Session #3

Cameras and Technology | July 30, 2026

Follow-up Information Requested by Attendees

Results from QR code quiz

- Flock cameras use facial recognition.
 - 12 answers
 - True – 3
 - False – 9
 - **Correct answer: False (75% answered correctly)**

Flock license plate readers do not use facial recognition technology. Searches are based on vehicle characteristics — Flock cannot recognize, identify, or track individuals.

Colorado Senate Bill 22-113 requires any state or local agency that uses, develops, or procures facial recognition technology to file a notice of intent with its reporting authority (City Council) and specify the technology's purpose. Thornton PD has not filed that notice — meaning by law, TPD does not and cannot use facial recognition.

- ALPR data is stored for 90 days before being automatically deleted.
 - 12 answers
 - True – 4
 - False – 8
 - **Correct answer: False (67% answered correctly)**

Thornton PD's ALPR data is stored for 30 days before being automatically deleted, unless it's specifically retained as evidence in an ongoing criminal investigation.

Retention periods vary by agency, so other communities may store data for longer or shorter windows.

- Thornton PD can use ALPRs to watch where your car goes throughout the day — like the grocery store, the doctor, or your kid's school.
 - 12 answers
 - True – 6
 - False – 6

- **Correct answer: False (50% answered correctly)**

ALPRs capture a single image at a single point in time, in a single location, typically showing the rear of the vehicle. Each camera works independently and only records vehicles that pass directly in front of it. An ALPR camera does not follow, track, or monitor a vehicle's movement throughout the day. It also does not know who is driving, where the vehicle is coming from, or where it is headed next.

If a vehicle happens to pass multiple ALPR cameras, TPD can see that it was in more than one location at different times, but this is not the same as active, real-time tracking or continuous surveillance of someone's daily movements.

- Federal law enforcement agencies can request Thornton's ALPR data.

- 13 answers

- True – 11
- False – 2

- **Correct answer: False (15% answered correctly)**

Federal agencies do not have the ability to request TPD's ALPR data through the Flock system. TPD controls its own data sharing settings and those settings do not permit federal agencies to even request access.

- Per department policy, any Thornton officer can look up your travel history using ALPRs whenever they want.

- 12 answers

- True – 1
- False – 11

- **Correct answer: False (92% answered correctly)**

All ALPR searches must be for a legitimate public safety purpose, and every search is logged and auditable. Any allegation of misuse of Thornton Police Department data, including Flock data, is subject to investigation and discipline if sustained.

- Officers are required to enter a case number every time they search ALPR data.

- 12 answers

- True – 6
- False – 6

- **Correct answer: False (50% answered correctly)**

Officers are required to have a legitimate public safety purpose for every ALPR search, which may include a case report number, call for service number, or another documented investigative reason. Real-time alerts are the exception. Officers use

these alerts to quickly check whether a vehicle has appeared elsewhere in Thornton, helping locate stolen vehicles or vehicles connected to a crime. When an alert was set by another agency, TPD personnel may not have immediate access to that agency's case report number. Requiring a case number for each of these checks isn't practical and would slow down real time investigations. Even so, all searches must be tied to an active investigation or training purpose, and department policy is reviewed and updated as the technology evolves.

- Thornton has revoked more than 2,000 outside agencies' access to its ALPR data.
 - 14 answers
 - True – 11
 - False – 3
 - **Correct answer: True (79% answered correctly)**

The Thornton Police Department audits searches of its ALPR data regularly to ensure they comply with state law and department policy. If a search is conducted by an outside agency for a reason that is not consistent with those requirements, the agency's access to Thornton's data may be revoked. Access is most often revoked when a search does not include a clear investigative reason.

- Businesses that use their own ALPR cameras automatically share their data with the city.
 - 14 answers
 - True – 0
 - False – 14
 - **Correct answer: False (100% answered correctly)**

Some private businesses in Thornton, such as Home Depot, use ALPR systems on their own property. Access to that data is controlled by the business and can only be shared with individual law enforcement agencies at their discretion. Other agencies cannot access this ALPR data from TPD.

- Flock Safety sells Thornton's ALPR data.
 - 14 answers
 - True – 1
 - False – 13
 - **Correct answer: False (93% answered correctly)**

Flock does not sell customer data. Customers, including TPD, remain in control of their data at all times and choose who that data is shared with.

What is the cost of the red-light camera program?

From January through June of 2026, Thornton Police Department has spent \$235,200 on the red-light camera program.

What is the cost of Body Worn Cameras?

The Thornton Police Department currently utilizes a consolidated technology bundle through Axon which includes Body Worn Cameras, Tasers, interview room recording technology, and a digital evidence management system. The annual cost for these bundled systems is \$561,172.

How long are Body Worn Camera videos retained?

Body worn camera video is retained in accordance with the City of Thornton Records Retention Schedule.

- Major felonies and violent crimes (i.e., arson with fatalities, forgery, unrecovered firearms, homicides, kidnapping, deaths, sexual assault on a child and officers killed.) are retained permanently.
- Sexual Assaults (excluding sexual assault on a child) are retained for 99 years.
- Other felony crimes, death investigations (non-criminal), or traffic fatalities are retained for 10 years.
- Internal Affairs Investigations and Police Action (i.e., reviews of use of force, pursuits, officer-involved traffic accidents, etc.) retained for 5 years.
- Misdemeanor crimes, code compliance, non-fatal traffic crashes, and traffic stops are retained for 3 years.
- Non-evidentiary recordings are retained for 2 years.

Is Thornton PD ALPR data automatically deleted?

Yes, all TPD ALPR data is automatically deleted after 30 days, unless it is specifically retained as evidence in an ongoing criminal investigation. See below for more detailed information about data deletion.

The following information is provided by Flock Safety:

Flock uses Amazon Web Services cloud storage and Key Management Service (KMS)-based encryption, limiting access to the encryption keys. All CJIS data is stored in the AWS GovCloud and is only available to Law Enforcement agencies. No CJIS data is shared with non-Law Enforcement Flock Safety Customers.

AWS is the only cloud provider that is CJIS compliant in all 50 states. The zero-trust security model built on AWS KMS and the Nitro System means that when you delete Criminal Justice Information (CJI), you can be confident that:

- *The data is permanently removed from Simple Storage Service (S3)*
- *No AWS personnel had access to it before, during, or after deletion*
- *The deletion is logged and verifiable through CloudTrail*

AWS's deletion mechanisms align with requirements from:

- *GDPR (Right to Erasure / Right to be Forgotten)*
- *SOC 2 (Data retention and disposal controls)*
- *ISO 27001 (Information security management)*
- *NIST 800-53 (Security and privacy controls)*
- *FedRAMP (Federal security requirements)*

Data deletion is enforced automatically at the AWS infrastructure level and backed by verifiable, tamper-proof logs. Once the 30-day retention threshold is reached, data is irreversibly purged and cannot be recovered by anyone – including Flock or AWS.

There are four key pillars in place for verifiable data deletion:

1. Automated & Irreversible Purging

- *S3 Lifecycle Policies: Deletion is fully automated. At the 30-day mark, AWS S3 Lifecycle rules automatically trigger permanent object deletion without requiring human intervention.*
- *Irreversible Action: Per AWS core architecture, once an object or object version is permanently deleted, it cannot be retrieved by any mechanism.*

2. Tamper-Proof Audit Trail (Chain of Custody)

- *AWS CloudTrail & Server Access Logs: Every automatic deletion generates a cryptographic, timestamped event. These logs record what was deleted, when it was deleted, and which policy triggered it.*
- *Integrity Validation: CloudTrail logs use cryptographic validation to prove they have not been altered, forged, or deleted, providing a forensically sound audit trail.*

3. Real-Time Verification & Searchability

- *CloudWatch Monitoring: System metrics (such as total object counts and storage size) actively monitor and confirm storage reduction as deletions occur. Alerts trigger if automated deletions ever fail or pause.*

- *OpenSearch Audit Logs: Index and user activity logs capture deletion events, providing searchable proof of record deletion.*

4. Hard Infrastructure & Cryptographic Guarantees

- *Crypto-Shredding: Data is encrypted using AWS KMS. Deleting or revoking the encryption key renders any residual bits permanently unreadable.*
- *AWS Nitro System: Physical hardware isolation prevents any AWS personnel from accessing or restoring customer data before, during, or after deletion.*

What is the cost of the Flock system?

Thornton Police Department pays approximately \$51,000 per year for the Flock system.

What is the average number of weekly searches by TPD staff in the system?

The number of total user search sessions over the last 30 days can be found on [TPD's Flock Transparency Portal](#).

Published on Aug. 19, 2026