To: Chairman McKay and the Fairfax County Board of Supervisors,

Thank you for your letter seeking information about the technical and contractual safeguards Flock has put in place to ensure Fairfax County's LPR deployment is aligned with Virginia law, Fairfax County Police's policies, and the values of your community. As the Founder and CEO of Flock, I take nothing more seriously than building our technology to enhance public safety while enabling accountability and transparency.

Enclosed within this packet are the detailed answers to your specific questions and technical documentation to support your inquiries about data deletion and sharing, auditing and accountability, and machine learning training. However, I wanted to share a few of the most important principles we hold at Flock up front.

What Flock License Plate Recognition (LPR) technology is and is not

- Flock's LPR cameras are motion-activated cameras that capture still images of vehicles. They do not record live video and do not enable the search of people.
- Flock does not utilize facial recognition capabilities in any of our products.

Data Ownership and Sharing

- All Flock customers own and control the data collected by our technology on their behalf. Flock has never sold and will never sell customer data.
- Only the customer can choose whether or not to share their data with any other law enforcement agency. There is no sharing enabled by default.

Local Control and Virginia Safeguards

Flock has implemented technical controls in Virginia to ensure LPR is used in accordance with state law:

- Restrictions on Federal/Out-of-State access: Virginia LPR law (§ 2.2-5517) prohibits law enforcement agencies from sharing or disseminating LPR data to any out-of-state or federal entity. Virginia-based Flock customers are not visible to federal users or out-of-state agencies for sharing requests.
- 21 day retention schedule: Virginia LPR law (§ 2.2-5517) sets a maximum of 21 day retention for Virginia law enforcement users, so this is the maximum permitted for these customers in the Flock system.
- Prohibited searches: To comply with VC § 15.2-1726.1, Flock applied a statewide search filter that blocks searches that indicate they may be related to immigration enforcement.

I have full confidence that Flock's LPR system can continue to solve crime and keep Fairfax County residents safe, while remaining in accordance with state law and local policy. I also welcome the opportunity to meet individually with any of you, the full Commission, or bring in my Legal, Policy, or Product teams to dive deeper on any of these topics.

We value our partnership with Fairfax County and look forward to the continued impact we can make together.

Sincerely,



Garrett Langley, CEO and Founder, Flock

flocksafety.com (866) 901-1781 | support@flocksafety.com

1. Who owns, controls, and can access Fairfax County's data?

What does it mean in practice that customers own and control their data? Can Flock employees, contractors, or subcontractors access, copy, or use Fairfax County's data for product improvement or AI development? Can Flock make material changes to data policies without approval?

- **Data Ownership**: Flock customers, including Fairfax County, own all the data classified as "customer data" gathered by their systems. This is clearly defined in section 1.6 of our Terms & Conditions: "Customer Data" means all (a) data and information captured by Flock Hardware on behalf of Customer through the Flock Services (e.g., images, audio, and/or video) and metadata associated therewith, (b) content input into the Web Interface by Customer or its Authorized End Users, and (c) data and information provided to Flock through the Flock Services by third parties at Customer's direction. In plain terms, all images, associated metadata, and search information is owned by the customer. Flock's Terms (Section 4.1) explicitly state that Flock cannot sell customer data.
- **Flock Employee Access:** Access to customer data by Flock personnel is strictly limited. Flock personnel do not have general access to customer data, all access is contractually limited and occurs only when reasonably necessary to provide customer support or address system issues. The same policy applies for contractors and subcontractors. Additionally, all access is logged and reviewable.
- **Use for Machine Learning Development:** To improve the accuracy of our Vehicle Signature™ technology, Flock uses a fraction (less than one percent) of aggregated images, which are stripped of all metadata and identifying information, from customers who have opted into allowing this. Based on Flock's interpretation of Virginia state law, no Virginia agency data is included in this machine learning training.
- **Product Improvement:** Flock can aggregate and analyze product usage information for product improvement. For example, if Flock is assessing whether a feature is valuable or not to users, it can look at aggregated usage data for the feature to understand how often it is used.
- **Policy Changes:** Flock cannot make material changes affecting data retention, search, or sharing without customer approval. These settings are controlled by the customer within the platform.

2. Can anyone outside Fairfax County access Fairfax County's data?

Can an officer or agency outside Fairfax County, including federal agencies like ICE or DHS, query and receive results from Fairfax County cameras without local approval?

- **General Flock Policy**: Access by any outside entity is under full control of the customer. No sharing relationship is automatically on and any sharing relationships can be granted, changed, or revoked only by Fairfax County.
- **Federal Agency Access:** For any federal agency to access a local agency's data, a three-gate system must be completed:
    - The local agency must first change its settings to opt-in to receiving sharing requests from federal agencies (this is off by default).
    - The federal agency must submit a formal request for access.
    - The local agency must review and approve that specific request.
- **Flock does not have a contract with ICE.**
- **Virginia-Specific Compliance**: Virginia state law (§ 2.2-5517) prohibits law enforcement agencies from sharing or disseminating LPR data to any out-of-state, federal, or private/commercial entity, with limited exceptions. Flock's system is designed to technically enforce these state-level restrictions. Agencies in Virginia are not visible to federal users or out-of-state agencies for sharing requests.

3. How are interstate legal conflicts prevented?

What prevents an outside agency from using Fairfax County's data to investigate conduct that is legal in Virginia? Does Flock technically enforce Virginia law, and can Fairfax County block specific jurisdictions or categories of searches?

- **Virginia-Specific Compliance:** Virginia law prohibits sharing LPR data with out-of-state and federal agencies, and our platform technically enforces this by preventing such sharing connections from being made. To prevent searches for prohibited purposes, for all Virginia agencies Flock has automatically applied Search Filters that block attempts to search for terms related to immigration.

4. What can Flock's AI and advanced searches actually do?

What are the capabilities of Flock's AI and advanced searches, including natural language, pattern searches, and tools that might tie searches to individuals? What controls prevent "fishing expeditions," and can they be overridden?

- **LPR Machine Learning**: Flock's Vehicle Signature™ technology used to provide objective, actionable evidence about vehicles. Its primary functions are Optical Character Recognition (OCR) to read license plates and machine learning to identify vehicle characteristics like type, make, and color. No Flock devices use facial recognition.
- **FreeForm Search**: FreeForm is an advanced search capability that allows investigators to use natural language to search for vehicles based on descriptions (e.g., "blue Honda with a bike rack"). This feature is moderated to flag queries that could be inappropriate, such as specific language that would implicate First

Amendment rights. FreeForm Search on LPR focuses on vehicles and cannot be used to search for people.

- **Auditing Controls**: All searches are subject to the same strict auditing requirements. Every query requires a documented Offense Type and, starting Jan. 1, 2027, a case code (as of Jan. 1, 2027). The Offense Type and Case code are recorded in an audit log, along with the time, user, and parameters of the search. These controls cannot be overridden by users. In addition, Flock has implemented a tool called Audit Assistance, an automated monitoring tool designed to detect abnormal search activity and flag it for administrator review.



How do you know Data is Actually Deleted?

Proving Data Deletion in AWS

May 8, 2026
Flock AWS Account Team

Summary

One of the questions customers ask is: "How do I know my data is actually deleted?" This is a fair question — especially for organizations handling sensitive data subject to compliance requirements like CJIS. This white paper explains how AWS ensures data is permanently removed from Amazon S3 buckets, and how Flock's use of these services in their AWS environment — S3 Lifecycle Policies, AWS CloudTrail, Amazon CloudWatch, and Amazon OpenSearch — work together to provide verifiable proof that deletion has occurred.

The short answer: AWS provides multiple layers of evidence — from API-level audit logs to automated deletion policies to real-time monitoring — that together create an airtight chain of custody that your data has been permanently removed.

How S3 Deletion Actually Works

What Happens When You Delete an Object

When an object is deleted from Amazon S3, the behavior depends on whether versioning is enabled:

- **Without versioning**: The object is permanently deleted. It cannot be recovered. AWS confirms the deletion by returning a "deleted" result in the API response.
- **With versioning**: A "delete marker" is placed on the object, making it invisible to normal requests. The previous version still exists until you explicitly delete it or a lifecycle policy removes it.
- **Permanent deletion of a version**: When you delete a specific object version (or when a lifecycle policy expires it), that version is permanently removed from AWS infrastructure. It cannot be recovered by anyone — including AWS.

Key Point: Deletion Is Irreversible

AWS documentation is explicit: "Deleting an object can't be undone." Once an object or object version is permanently deleted, there is no mechanism — not even for AWS engineers — to retrieve it. This is by design and is enforced at the infrastructure level.

S3 Lifecycle Policies: Automated, Guaranteed Deletion

What They Do

S3 Lifecycle Policies are configurable rules that automatically manage objects throughout their life.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

How You Know It Worked

1. **The policy is declarative and auditable**: Your lifecycle configuration is stored as part of the bucket's settings. You can retrieve it at any time to confirm what rules are in place.
2. **S3 executes lifecycle rules automatically**: Once configured, AWS guarantees execution. Objects that meet the expiration criteria will be deleted — there is no manual step that could be skipped.
3. **CloudTrail logs the lifecycle actions**: Every object expiration triggered by a lifecycle policy generates a CloudTrail event, giving you a timestamped record of what was deleted and when.
4. **You can verify absence**: After expiration, attempting to retrieve the object returns a "404 Not Found" or "NoSuchKey" error — direct proof the object no longer exists.



EXAMPLE-A typical compliance-oriented lifecycle policy might include:

- *Permanently delete noncurrent versions after 30 days*
- *Remove expired delete markers after 1 day*

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

This ensures that even versioned objects are permanently purged within a defined, auditable timeframe.

AWS CloudTrail: Your Deletion Audit Trail

What CloudTrail Captures

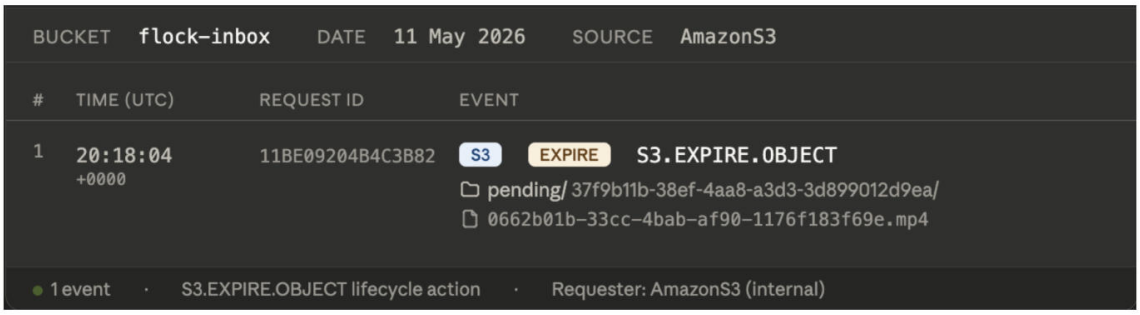
AWS CloudTrail records every API call made in your AWS account. For S3 deletion, this includes:

- **DeleteObject** — Records who deleted what object, from which bucket, at what time, and from what IP address.
- **DeleteObjects** (batch) — Same as above, but for bulk deletions.
- **Lifecycle-triggered expirations** — In addition to Amazon CloudTrail, Amazon S3 Server access logging provides detailed records for the requests that are made to a bucket. When S3 automatically deletes objects based on lifecycle rules, they are captured in Amazon S3 server access logs.
- **PutBucketLifecycleConfiguration** — Records when lifecycle policies are created or modified, and by whom.

Why This Matters for Proving Deletion

AWS CloudTrail and S3 Server Access Logging gives you:

- **Who** performed or triggered the deletion
- **What** was deleted (bucket name, object key, version ID)
- **When** it happened (precise timestamp)
- **How** it was initiated (console, CLI, SDK, or lifecycle automation)
- **Tamper-proof records**: CloudTrail supports log file integrity validation. You can cryptographically verify that log files have not been modified, deleted, or forged after delivery. This means your deletion records are forensically sound.



Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Amazon CloudWatch: Real-Time Deletion Monitoring

Metrics That Prove Deletion Is Happening

CloudWatch provides S3 bucket-level metrics that give you visibility into deletion activity:

- **NumberOfObjects**: Track the total object count in a bucket over time. A declining count after lifecycle policies take effect is direct evidence of deletion.
- **BucketSizeBytes**: Monitor total storage size. Decreasing storage confirms objects are being removed.
- **Custom Metrics**: You can publish custom metrics from CloudTrail events to track deletion rates, failed deletions, or anomalies.

Alarms and Anomaly Detection

You can configure CloudWatch to:

- **Alert you if deletions stop**: If your lifecycle policy should be deleting objects daily but the object count plateaus, an alarm can notify you of a potential issue.
- **Detect anomalous deletion patterns**: Unusual spikes in deletion activity could indicate unauthorized access — CloudWatch anomaly detection can flag these automatically.
- **Create dashboards**: Build visual dashboards showing deletion trends over time for compliance reporting.

Amazon OpenSearch Service: Audit logs

Enabling Audit logs in Amazon OpenSearch cluster enables tracking user activity on OpenSearch clusters, including authentication success and failures, requests to OpenSearch, index changes, and incoming search queries. These audit logs are automatically vended to CloudWatch Logs. When indices are deleted in Amazon OpenSearch Service, the audit log captures this as an INDEX_EVENT category on the transport layer. Additional key fields for index deletion events include the index/indices being deleted, who performed the deletion and when it occurred providing chain of custody documentation.

Auditability for Amazon S3 and Amazon OpenSearch objects

When all four services are combined, you get an end-to-end deletion verification system:

	Layer	What It Proves	Evidence Type
1	**S3 Lifecycle Policy**	Deletion rules are in place and enforced	Configuration (auditable, versioned)

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

2	**S3 API Response**	Individual objects were deleted successfully	Real-time confirmation
3	**AWS CloudTrail**	Who deleted what, when, and how	Tamper-proof audit logs
4	**Amazon CloudWatch**	Deletion is happening at expected rates	Metrics, trends, and alarms
5	**Audit Logs for Amazon OpenSearch**	Who deleted what, when, and how	Tamper-proof audit logs

AWS Infrastructure-Level Guarantees

AWS provides infrastructure-level assurances:

Physical Media Handling

- AWS storage devices are decommissioned using techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization").
- Storage media is cryptographically erased or physically destroyed when decommissioned.
- AWS data centers undergo regular third-party audits (SOC 1, SOC 2, SOC 3, ISO 27001) that verify these processes.

Encryption at Rest

- Flock's is encrypted with AWS KMS (which is recommended and relevant to your CJIS compliance posture), deleting the encryption key renders all encrypted data permanently unreadable.
- This provides a "crypto-shredding" capability: destroy the key, destroy access to the data.

The Nitro System and Zero-Trust Architecture

As noted in your CJIS compliance documentation, the AWS Nitro System ensures that AWS personnel cannot access customer data on the underlying infrastructure. This means:

- No AWS employee can recover your deleted data
- The hardware itself enforces isolation
- Customers retain complete control and ownership of their data

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Compliance and Regulatory Alignment

CJIS Compliance

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 S3
- No AWS personnel had access to it before, during, or after deletion
- The deletion is logged and verifiable through CloudTrail

Additional Compliance Frameworks

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)

Conclusion

The question "How do you know if data is actually deleted?" has a clear, multi-layered answer on AWS:

- **You configured it**: Lifecycle policies define exactly when and how data is removed.
- **AWS executed it**: S3 automatically and irreversibly deletes objects per your policies.
- **You have proof it happened**: CloudTrail provides tamper-proof, timestamped records of every deletion.
- **You can see it in real time**: CloudWatch metrics show deletion activity as it occurs.
- **You can search the evidence**: OpenSearch gives you instant access to your complete deletion history.
- **The infrastructure guarantees it**: The Nitro System, KMS encryption, and NIST 800-88 media handling ensure data cannot be recovered by anyone — including AWS.

For an organization like Flock Safety operating under CJIS requirements, this combination of automated policies, cryptographic verification, real-time monitoring, and

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

infrastructure-level guarantees provides the highest level of assurance that deleted data is truly, permanently gone.

References/Supporting Documentation:

- **Deleting objects from a directory bucket** — docs.aws.amazon.com/AmazonS3/latest/userguide/directory-bucket-delete-object.html
- **Deleting multiple objects** — docs.aws.amazon.com/AmazonS3/latest/userguide/delete-multiple-objects.html
- **Deleting objects (S3 console)** — docs.aws.amazon.com/AmazonS3/latest/userguide/delete-objects.html
- **Nitro**- https://aws.amazon.com/ec2/nitro/
- AWS Digital Sovereignty Pledge: Control without compromise

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Flock Safety

Flock Safety Policy for Responding to Legal Demands for Customer Data

Overview

Flock Safety is committed to honoring our contractual obligations to our customers to protect the integrity and privacy of customer data, in compliance with all federal and state laws.

When Flock is confronted with requests for information, Flock always:

- analyzes the source of the request, the context, and legality;
- notifies and works with the affected customer, when allowed by law; and
- responds when a court orders Flock to provide data.

Methods of Service

As a threshold matter, Flock will analyze if the requesting party properly served Flock with legal process. Flock has established protocols in our Evidence Policy by which we will accept legal process from law enforcement; all other entities must comply with traditional methods to effectuate legal service of process in order to compel a response from Flock.

Preservation

If Flock determines that it has been properly served with legal process, Flock will evaluate whether to place a temporary hold to preserve the requested data while it performs the process outlined below.

Notification

In strict adherence to Flock's Privacy Policy, we will use reasonable efforts to provide notice to the customer(s) whose data is the subject of the legal demand ("affected customer") when legal demands are received, unless we are explicitly prohibited from doing so by law. Flock

will notify customers when any such data is sought in response to required disclosures from government, law enforcement, or third parties. Flock will give customers seven calendar days to pursue any legal remedy to challenge the legal demand. Notice may be reasonably withheld if prohibited by law or if Flock believes that such notice may pose immediate risk of serious injury or death to a member of the public.

Process

Court Ordered Demands

Flock will convey to the requesting agency that data is owned exclusively by the affected customer and will request that the legal process be redirected to the affected customer.

Flock's policy is to respond to compulsory legal demands that Flock determines, in good faith, are not overbroad and appear relevant to a legitimate purpose.

Flock carefully reviews all submissions to ensure that there is a valid legal basis for each request. If any request is considered to be unclear, inappropriate, over-broad, or without legal basis, Flock reserves the right to challenge or reject such request.

Compulsory Process - Customer and Flock Object

Should Flock—or when able to be notified, Flock jointly with the affected customer—have a good-faith legal objection to a properly served compulsory legal demand, Flock may initiate formal judicial review. Flock will comply with any final judicial decision.

Compulsory Process - Only Customer Objects

Once Flock communicates the request and coordinates with the affected customer, should the affected customer and Flock disagree about the legality of a properly served compulsory legal demand, the affected customer—without the assistance of Flock—may pursue any legal remedy to challenge the legal demand. Flock will comply with any judicial stay or order in proceedings initiated by the affected customer. Flock will comply with any final judicial decision.

In the absence of a timely request for judicial intervention by the affected customer, Flock will comply with the compulsory legal demand as specified in the legal demand and/or in compliance with state and federal law, if the terms of compliance are not specified.

Legal Requests

Upon receipt of a non-compulsory legal demand or an administrative subpoena—unless prohibited by law—Flock will inform the affected customer. Flock will convey to the requesting agency that data is owned exclusively by the affected customer and will request that the legal process be redirected to the affected customer. In consultation with counsel for the affected customer, Flock will decide whether to comply with the request or if there is a good faith reason for non-compliance.

Non-Compulsory Process - Customer Does Not Object

Once Flock communicates the request and coordinates with the affected customer, should the affected customer determine that it does not have an objection to compliance with the agency's request, Flock will notify the requesting agency so that the requesting agency may seek the requested data directly from the affected customer. The affected customer can provide the requesting agency with the responsive documents.

Non-Compulsory Process - Customer and Flock Object

Once Flock communicates the request and coordinates with the affected customer, should Flock and the affected customer jointly decide not to comply with the request without judicial enforcement, Flock will notify the requesting agency in writing of that determination. If the agency responds with a compulsory legal demand, Flock will follow the policy for compulsory legal demands as outlined above.

Emergencies and Exigent Requests

Flock reserves the right to respond immediately to urgent law enforcement requests for information as outlined in our Evidence Policy. Flock notifies a customer after disclosing data in response to an emergency request except in certain circumstances, such as when Flock is prohibited from doing so by law.

EVERY SEARCH. MULTIPLE SAFEGUARDS.

Flock

Built-in controls *at every stage.*

Every search in Flock goes through multiple layers of controls before, during, and after it happens.

BEFORE
Set clear boundaries

DURING
Run the search

AFTER
Ensure accountability

1. Only authorized users
Access is based on role, permissions, and policy.

2. Search limited by policy
State laws and Offense Type Search Filtering *(coming soon)* limit what can be searched.

3. Policy-based safeguards
Log investigative purposes and block restricted use cases automatically based on policy.

4. Search executes
The search runs within approved parameters.

5. Every search is logged
Who searched, what was searched, when, and why—recorded for review.

6. Audit Assistance
Built-in tools make audits faster and more complete.

7. Atypical use detected
Documented workflow allows quick review of atypical activity early.

8. Supervisor oversight
Agencies review, investigate, and take action when needed.

Local control

Agencies decide who gets access, how searches are used, and how data is retained and shared.

Bounded by policy

Searches run only within approved laws, policies, and justifications.

Detect and review

Every search is recorded, reviewed, and accountable. Atypical activity is surfaced for a closer look.

THE RESULT

Justified. Logged. Reviewable.

Transparency you can see.
Accountability you can prove.

Learn more about our commitment to trust and accountability at **flocksafety.com/trust**