



About Flock Safety

Flock Safety is an American company founded and headquartered in Atlanta, Georgia with the mission to eliminate crime and build safer, thriving communities. Flock partners with over 5,000 agencies across the country to provide first responders with advanced technology to help them prevent and solve crimes, achieve justice for victims of crime, locate missing people, and keep our neighborhoods safe. Flock is proud of its role in maintaining safe, prosperous and welcoming places to live, work and visit.

Frequently Asked Questions

What is a Flock License Plate Reader?

A Flock license plate reader (LPR) is a fixed camera that takes a photo of the back of a passing vehicle on a public right-of-way, capturing the license plate and rear of the vehicle.

What the Flock LPR camera is used for: The cameras are used by law enforcement agencies to identify specific vehicles tied to crime or missing people.

What the camera captures: The LPR camera captures the license plate, as well as other characteristics obvious to the naked eye, such as vehicle make, model, color and identifiers like a bike rack.

What the camera does not capture: The cameras do not capture any personally identifying information, such as who is in the vehicle, facial recognition, or any DMV information connected to the license plate.

Has Flock been hacked? How does Flock keep customer data and related servers and systems safe?

Flock's systems, servers and customer data have never been breached or hacked.

Flock not only has a team of cybersecurity experts that work to keep the system safe every day, they also employ independent auditors and stress testers to ensure the system is secure and to identify and fix any vulnerabilities.

Flock Safety is designed to provide a comprehensive and secure platform for public safety technology. Our end-to-end data architecture ensures the seamless collection, processing, storage, and analysis of data, including at rest and in-transit, prioritizing security and privacy at every stage.

Flock Safety cameras have no public IP, and therefore, are not addressable remotely to access footage. All data collection points are equipped with secure communication protocols to protect data in transit from interception and tampering. All data is encrypted using industry-standard algorithms (AWS Key Management Service or KMS) before being transmitted to our servers. CJIS data is stored in the AWS GovCloud.

In addition to being certified by the FBI's Criminal Justice Information Services (CJIS), we are NDAA, SOC2 (Type II), SOC3, ISO 27001, Higher Education Community Vendor Assessment Tool (HECVAT), and FERPA-compliant. We are also aligned with the security protocols established by NIST Cybersecurity as well as the Cloud Security Alliance's CAIQ framework.

Additional security precautions include:

- Role-Based Access Controls (RBAC): Ensures users access only the data necessary for their roles.
- Data Encryption: All data is encrypted both in transit and at rest using industry-leading methods.
- Default Multi-Factor Authentication (MFA): Adds an extra layer of user verification for system access.
- Redundancy and Disaster Recovery: Utilizes AWS's geographically dispersed data centers to ensure data availability and durability.
- Data Retention and Deletion: Data is automatically deleted after (thirty) 30 days following strict protocols.

You can read more about Flock's cybersecurity efforts [HERE](#)

(<https://www.flocksafety.com/blog/flock-safety-cybersecurity-how-we-protect-customer-community-data>)

Who owns the data (photos and connected metadata) captured by the cameras? Also, can you share it, and who controls that? What about transparency in the use of the system?

Your community owns your data and is in control of which agencies can access your data and under what conditions you will share your data. Flock makes sharing controls highly customizable so that your sharing settings can align with your community's values and applicable laws and regulations. Flock Safety will never share your data without your permission, unless legally required. Flock will never sell your data.

Only the authorized users your agency designates will have access to your system, and even then every search they make must have a reason in order to do a search. Every search made by one of your authorized users is logged and able to be audited so you can see when and how your system is being used. Flock recommends every community perform regular audits to ensure compliance with your community's laws and regulations.

In summary

- Your agency owns your data
- Your agency controls if/with whom you share your data with
- All activity in the system is logged for transparency purposes

What happens to the data (photos) after it's captured?

Flock customers own their data. After the data (photos) are taken, it is securely stored on the AWS GovCloud server for the retention period defined in each customer agreement. Generally, this is a 30 day retention period, unless otherwise defined by the agency or state law. After the retention period, the data is hard deleted and unrecoverable. Agencies may choose to download a specific photo connected to an investigation, which is then stored on a local agency server.

Are Flock products accurate?

Flock is committed to the highest standards of accuracy and has implemented robust safeguards to minimize and mitigate errors. Our ALPR system has an accuracy rate in the high 90th percentile (nearly 99%) and is continuously improving through machine learning.

To prevent action based on a potential misread, our system includes several layers of protection. First, Flock Safety confirms both the Optical Character Recognition (OCR)/plate and the state of the plate are both a match before sending a Hot List notification -- this is an extra step that legacy LPR systems do not perform.

Second, the system flags low-confidence reads to the user.

Finally, we recommend that all partner agencies adopt a policy requiring an officer to visually confirm that the scanned plate matches the alert and confirm that the stop meets all applicable law and policies before taking action. This human-in-the-loop verification is a critical safeguard.

Does Flock's technology unfairly target minority communities?

LPR technology reduces the potential for bias by only alerting law enforcement to vehicles *known* to be associated with a crime rather than vehicles an officer *thinks* might be associated with a crime. This reduces unnecessary and potentially negative interactions between vulnerable communities and law enforcement.

The historic Oakland chapter of the NAACP powerfully states how Flock's LPR technology both reduces bias and increases safety for Black and Brown communities:

"In a moment when our communities are demanding both public safety and equitable justice, Flock Safety's LPR technology offers a powerful tool to reduce bias in policing. These cameras are designed to detect only vehicles associated with a crime, removing the subjective judgment that too often leads to disproportionate stops and harmful interactions with Black and Brown residents. It is a clear example of how technology can support safer, fairer policing." [Full Letter](#).

Does Flock technology collect personal information or use facial recognition?

No. Flock's products do not collect any sensitive information, such as information that can be used to distinguish or trace a person's identity. In addition, Flock does not use facial recognition technology.

Does Flock violate the 4th amendment? Are Flock's products unconstitutional?

Flock's license plate reader technology, as well as other products, do not violate the 4th amendment.

The use of Automated License Plate Reader (ALPR) technology by law enforcement has been consistently upheld by courts as constitutional. Fourth Amendment case law overwhelmingly shows that LPRs do not constitute a warrantless search because they take point-in-time photos of cars in public and cannot continuously track the movements of any individual. Appellate and federal district courts in at least fourteen states have upheld using evidence from license plate readers as constitutional without requiring a

warrant. Courts consistently find that there is no reasonable expectation of privacy in a license plate, which is issued by the government for the express purpose of being publicly visible.

LPR technology is fundamentally different from the types of continuous, pervasive tracking of individuals that courts have scrutinized in cases like *Carpenter v. United States*.

In the cited Norfolk case, a federal court decision issued in *Schmidt v. City of Norfolk* represented a clear and definitive legal win for license plate recognition (LPR) technology as it is responsibly deployed today.

In the case, plaintiffs challenged the City of Norfolk's use of LPRs under the Fourth Amendment. The Court granted Norfolk's motion for summary judgment against Plaintiffs and upheld the constitutionality of the City's LPR program, reinforcing well-established legal precedent and rejecting the argument that the technology constituted an unconstitutional search.

You can read more [HERE](#)

(<https://www.flocksafety.com/blog/federal-court-confirms-license-plate-readers-are-constitutional>)

Does Flock use multifactor authentication for users?

MFA Is Always the Default: In November 2024, Flock made Multi-Factor Authentication the **default for all users**. Customers authenticate using a username, password, and use a Time-based One-Time Password (TOTP) for multi-factor authentication. MFA is supported through common providers including Okta and Google Authenticator. For Single Sign-on (SSO), Flock supports multiple authentication methods including SAML, OIDC, and Azure-specific SSO.

In a very successful effort, following the decision to make MFA a default, Flock proactively conducted outreach to thousands of law enforcement customers to convey the importance of MFA and help them enable it. A significant number of Flock's law enforcement customers now use either MFA or Single Sign-on. For a very small group, the account administrator has chosen not to use MFA for their agency. This is always due to a local customer decision — for example, if the agency does not leverage personal phones for work purposes. We regularly contact this group of customers to remind them that MFA is the preferred best practice for organizations.

Is Flock mass surveillance?

No. Flock ALPRs do not and cannot track vehicles, much less individual people. ALPRs take a point-in-time image of the rear of vehicles on public roadways. They are incapable of tracking the whole of anyone's movements, a determination that has been consistently made by Courts across the country. Courts have also uniformly held that there is no reasonable expectation of privacy on public roadways. The vast majority of images captured by Flock ALPRs are not used for any investigation, and are permanently deleted at regular intervals, without ever having been accessed or seen by anyone