

Data Ownership and Sharing

Your community owns 100% of your data and is in complete control of who can access your system and under what conditions you will share your data with other cities so that it aligns with your values. When your Flock system is activated, there is no sharing enabled by default.

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 permanently 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.

Flock does not have a general right of access to Agency data. Flock's contractual obligations outline specific conditions under which Flock may access, use, preserve, or disclose data. It does not grant discretionary access to Flock.

Flock's commitment to data security

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.

Drop down menus

Offense type drop down menus are now mandatory for Flock searches.

Multifactor Authentication

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.

Flock relationship with federal government and previous pilot

Between May and August of 2025, Flock had limited, non-contractual pilots with CBP and HSI. These limited pilots were to assist those agencies, who conduct high-level investigations of significant importance: combatting human trafficking and fentanyl distribution. Flock no longer engages in non-contractual pilots with federal agencies, and Flock does not have a contractual relationship with any U.S. Department of Homeland Security agencies.

Flock does not work with U.S. Immigration and Customs Enforcement (ICE) or any other sub-agency of the Department of Homeland Security. Flock does not partner with ICE. ICE does not have direct access to Flock cameras, systems, or data.

Senator Wyden Letter

Flock Safety values the concerns raised by Senator Wyden's office and recognizes how our security controls are essential to the trust of platform and customers. Flock is relentlessly focused on data integrity and security, and these questions are important to us. We're proud of our robust security program, administered by a team of experts with collective decades of experience in the industry. Our [security-by-default approach](#) includes rigorous controls, validated through independent third-party attestations including SOC 2 principles and ISO certifications.

Flock disagrees with the assertions made by Senator Wyden's office that the Flock platform is not sufficiently secure, and we are confident in our robust security program. We have requested a meeting with the Senator in good faith to explain the above.

Youtube Videos claiming to have hacked Flock

Flock's servers, customer data and other systems have never been hacked, period. We are aware that a person on a youtube video got ahold of one of our cameras and took it apart. He, however, never gained access to any Flock server, data, or other information. His access was equivalent to factory settings on the device.

Flock has never violated or been credibly accused of violating federal law

More information can be found at the following websites:

<https://www.flocksafety.com/privacy-ethics>

<https://www.flocksafety.com/blog/does-flock-share-data-with-ice>