



September 8, 2026

Transmitted via email

Chairman Josh Hawley
Subcommittee on Crime and Counterterrorism
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Hawley:

Thank you for your August 26, 2026 letter. We appreciate the opportunity to discuss the privacy, accountability, security, and transparency safeguards that we have built into our platform, and the ongoing dialogue we have had with your office.

Flock is a safety technology platform that helps communities take a proactive approach to public safety and crime prevention, while respecting and protecting core civil liberties. We are proud that our hardware and software suite supports cities, law enforcement, businesses, schools, and neighborhoods with tools for public safety and investigations. We see the positive public safety impact these technologies deliver to communities every single day, [including in the State of Missouri](#). Flock is trusted by thousands of communities, law enforcement agencies, and businesses across the United States to provide timely investigative information, with industry-leading features and safeguards designed to protect privacy and data integrity and to promote responsible use.

Flock was founded in 2017 on the proposition that law enforcement should be equipped with effective public-safety tools while civil rights and liberties are protected, not traded away. Our Ethical Creed¹ rests on the belief that transparency and accountability are crucial to establish and maintain trust between communities, government, and law enforcement. Technology can help accomplish this by capturing objective, accurate information, while helping to safeguard against misuse and infringement on constitutionally-protected rights. These are not new concepts at Flock; they have been a part of our philosophy, built into our technology, since the beginning. As we continuously work to improve the functionality and efficacy of our technologies, so too do we continuously work to improve their transparency and accountability features and their privacy safeguards.

We appreciate your leadership on these important issues. We agree that the rules that protect Americans should be set by law and not solely by the policies of any single company. Flock does not believe that Americans' privacy should depend on one vendor's good judgment, its current leadership, or its commercial incentives. That is why Flock has consistently supported clear, sensible legislation governing how this technology is used. Durable legislation and legal standards are the foundation of the public trust on which our business depends. We would welcome the enactment of a coherent federal framework, and we stand ready to work with your office and with Congress on its efforts to help protect privacy without depriving communities of tools that solve crimes and save lives.

¹ Flock Safety Ethical Creed, available at <https://www.flocksafety.com/legal/flock-safety-ethical-creed>.



We recognize the importance of, and are committed to building upon, the significant, proactive steps we have taken over the last year to strengthen our ability to prevent and detect misuse of our technology. For example, in April, we announced the launch of Trust & Compliance, a suite of products and services bringing together best-in-class data privacy controls, transparency tools, and accountability features in one system. Trust & Compliance reflects Flock's broader vision: that responsible public safety technology isn't just about solving crime; it's about building systems of oversight that allow communities to trust the tools their agencies use.

Central to this launch was a new industry-leading tool, Audit Assistance, which greatly enhances the efficacy of pre-existing audit logs by continuously monitoring system activity, and surfacing search patterns recorded in an agency's audit log, that fall outside typical usage. Audit Assistance helps agency administrators proactively see when activity warrants a closer look, allowing them to review, document, and respond to potential concerns. More than one-third of our customers voluntarily adopted Audit Assistance since its launch. And we went further, announcing last month that we will require all law enforcement customers to adopt this feature by the end of the year. The tool works: since roll-out it has surfaced multiple instances of misuse, including instances that have led to professional sanctions and even to arrests. In addition, we are instituting a "proactive lockout": when a user's activity meets defined criteria for abnormal behavior, Flock will automatically suspend access pending administrator review. The goal is to intervene before misuse becomes recurring or widespread.

These changes reflect years of work and continuous deliberation. They are not the end of that work, but simply the most recent examples of our commitment to safety, privacy, transparency, and accountability. We are not perfect. We will keep listening, improving, and building a better standard for public safety technology. Our team, including appropriate technical personnel, would welcome the opportunity to brief your staff on any of these safeguards, and to work with you on legislation that serves public safety while protecting the privacy of law-abiding Americans. We believe we share that underlying goal, and we appreciate your engagement.

* * *

Enclosed herein, Flock is producing records responsive to your requests, available at FLOCK-SEN-JH-00000001 through FLOCK-SEN-JH-00000366. Public release of certain non-public information may enable bad actors to circumvent Flock's safety guardrails or efforts to combat abuse. As a result, we request that you and your staff treat the documents and information provided by Flock as confidential. In the event that you or your staff plans to publicly release any previously non-public documents or materials provided by Flock, or if you plan to include such information in any public report or forum, Flock requests reasonable notice and a reasonable opportunity to address the potential release, including an opportunity to propose redactions regarding personally identifiable information to protect the privacy and safety of its employees, and business confidential materials.

Sincerely,

A handwritten signature in black ink, appearing to read "Dan Haley", with a large, stylized flourish extending from the end.

Dan Haley

Chief Legal Officer, Flock



1. State the parameters under which your customers can conduct a statewide or nationwide search of vehicle or driver data, as well as whether those features are enabled by default.²

Each Flock customer controls its own sharing. The customer agency exclusively owns the footage its cameras generate and decides whether (or not) to share it. In other words, Flock does not enable data sharing by default, and a new Flock customer initially is not sharing with any other customer.

A customer's cameras are included in the statewide or nationwide search networks only if the agency affirmatively opts into one of those networks. Statewide and nationwide networks are limited to law-enforcement organizations and are reciprocal: an agency that opts in can search, and be searched by, other agencies that have opted-in. Permitted searches must be exact full-plate matches only—not partial plates, vehicle descriptions, or location sweeps. Separate from network participation, agencies can also establish one-to-one sharing relationships, although our policies prohibit law enforcement agencies from sharing with private agencies. Any sharing relationship can be revoked by the customer at any time.

We also recently introduced Offense Type filtering for sharing. Now, cities can choose which types of offenses are permissible for other agencies to access their cameras. For example, City A could allow City B to search its cameras only for a stolen vehicle, missing person, or violent crime. This gives communities more control over data sharing while preserving collaboration where policies, norms, and practices align.

Moreover, in states that legally restrict data sharing, we have hardcoded those restrictions to facilitate compliance: the platform blocks prohibited out-of-state and federal sharing. Over time, Flock has dedicated significant engineering effort to implement additional structural, technical, and compliance safeguards to help ensure that federal access remains limited, transparent, and controlled locally. Flock has continuously strengthened its safeguards because local control is a core design principle. In particular, in August 2025, Flock established a separate organization type for federal agencies with different tools and stricter limitations than local agencies. All federal organizations were removed from statewide and nationwide networks, and federal agencies can no longer access these search tools.

2. State the default retention period for each category of data Flock collects, and identify every change to that default since January 1, 2021, including the date of each change and the reason for it. State the maximum period a customer may select, whether Flock approval is required to exceed the default, and how many customers currently retain data beyond the default.

Flock's clients are and always have been in charge of their data retention periods. When Flock was started nine years ago, the default recommended retention period was set at 30 days, unless state or local policy required a shorter or longer period. We believed this struck an appropriate balance between safety and privacy, absent controlling local authority or applicable law. We recently announced that we have updated our recommended default to a 7-day retention period for new law enforcement customers. This is in line with our analysis that shows that over 90% of searches without a full plate are done within a week, and we believe this shift represents an appropriate acknowledgement of widespread questions and concerns about data availability and retention, while preserving system efficacy and local control. We also introduced "Evidence Mode": a feature that addresses the exceptional cases where detectives can preserve specific data as evidence for an active investigation in cold storage, consistent with existing laws and policies.

² Flock's responses to the questions in the August 26 letter focus on license plate reader products and United States-based customers.



Existing law enforcement customers may keep their current retention period or transition to 7 days at their discretion. While any customer may request a longer period, that period must be approved through a public, democratically accountable process—either by an elected governing body, such as a city council, county commission, or by an elected official. The purpose is to ensure that a decision to retain data beyond the recommended default is not made informally by an individual department or administrator, but with accountability to the community. We note, however, that presently only approximately 3% of law enforcement customers have a retention period greater than 30 days. The maximum extended retention a customer may establish in our system is one year unless otherwise required by applicable law.³

3. State the total number of confirmed instances of misuse of Flock systems or data known to Flock, by year, since January 1, 2021. For each, state whether the misuse was first identified by Flock’s own monitoring, by the customer, or by a third party.

Abuse of Flock technology, at any level, is unacceptable. The audit log functionality was built into our system from the beginning, so that every search creates a record. As discussed above, implementation this year of our Audit Assistance tool—use of which will be mandatory by the end of the year for all law enforcement clients—has exponentially increased the efficacy of that audit functionality.

Our Terms and Conditions clearly state that customers may only use our technology for a “Permitted Purpose,” defined as “a legitimate public safety and/or business purpose, including the awareness, prevention, and prosecution of crime; investigations; and prevention of commercial harm, to the extent permitted by law.”⁴ Our terms also prohibit customers from using Flock Property “in violation of Applicable Law or to mislead, harass, stalk, or otherwise impose upon or violate the rights of any person.” Accordingly, misusing our technology is a violation of our Terms and Conditions and, in many cases, of the law; it is exactly the conduct our safeguards are designed to prevent, surface, and support our customers in addressing.

We combine technical limits, supervision tools, and clear rules to prevent and enable detection of misuse. We have built our license plate reader platform so that existing state law is enforced in technical code rather than merely promised in a policy. When a state sets a rule, Flock does not ask its customers to honor it voluntarily; we build compliance into our products. Statutorily-mandated restrictions in a given state are written directly into the platform, cannot be toggled off in any dashboard, and cannot be altered or waived by a customer’s own administrators or even by Flock’s support personnel. Flock also offers search filters to all law enforcement customers, which provide built-in guardrails within Flock’s search experience that prevent searches tied to LPR use cases prohibited by law or by agency policy. They serve as an added line of defense to help ensure the LPR platform will not be used in ways that conflict with state or local regulations or values.

Beyond the protections afforded by law, Flock has outlined clear permitted uses for its products, found in our policies and our contracts with each customer. For example, law enforcement agencies must designate “administrators” who control the use of the Flock cameras, and only approved users in a local agency can access license plate reader data based on job role. In addition, searches are recorded, and logs and review tools help agencies check usage. Every organization search log reflects the user, agency, reason, date and time,

³ For example, New Jersey law enforcement guidelines require that license plate reader data is retained for three years. See Attorney General Law Enforcement Directive No. 2022-12, available at [https://www.nj.gov/oag/dcj/agguide/directives/ag-Directive-2022-12_Updated-Directive-Regulating-Use-of-Automated-License-Plate-Recognition-\(ALPR\)-Technology.pdf](https://www.nj.gov/oag/dcj/agguide/directives/ag-Directive-2022-12_Updated-Directive-Regulating-Use-of-Automated-License-Plate-Recognition-(ALPR)-Technology.pdf).

⁴ Terms and Conditions, available at <https://www.flocksafety.com/legal/terms-and-conditions>.



networks searched, case number, and search parameters. Searches must also relate to a specific investigation with a stated search reason, which is selected from a drop down list. The list includes the National Incident-Based Reporting System (“NIBRS”)-based offense types, along with other common uses of Flock, such as missing and endangered persons. In July 2025, we introduced an optional case code requirement for searches (meaning the requirement could be toggled on or off by the customer). Results from participating agencies have been promising, so we will now require case codes for all law enforcement searches by the end of the year (the function will no longer be optional). Following this change, agencies will be able to bypass the requirement only in emergencies, with every exigent search flagged for administrator review. Flock supports those reviews through platform controls and expertise, many of which are surfaced for agency review through the Audit Assistance Tool, as discussed above. Additional information regarding Flock’s search policies is included in response to question 4.

The underlying search records are owned and controlled by each customer agency. Flock does not maintain a single consolidated count of confirmed customer misuse. Nor is Flock ordinarily privy to the case-specific facts necessary to determine whether a pattern of searches served a legitimate investigative purpose, the identity of the person associated with a searched plate, or whether the activity violated the agency’s policies. Those determinations are therefore properly made by the customer agency, which has the investigative context, supervisory authority, and responsibility to govern, monitor, and—where appropriate—sanction its users’ activity.

4. Describe what a user must enter to justify a search. State whether that entry is validated against any external record, whether a supervisor must approve it, and whether a search proceeds if the field is left blank or filled with generic text such as “investigation.”

Flock has always required users to document the reason for each search, but until last year that documentation was entered in a free-text field which, in some cases, resulted in non-specific documentation. In December 2025, Flock deployed a required Offense Type field for law-enforcement searches. Now, each user must select a standardized category that identifies the purpose of the search; the selection is recorded in the audit log.

As discussed above, the Offense Type menu correlates to NIBRS offense categories, the FBI’s crime data reporting standardization schema. We have adjusted and supplemented these offense categories to reflect common, legitimate license plate reader uses that do not fit neatly within a criminal-offense code. It includes criminal-investigation categories and other recognized law-enforcement purposes, such as missing or endangered-person matters and warrant or court-order enforcement. Agencies may remove categories from the menu; if no listed category fits, the user selects “Other” and must provide a free-text explanation or agency-standardized options. In addition, an administrator may require a case number on every search. As discussed above, by the end of this year, a case number/code will be required by Flock for every law enforcement search, with the limited exception of searches pursuant to exigent circumstances, which will be flagged for a local administrator to review.

As discussed in response to question 3, agencies retain responsibility for configuring the offense-type selections and auditing their users’ searches. All searches are memorialized in an agency’s Organization Audit. Organization Audits can be exported at any time. The following pieces of information are recorded on every search run by an agency and included in Organization Audits for administrator review:



- User name
- Networks included in the search
- Time Frame of the search
- License Plate (if included in the search)
- Reason for the search being conducted (which includes Offense Type)
- Case # (if included in the search)
- Filters (if included in the search e.g. make, model, color)
- Text Prompt (if included in the search - FreeForm feature)
- Moderation (if triggered by the search - FreeForm feature)
- Search Time when this search was conducted by the user
- Search Type (which kind of search method was used).

5. Describe every restriction Flock imposes on the purposes for which its systems may be searched. State whether Flock has assessed whether those restrictions can be circumvented and, if so, the result of that assessment.

Please see the response to question 3.

6. State Flock's measured accuracy at the level of a complete and correctly attributed vehicle identification. Identify the testing that produced that figure and state the rate at which alerts are later determined to be incorrect.

Flock offers "Hot List" alerts, which notify law enforcement when a known suspect's vehicle is in the area. These real-time notifications work by connecting Flock cameras with data derived from the National Crime Information Center, state databases, and local law enforcement agencies. When a vehicle with a warrant or a stolen vehicle passes a camera, officers receive a notification enabling them to respond accordingly, and prevent the suspect from committing any further crimes.

We understand that an inaccurate read or an unverified alert can have serious consequences for an individual, as the examples in your letter illustrate. Accuracy is engineered, measured, and continuously improved, as Flock's LPR technology performs multiple checks before a hot-list alert is generated. The camera first captures an image and uses machine-learning models to interpret the license plate. Each read is assigned a confidence score, and low-confidence reads are filtered out rather than treated as certain identifications or sent to officers as alerts. The system then compares both the interpreted plate and the issuing state against the applicable hot-list record. Only after those steps does the system generate an alert. A hot-list alert is a lead—not a conclusion. A properly-trained officer will independently verify the vehicle and circumstances before taking action.

Flock separately evaluates plate-read accuracy and hot-list alert performance. Plate-read accuracy asks whether the camera correctly identified the characters appearing on the plate. Our latest findings from July 2026 found the following capture and OCR rates:

Test	Results
Clear Weather LPR Capture Rate* ⁵	>99% LPR capture rate on a two-lane roadway with optimal camera placement and installation.
Rain LPR Capture Rate*	>99% LPR capture rate on a two-lane roadway with optimal camera placement and installation.
Dawn/Dusk LPR Capture Rate*	>98% LPR capture rate on a two-lane roadway with optimal camera placement and installation.
Optical Character Recognition (OCR) Accuracy	>96% LPR OCR accuracy on a two-lane roadway with optimal camera placement and installation.
License Plate State Accuracy	>97% LPR plate state read accuracy on a two-lane roadway with optimal camera placement and installation.

These high capture and OCR rates, combined with our verification process of filtering out low-confidence reads, has led to Flock’s LPR hotlist alerting system generating approximately nine reported inaccuracies for every one million alerts.

A hot-list “hit” can fail to result in an enforcement action for a number of reasons that do not mean the LPR inaccurately read the plate. For example, the underlying hot-list record may have changed, the vehicle may have lawfully changed status, the officer may be unable to locate the vehicle, the vehicle may no longer correspond to the circumstances reflected in the database, or the officer may determine through independent verification or assessment that the alert should not be acted upon. No system can protect entirely against human error. However, our high and continuously-improving rate of accuracy, combined with the safeguards described above, help to make those human errors rare and will continue to decrease error prevalence over time.

7. Identify every category of data that Flock’s deployed devices capture, including still images, video, audio, wireless signals, and any biometric identifier. For each, state the date on which Flock began capturing it and whether customers may decline.

Flock’s stationary LPR camera captures still images of vehicles and their surroundings. License-plate characters and associated vehicle attributes are derived from those images. The system also records a timestamp, camera/location, and device-health metadata. Flock’s LPR cameras do not capture audio, wireless-device signals, or biometric templates.

⁵ Items marked with an asterisk reflect testing on our latest-generation LPR cameras.



8. State whether Flock links data captured by its devices to any external data source, and identify each such source, including commercial data brokers and public records aggregators. State whether Flock has ever ingested, licensed, evaluated, or tested data obtained from a security breach.

Flock's camera products do not enrich device captures with commercial data-broker or public-records databases. License plate reader products collect the data generated by the deployed device and make it available within the customer's authorized Flock environment.

Flock also offers an investigator-led AI tool, Flock OS. Flock OS can aggregate and synthesize information from data sources the customer is already authorized to access and use, including the customer's Flock data and connected third-party sources. Flock's Nova (now known as Flock OS Notebook) platform pulls together agency data (RMS, CAD, jail, OSINT, LPR, and public records). Neither Flock OS nor the legacy-product Flock Nova independently create a new database or grant a customer access to data it otherwise lacks authority to access. Customers with Flock OS or Flock Nova are entitled to provision their users with access to Flock-provisioned data sources, which includes data procured from commercial data brokers and public records aggregators.

When Flock acquired the product that became Nova, the acquired software included a dark-web data source that may have contained information originally obtained through security breaches. After acquisition, Flock made a policy decision not to provide this breach-derived dark-web data source.⁶

9. State whether multi-factor authentication is required of all users and, if it has not always been required, when it became mandatory.

Yes—multi-factor authentication is now mandatory for customers. In the past, multi-factor authentication was available as a recommended, but optional, control at the customer level. We maintained this optionality because some agencies faced technical limitations on their ability to effectively deploy multi-factor authentication. As technology has continued to improve, Flock is now able to—and does—require the use of multi-factor authentication for all of our customers. Flock has required multi-factor authentication for its own employees, and hardware-based authentication for privileged administrators, for a considerably longer period.

10. Describe in detail whether Flock has the capability to biometrically track individuals and explain what physical or technical limitations exist or are imposed on such biometric tracking.

It is not possible to search specifically for humans in images taken by Flock's license plate readers, which are designed and deployed to capture vehicles, and Flock does not operate facial-recognition technology. It is possible to search for the presence of people in images taken by Flock's non-license plate reader cameras, but searches must be related to elements visible in footage, such as shirt color, glasses, etc., not a biometric template. Searches related to race, skin tone, or ethnicity are blocked.

⁶ Flock Safety, *Correcting the Record: Flock Nova Will Not Supply Dark Web Data*, Flock Safety Blog, available at <https://www.flocksafety.com/blog/correcting-the-record-flock-nova-will-not-supply-dark-web-data>.