September 1, 2026

Transmitted via email

Delegate Tristan Leavitt
Delegate Ryan Browning
Delegate Patrick Lucas
West Virginia House of Delegates Building 1,
Room 231E 1900 Kanawha Blvd.
East Charleston, WV 25305-0470

Dear Delegate Leavitt, Delegate Browning, and Delegate Lucas,

Thank you for your letter to Garrett Langley. On behalf of Garrett and Flock, I appreciate the opportunity to respond to your questions and to discuss Flock's work in partnership with West Virginia's communities and law enforcement — work that is all the more urgent given the opioid and overdose crisis your letter references and the proven value of Flock technology in the fight against the scourge of drug trafficking. I also welcome the opportunity to correct the misimpression, reflected in your letter, that Mr. Kane's August 9 testimony was less than candid. We appreciate the chance to set the record straight, to clarify where technical distinctions may have been lost or misinterpreted in a fast-paced, live exchange, and to provide the detailed information you have requested.

Founded in 2017, Flock's mission is to make communities safer and more equitable by providing objective, accurate evidence to solve and deter crime. We see the positive public safety impact these technologies deliver to communities every single day. In August 2026, a man accused of domestic violence homicide in Vero Beach, Florida was located in West Virginia with the assistance of Flock License Plate Readers following a multi-state investigation involving significant law enforcement cooperation. Cases like these represent an all too familiar dynamic — crime doesn't respect jurisdictional boundaries. It's critical that the brave men and women in law enforcement maintain access to the tools they need to collaborate, while ensuring those tools are backed by accountability mechanisms built directly into public safety products and strong guardrails enshrined in law.

Our Ethical Creed is built on the belief that transparency and accountability foster trust between law enforcement and the communities they serve. We hold ourselves to that standard, and we take seriously any suggestion that we have fallen short of it. Just as no technology system is perfect, neither is any individual. Flock always endeavors to give full, complete, and truthful answers to the public and the officials who represent them. When questions touch highly technical subject matter — authentication requirements, encryption architecture, product-by-product configuration, statistical accuracy measures — precision matters, and important details and distinctions can easily be lost in a live hearing. Several of the matters raised in your letter fall into exactly that category.

Multi-factor authentication. Your letter treats three statements — that two-factor authentication has been standard practice "for a long time," that mandatory customer adoption occurred "within the last year," and that our recent blog post announced mandatory MFA "at the beginning of this month" — as if they contradict one

another. They do not. There is a meaningful difference between a security control being *available*, being *standard practice*, and being *mandatory*. Two-factor authentication has been available on the Flock platform, and standard practice among Flock's own personnel, for years, which is what Mr. Kane intended to convey when asked whether the feature existed and was long-standing. At the customer level, two-factor began as a defaulted-on optional feature; optional because some agencies informed us that they lacked the technical capacity to support it. It was then subsequently made mandatory, as technological options expanded, as Mr. Kane described. Our recent announcement reflects the final step in that rollout. Mr. Kane asked during the hearing whether you were referring to the corporate or customer level. This was the conduct of a witness drawing an accurate distinction, not obscuring one.

Security of the Flock system. Mr. Kane testified, accurately, that Flock's database — the system that houses customer data — has never been breached, and that no unauthorized party has ever gained access to it. That remains true. The separately-disclosed and distinct matter he subsequently referenced involved a device-configuration issue that, due to a vendor error, briefly exposed a limited number of camera streams to the public internet. Flock assessed this issue, promptly remediated it, and publicly addressed it. It is important also to note that "exposed to the internet" does not mean that any member of the public could easily access the device (as, indeed, the public is invited to access countless video streams of public places made deliberately available for viewing on the internet by communities across the country, including in West Virginia). The Flock cameras that were inadvertently exposed required specific knowledge of the camera IP address for access. In any event, a transient device-configuration exposure of individual devices is a materially different thing from an intrusion into the system that holds customer data, and Mr. Kane appropriately drew that distinction. We recognize the distinction can be read as fine parsing to those who do not work with these systems daily. It is not offered to evade the question; it is offered because the question is technical and deserves a technically precise answer.

Federal pilots. Your letter juxtaposes Mr. Kane's March 2026 Connecticut testimony with our August 2025 statement regarding limited pilots with CBP and HSI. These are reconcilable on their own terms, and we set out the reconciliation in full in our response to Request 5. In short, a limited, non-contractual pilot with access to the opt-in sharing networks within the Flock platform to assist with human-trafficking and fentanyl interdiction is a different arrangement from a contractual data-sharing relationship to funnel data to federal entities or in response to legal process. Again, this distinction may not have been clear in the context of rapid-fire Q&A in a live hearing, but it is real.

Correcting the record where warranted. Where Flock has identified an instance in which its public communications were imprecise or incomplete, it has said so and corrected the record — as your own letter acknowledges regarding our August 2025 statement. That is the mark of a company that takes accuracy seriously. We do not accept the broader characterization your letter draws from these episodes, but we do accept and embrace the underlying obligation: to communicate with lawmakers and the public precisely and completely. The transparency and accountability features engineered into our technology exist to serve that same obligation, and we continue to strengthen them.

I appreciate this opportunity, and my team would welcome the chance to provide a briefing to the Committee, including appropriate technical personnel, to walk through any of the matters above as you consider legislation in the 2027 session. We have prepared responses to each of your categories of requests below and look forward

to addressing them in detail.

Sincerely,

Dan Haley, Chief Legal Officer

Flock

cc: Kevin Kane, Flock Safety
Delegate Ryan Browning
Delegate Patrick Lucas
Chairman Chris Phillips, West Virginia House Committee on Government Organization
Chairman JB Akers, West Virginia House Committee on the Judiciary
Speaker Roger Hanshaw, West Virginia House of Delegates
President Randy Smith, West Virginia Senate

I. Security Incidents & Unauthorized Access

Flock Safety takes the security of customer data, including video and license plate data, extremely seriously. Because Flock operates technology used by thousands of public safety agencies and handles information associated with active criminal investigations, our security program is designed around continuous prevention, detection, testing, investigation, and remediation rather than the unrealistic assumption that a system will never experience a security event. Our central cloud environment has to-date never been compromised by an external attacker, and Flock is not aware of an incident in which an attacker breached Flock's cloud infrastructure. That is distinct from the broader security environment in which Flock operates, where there are continuous attempted attacks and where vulnerabilities can arise at the customer, credential, device, application, or infrastructure level.

Flock has built a layered security program to address those risks. The program includes a dedicated cybersecurity organization spanning Governance, Risk & Compliance, Product Security, Incident Response, Offensive Security, and DevSecOps; continuous vulnerability scanning and remediation; endpoint detection and response; SIEM-based security monitoring; web application and boundary protections; hardened infrastructure; hardware-based authentication for privileged administrators; annual security awareness training; and an active incident-response relationship with Google Mandiant. Flock also maintains recurring SOC 2 Type II,ISO 27001, 27701, 27017, 27018 and 42001 audits and annual independent penetration testing. Internally, Flock's security posture has matured substantially since 2022, including stronger identity and authentication controls, least-privilege and segregation-of-duties controls, hardened infrastructure, expanded vulnerability scanning, Secure Boot and device authentication, and stronger controls around third-party software and data protection.

Importantly, Flock does not rely solely on compliance audits or point-in-time assessments. Flock maintains an internal offensive security capability and last year engaged Bishop Fox, one of the country's leading dedicated offensive security firms, to conduct independent adversarial testing across Flock's hardware, software, and

cloud infrastructure. The engagement was deliberately designed to test the platform as an integrated system, including business logic and attack paths that may not be identified through conventional vulnerability scanning. Bishop Fox operates independently and is subject to contractual, security, insurance, and personnel requirements appropriate for systems that handle criminal justice information. Flock's stated objective is not to obtain a report saying that no vulnerabilities exist; the purpose of adversarial testing is to identify weaknesses before they can be exploited and then remediate them.

Flock also welcomes independent validation outside of its own security organization. Most recently, the Miami-Dade Sheriff's Office Cyber Crimes Bureau independently assessed Flock's LPR technology using production devices taken directly from the field rather than equipment supplied by Flock. The assessment attempted to replicate publicly described techniques, such as those referenced by delegates in the meeting of the Joint Standing Committee on Government Organization, for obtaining unauthorized access and was unsuccessful. This type of customer-led assessment is an important component of Flock's broader security model because it provides an independent test of whether a theoretical or reported vulnerability can actually be translated into unauthorized access against deployed production equipment. The assessment found all previously public vulnerabilities were, in fact, remediated and found no new vulnerabilities in their assessment.

Flock likewise treats publicly reported vulnerabilities as security issues to be investigated and remediated rather than dismissed simply because exploitation may require unusual circumstances. Flock maintains a Coordinated Vulnerability Disclosure (CVD) program and is a member of CISA's CVE Numbering Authority (CNA) program. This program enables safe collaboration with independent researchers to share vulnerabilities found in Flock systems with Flock. In response to independent research concerning Flock hardware and software, Flock has evaluated the reported issues, registered applicable vulnerabilities with the CVE system, and implemented hardware and software updates. Flock continues to issue updates and backport security fixes as necessary.

Flock's approach to unauthorized access also depends on comprehensive logging and forensic capability. Customer-facing audit logs capture the user, search parameters, time, networks involved, offense type, and other relevant information. Backend identity and infrastructure logs provide additional information concerning authentication, IP addresses, application activity, and infrastructure events. These records are used by our team to identify suspicious activity and support investigations. Flock maintains specific records of failed authentication attempts, brute-force activity, blocked requests, anomalous API use, and other indicators of compromise, and the security team monitors and triages those events as part of its incident response process.

An unauthorized-access event that involves a customer's environment—for example, a compromised credential, former employee retaining access, or improper sharing of credentials— is materially different from a compromise of Flock's own infrastructure. Flock assists customers in identifying and investigating those circumstances and uses the information learned from those events to determine whether product, process, or access control changes are appropriate. Flock has taken platform-wide steps, like mandating two-factor authentication, when customer-side risks demonstrated that additional protections would benefit the broader customer base. Flock has progressively strengthened its authentication architecture, including MFA for employees, hardware-based authentication for privileged administrators, and customer MFA and Single-Sign On (SSO) capabilities. More recently, Flock moved from available and optional to mandatory MFA for law

enforcement users as part of its broader security and accountability improvements. These measures reflect an important principle of Flock's security program: when an event or vulnerability reveals an opportunity to improve the security baseline, Flock applies the lesson broadly rather than treating the matter as an isolated incident.

Flock's security posture should therefore be evaluated as a continuous security program rather than solely by asking whether a particular category of event has ever occurred. Flock continuously monitors for attempted compromise, independently tests its products, engages customers and outside researchers to challenge its assumptions, maintains substantial audit and forensic capabilities, and remediates identified vulnerabilities through software, hardware, authentication, infrastructure, and process changes. The most recent security updates, including mandatory MFA, independent Bishop Fox review, and a formal Coordinated Vulnerability Disclosure program, are further evidence that Flock is continuing to raise its security baseline as the threat landscape evolves. This layered approach, combining preventative controls, continuous monitoring, independent adversarial testing, customer-led testing, incident response, and aggressive remediation, is the appropriate measure of the security of a modern public safety technology platform.

II. Surveillance Scope & Data Sharing

Flock Safety's approach to data sharing is fundamentally based on customer control. Flock does not own customer camera data for purposes of independently deciding who may access it. Rather, customers control whether their networks participate in sharing relationships, and Flock has continued to add technical safeguards that make those choices more transparent and customizable.

This is also the appropriate context for understanding Flock's historical relationship with federal agencies. In the past, Flock engaged in limited, time-bound pilot programs for prospective federal customers. In 2025, Flock enabled an HSI pilot from March 3 through May 1 and a CBP pilot from May 9 through August 24. Flock publicly announced in August 2025 that it would no longer conduct pilot projects with federal agencies.

The distinction between a pilot to use the platform and a data-sharing relationship is important. The pilots were temporary and limited evaluations of Flock's technology, focused on a specific and defined use case (in this instance, fentanyl interdiction). This included access to Flock's opt-in Nationwide and Statewide networks and the ability to request sharing relationships with other law enforcement users. The sharing model was therefore not a national pool of data that Flock or any federal agency can search at will. The Nationwide network is an optional network that participating law-enforcement agencies elect to join. It is designed specifically for license-plate investigations: an authorized user can submit the full plate number of a known vehicle and search participating law-enforcement camera networks. An agency that does not opt into the Nationwide Network is not part of that network, and Flock has disabled the feature altogether in jurisdictions where applicable law or policy requires it, including California. Additionally, due to the lessons we learned from the federal pilots, Flock's current architecture expressly separates federal organizations from these networks: federal agencies are not included in Statewide or Nationwide Networks and may only participate in the Flock platform through

one-to-one sharing relationships that are explicitly established by the relevant local or state agency, subject to applicable law and policy. Flock has also created a separate federal organization designation so that local agencies can easily identify when a sharing request originates from a federal organization.

The Nationwide Network is an LPR capability. There is not an equivalent national network for Flock's video products. Access to video footage is governed through the direct sharing relationships and access controls applicable to video systems. A local agency can share access to its LPR images or video footage with another authorized organization through the platform if both participating agencies agree.

The question regarding natural-language searches of people also requires an important technical distinction. Flock's video products have computer-vision capabilities, including people detection, person-related alerts, and FreeForm. Those capabilities are intended to allow an investigator to describe observable characteristics or events in footage and retrieve potentially relevant video. They are not facial recognition, and the platform does not create a nationwide biometric database of individuals. Accordingly, the answer to whether a Flock video camera can return a result based on a description such as height, hair color, eyewear, or a facial scar should not be framed as though Flock is enabling biometric identification. Flock's video-search functionality can use computer-vision attributes of a person or their clothing that is present in footage to help locate relevant video, but it is not facial recognition technology. The fact that a user may be able to search for an observable characteristic such as the presence of eyeglasses or grey hair is not equivalent to facial recognition or the identification of a person from a biometric template. Natural language searches also have guardrails. Users cannot conduct searches using prohibited attributes such as race, ethnicity, religion, nationality, or behavioral stereotypes, sexual content or innuendo, or offensive words, phrases, or slurs.

III. Accuracy & False Positive Rates

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. The properly-trained officer will independently verify the vehicle and circumstances before taking action.

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.

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*[1]	**>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.

IV. Internal Oversight and Employee Access Controls

Flock's internal access model is designed around least privilege and role-based access rather than broad, division-wide access to customer information. For that reason, the premise of identifying each corporate division that has "access to all customer data" does not accurately characterize how access to the Flock environment is structured. Access to production systems and customer information is granted according to an employee's specific job responsibilities, and privileged access is separately controlled, monitored, and subject to additional safeguards. Flock's information security program expressly incorporates least-privilege controls, separation of duties, privileged-user controls, periodic review of user privileges, and logging of privileged functions.

Only a limited subset of personnel require elevated technical access in order to perform functions such as operating the production environment, responding to security incidents, supporting customers, maintaining the platform, or investigating technical issues. Even within those functions, access is not equivalent to unrestricted ability to conduct customer searches for personal or investigative purposes. Flock's security organization, for example, is divided across Governance, Risk & Compliance, Product Security, Incident Response, Offensive

[1] Items marked with an asterisk reflect testing on our latest-generation LPR cameras.

Security, and DevSecOps, with different responsibilities and corresponding access requirements.

The same principle applies to account administration. Flock requires individual user identities and has implemented controls designed to ensure that access remains attributable to the individual employee. Flock's policies restrict shared accounts, require authentication and access controls for privileged users, and provide for disabling or modifying access when personnel leave the company or change roles.

Flock's oversight model therefore does not depend on a periodic exercise in which the company manually reviews every employee's every interaction with customer data. Instead, it combines preventative access controls with comprehensive technical logging, automated detection and continuous security monitoring, periodic privilege reviews, and targeted investigation when activity presents an indication of misuse or a security concern, as all employee access is logged for review. Flock's security policy specifically contemplates personnel sanctions, termination and transfer procedures, incident handling, and response to information being exposed to unauthorized personnel.

This approach is consistent with Flock's formal information security requirements. The company maintains controls for account management, automated account monitoring for atypical usage, access enforcement, separation of duties, least privilege, review of user privileges, logging of privileged functions, audit-record review and analysis, continuous monitoring, independent assessment, and penetration testing. These controls form part of the framework against which Flock is regularly assessed through SOC 2, ISO, CJIS-related requirements, and independent security testing.

Accordingly, Flock's employee-access auditing is both continuous and risk-based. System activity is logged as part of the ordinary operation of the platform, while Security Operations and other appropriate teams use those records to identify anomalous or potentially unauthorized activity. Flock does not treat every employee access as presumptively suspicious, nor would it be appropriate for Flock to routinely second-guess the legitimate investigative activity of a customer agency simply because an employee has technical access to the system. Where Flock becomes aware of potential misuse, however, it investigates the activity to determine what occurred, whether the activity violated law or policy, whether access should be removed or restricted, and whether the incident identifies a need for a product or process change.

More broadly, Flock's internal oversight model is intended to reduce both the opportunity for and the consequences of inappropriate employee access. Individual identities, role-based permissions, least-privilege principles, privileged-user controls, MFA and hardware-backed authentication for sensitive administrative functions, comprehensive audit logging, continuous security monitoring, and incident-response procedures operate together. The appropriate measure is therefore not simply how many employees technically possess some form of access, but whether access is limited to employees who need it, whether their activity is attributable and auditable, whether anomalous activity can be detected, and whether Flock can promptly investigate and terminate inappropriate access. That is the framework Flock uses to protect customer information and maintain accountability for employee access.

V. Data Governance & Infrastructure

Flock stores customer data in Amazon Web Services East 1, located in Virginia, U.S.A., and has designed its production environment for both redundancy and recovery. Customer data is stored in encrypted AWS S3 containers, encrypted Flock databases, and encrypted online backup snapshots. Flock's contractual security commitments require AES-256 or better encryption for stored customer data and backups.

Flock's business continuity architecture specifically provides for multiple snapshots of operational databases so that data can be recovered in the event of a system failure. Backup restoration is restricted to designated Flock operations personnel and requires multifactor authentication. The backend is also designed to be resilient at the system level: a failure of an individual server can trigger automatic recovery or failover to another server performing the same function. Backup data remains subject to the same security, confidentiality, and retention controls as production data.

Flock's broader security program complements this resilience architecture with continuous infrastructure monitoring, intrusion-detection capabilities, endpoint detection and response, incident-response procedures, and annual independent security testing. Flock's information security framework expressly includes contingency planning, system backups, recovery and reconstitution, independent penetration testing, continuous monitoring, and incident response controls.

Ownership and governance of customer data and derivative information

The questions concerning "metadata, derivative data, analytics, insights, intelligence, and extracted data" are best answered by starting with the distinction between customer data and information that Flock creates or maintains in operating its service.

Under Flock's standard contractual structure, customer-controlled information collected and retained through the Flock services remains subject to the customer's rights and control. The customer determines who may access that information through the platform and can add or remove authorized end users. Flock's Information Security Addendum expressly describes the customer as controlling access to data obtained through the Flock services and restricts Flock from sharing customer data with third parties except as necessary to perform its contractual obligations or as otherwise permitted by the agreement.

At the same time, not every piece of information generated by Flock's systems is itself customer-owned data. Flock necessarily creates operational and security information in running the service, including infrastructure logs, authentication records, security telemetry, system metrics, usage data, and information necessary to maintain, secure, troubleshoot, and improve the platform.

Flock also does not maintain a single blanket retention period for every form of metadata, derivative information, analytics, or extracted information. Retention depends upon what the information is, why Flock maintains it, the customer agreement, applicable law, and whether it is necessary to operate, secure, or support the service. For example, customer audit logs are maintained separately from the underlying customer image

data, and backend security/access logs are retained for forensic and security purposes.

It is therefore imprecise to identify a single number of days as the “research retention period” for all metadata and derivative data. Some information is retained because it is itself part of the customer service; some is retained because it is necessary to maintain security, compliance, and system integrity; and certain information may be retained separately where permitted for product, analytical, or research purposes.

Flock’s information security framework is also structured to minimize third-party access to customer data. Flock performs due diligence on vendors, subcontractors, and subprocessors before granting access to Flock systems or customer data and evaluates their security controls against Flock’s own requirements.

Flock has both a wholly owned subsidiary in Finland as well as a non-U.S. vendor for data annotation purposes—but the existence of such a vendor relationship should not be characterized as a contract to provide that foreign entity with independent review access to Flock customer data. Images provided to the non-US annotation vendor are separated from the customer environment and are not accompanied by the customer data that would identify the originating agency, organization, account, users, or underlying investigation. Annotators receive only the limited visual material necessary to perform the assigned machine-learning labeling task; they do not have access to the customer’s platform, search history, audit logs, account information, case information, or other operational records. The annotation work is performed on decontextualized images rather than on a customer dataset. This annotation work is critical for improving the machine learning model to correct misreads and enables more accurate system processing. Annotation is the mechanism that turns raw device-captured content into usable learning data: people identify the relevant features, the model learns the pattern, and subsequent model versions can perform more accurately and consistently. The models need real-world examples of the conditions in which customers actually rely on the system, across difficult, variable conditions—different angles, lighting, weather, motion, occlusion, vehicle types, and camera environments. Training on representative images is foundational to reducing errors.

SOC 2 Type II

Flock’s security program is independently assessed rather than relying solely on internal representations. Flock undergoes annual SOC 2 Type II and ISO audits, and customer security commitments expressly provide that Flock and its independent external audit firm publish a SOC 2 Type II report annually. Customers may access the report through Flock’s Security Center (https://security.flocksafety.com/); Flock can facilitate access to the SOC Type II for you via this secure platform.