CHRIS PHILLIPS
(304) 340-3192

CHAIR - GOVERNMENT ORGANIZATION
JUDICIARY
HOMELAND SECURITY
RULES

BUILDING 1, ROOM 213E
1900 KANAWHA BLVD., EAST
CHARLESTON, WV 25305-0470
CHRIS.PHILLIPS@WVHOUSE.GOV

HOUSE OF DELEGATES
WEST VIRGINIA LEGISLATURE

September 3, 2026

Dan Haley, Chief Legal Officer
Flock Safety
3284 Northside Parkway NW
Atlanta, GA 30327

Mr. Haley:

Thank you for your September 1 letter. We appreciate the opportunity to correct the misimpression, reflected in your response, that a two-page exercise in corporate reframing constitutes an answer to nineteen specific information and document requests. We also welcome the chance to set the record straight on where clarity was lost—not in a "fast-paced, live exchange," but in the two weeks your legal team had to draft a considered written response.

Multi-Factor Authentication

Your letter asserts that Mr. Kane's two differing statements in his August 9 testimony and Mr. Langley's August 13 blog post do not contradict one another. While we do not dispute that "[t]here is a meaningful difference between a security control being *available*, being *standard practice*, and being *mandatory*," Mr. Kane was asked a very simple question by Delegate Browning: "Do you guys require two-factor authentication to log into the system?" As you may be aware, *require* means *mandatory*. Mr. Kane testified: "Yes." Delegate Browning then asked: "Is that recent?"—a highly reasonable question for Flock's Director of Government Affairs given that U.S. Senator Ron Wyden and U.S. Representative Raja Krishnamoorthi wrote a letter to the Federal Trade Commission last fall requesting an investigation into Flock Safety *precisely* because they asserted Flock did not require its customers to use multi-factor authentication to log into the system.[1] Mr. Kane's response to Delegate Browning—"It's been a standard practice for a long time"—implied to those listening that *requiring* two-factor authentication had been a standard practice for a long time, since Delegate Browning clearly was not asking how long two-factor authentication itself had been a standard practice.

What you describe as "a witness drawing an accurate distinction, not obscuring one" did not occur until Delegate Browning's questioning was over and Delegate Leavitt challenged Mr. Kane on the claim, noting: "There's been a lot of reporting that two-factor authentication is not required by the local departments. You say you guys have used two-factor authentication for a long time." Only then did Mr. Kane attempt to distinguish between Flock personnel and

[1] "Wyden, Krishnamoorthi Urge FTC to Investigate Surveillance Tech Company on Negligently Handling Americans' Personal Data," Nov. 3, 2025, https://www.wyden.senate.gov/news/press-releases/wyden-krishnamoorthi-urge-ftc-to-investigate-surveillance-tech-company-on-negligently-handling-americans-personal-data.

customers. When Delegate Leavitt clarified he was asking about when two-factor authentication became mandatory at the customer level, Mr. Kane testified: "I think that's been done within the last year."

While "the beginning of [August]"[2] may be literally "within the last year" from Mr. Kane's August 9 testimony, so too would have been a change made days after the fall 2025 FTC complaint from Senator Wyden and Representative Krishnamoorthi. Mr. Kane's failure to explain just *how* recently multi-factor authentication had been made mandatory left a highly misleading impression with the Legislature.

Your letter also introduces a new ambiguity on this issue. Mr. Langley's August 13 blog post read: "At the beginning of this month, we also made multi-factor authentication (MFA) mandatory for anyone logging into Flock, increasing our security standards for all customers."[3] Yet somewhat perplexingly, your letter reads: "More recently, Flock moved from available and optional to mandatory MFA for law enforcement users[.]" This raises the question of whether the multi-factor authentication requirement is limited to law enforcement users.

Data-Sharing with Federal Agencies

While we do not possess a transcript of Mr. Kane's March 4, 2026, testimony before the Connecticut General Assembly's General Law Committee, your letter still leaves us with the impression his testimony there was similarly misleading. Your letter sets up a straw man: "The sharing model was . . . not a national pool of data that Flock or any federal agency can search at will." It is clear that Flock's opt-in nationwide network does not operate in that manner.

Yet as reported, Mr. Kane testified that Flock had never had a data-sharing request come in from a federal agency. The fact that these federal agencies had to "request sharing relationships with other law enforcement users" (emphasis in original) does not change the fact that Flock's pilots with Homeland Security Investigations (HSI) and Customs and Border Protection (CBP) "included access to Flock's opt-in Nationwide and Statewide networks"—a massive amount of data. And while indicating those agencies were "prospective customers," your letter does not answer whether the request for that pilot, and the accompanying data, came from these federal agencies or from Flock Safety.

Security of the Flock System

Mr. Kane's testimony about the security of the Flock system was also highly misleading. No one disputes that "a transient device-configuration exposure of individual devices is a materially different thing from an intrusion into the system that holds customer data[.]" However, not only did Mr. Kane not draw that distinction in his opening testimony, he also failed when initially questioned about it to give the "technically precise answer" the Legislature "deserves."

---

[2] Garrett Langley, "Flock Updates Privacy, Accountability, Security, and Transparency Safeguards," Flock Safety Blog, Aug. 13, 2026, https://www.flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency.
[3] *Id.*

Delegate Lucas opened his questioning by saying: "You can't get on any social media without a lot of people saying certain things about it. So let me ask you a few questions. You said during your testimony that Flock Safety has never been hacked." Mr. Kane testified: "Yes, sir, that's correct." Delegate Lucas responded: "And that's good information. I'm glad to hear that, because there's information out there saying differently." *This* is when Mr. Kane should have acknowledged what he didn't acknowledge until two questioners later, when he admitted to Delegate Leavitt "[t]here are some videos on YouTube that purport to have hacked Flock."

We understand that the "device-configuration issue that . . . briefly exposed a limited number of camera streams to the public internet" was "due to a vendor error." However, while we appreciate you sharing the City of Ravenswood's public link to view the beauty of the Robinson River, the "countless video streams of public places made deliberately available for viewing on the internet by communities across the country" are typically just like the Ravenswood one: deliberately stripped of controls or the ability to access archives. This is very different from when Flock devices were "exposed to the internet": settings could be changed, diagnostics could be run, text logs streamed, and 30 days of archived footage could be watched or downloaded by anyone who found it.[4] A more detailed account approximately three weeks after the initial 404 Media story implied that both camera control and use of search or analytics features may have been exposed,[5] contrary to Flock's initial blog post publicly responding to these breaches.[6]

More significantly, that more detailed account raised the issue that beyond the cell phone vendor issue, the Flock hardware accessed was "designed with the assumption that network isolation is sufficiently hardening."[7] The author made twelve different recommendations for Flock, only one of which we were able to find public reports of Flock taking.[8] The same author

---

[4] Jason Koebler, "Flock Exposed Its AI-Powered Cameras to the Internet. We Tracked Ourselves," 404 Media, Dec. 22, 2025, https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves; Benn Jordan and 404 Media, "This Flock Camera Leak is Like Netflix for Stalkers," YouTube, Dec. 22, 2025, https://www.youtube.com/watch?v=vU1-uiUlHTo.

[5] The services exposed without requiring authentication apparently included ONVIF "ptz_service endpoint" [pan-tilt-zoom control] and "analytics_service" endpoints. Jon Gaines, "Finding 67 Flock Safety Live PTZ Camera/LPR Feeds and Debug Web Interfaces accidentally exposed without authentication to the internet," GainSec.com, Jan. 9, 2026, https://gainsec.com/2026/01/09/bird-hunting-season-finding-67-live-camera-feeds-and-debug-web-interfaces-accidentally-exposed-by-flock-safety.

[6] "Update on Limited Condor Device Configuration Issue," Flock Safety Blog, Dec. 23, 2025, https://www.flocksafety.com/blog/update-on-limited-condor-device-configuration-issue.

[7] "[T]he exposed device identifiers, cellular network information, and tunnel configurations provide sufficient data for an attacker to fingerprint, geolocate, and potentially target specific Flock Safety camera units. Leaked FRP tunnel session IDs and server addresses reveal the exact attack surface for accessing internal device services including RTSP video streams and HTTP management interfaces. The combination of missing ADB key initialization, SELinux policy failures, and verbose authentication logging creates multiple vectors for unauthorized access and privilege escalation. If exploited, an attacker could intercept video feeds, manipulate device configurations, or use compromised units as pivot points into Flock Safety's infrastructure. These findings represent systemic logging hygiene issues that expose sensitive operational and personal identifiable information across the entire device fleet." Jon Gaines, "Finding 67 Flock Safety Live PTZ Camera/LPR Feeds and Debug Web Interfaces accidentally exposed without authentication to the internet," GainSec.com, https://gainsec.com/2026/01/09/bird-hunting-season-finding-67-live-camera-feeds-and-debug-web-interfaces-accidentally-exposed-by-flock-safety.

[8] Flock "modified the diagnostic interface to require our technicians to log in with a username and password[.]" Chris Castaldo, "Flock Safety Cybersecurity: How We Protect Customer & Community Data," Flock Safety Blog,

later published a summary report on August 9, 2026—the same day Mr. Kane testified before our Legislature—that concluded:

> What I found across three devices and a shared Android app suite wasn't one clever bug. It was a posture: secure boot off, bootloaders unlocked, debug interfaces wide open, firmware in cleartext, credentials hardcoded, and—the one that still gets me—a wireless path to a shell that needs no root, no soldering, and no firmware mods at all. Just a shared hotspot password and an admin API that forgot to ask who you are.[9]

Data and Document Requests

To summarize: our concerns are not based off a one-time event that got lost in translation because West Virginia legislators "do not work with these systems daily."

Yet much in the same way Mr. Kane gave answers to the questions he may have wanted to be asked rather than those he *was* asked, most of the replies in your letter did not respond to the actual requests in our August 14 letter. Accordingly, we reiterate those requests in bold below:

I. Security Incidents & Unauthorized Access

A general description of your security program is not a substitute for the information we requested about raw video footage from Flock devices being accessed.

1. **For each year since Flock Safety's founding and for each Flock Safety product line, how many incidents is Flock Safety aware of where raw video footage has been accessed by unauthorized users?**

2. **What investigations did Flock Safety conduct of each instance of unauthorized access?**

3. **For each instance of unauthorized access, what was the cause of the security breach?**

4. **What remedial steps has Flock Safety taken after each security breach to prevent recurrence?**

II. Surveillance Scope & Data Sharing

6. **Were the CBP and HSI pilots requested by those agencies, or by Flock Safety?**

8. **What percentage of Flock Safety automated license plate reader users are currently opted into the National Lookup Tool?**

Mar. 27. 2026, https://www.flocksafety.com/blog/flock-safety-cybersecurity-how-we-protect-customer-community-data.

[9] Jon Gaines, "Bird Hunting Season: The Final Flight," Aug. 8, 2026, https://media.defcon.org/DEF%20CON%2034/DEF%20CON%2034%20presentations/DEF%20CON%2034%20presentations/DEF%20CON%2034%20-%20Jon%20Gaines%20-%20Bird%20Hunting%20Season%20The%20Final%20Flight%20-%20PDF%20v1.pdf.

10. **Will Flock Safety's Condor camera return FreeForm natural language search results for such bodily characteristics as height, hair color, wearing glasses, or a scar on one's face?**

This question did not ask about biometric identification. Your answer strongly implies the answer to the foregoing is yes. Please answer yes or no.

III. Accuracy & False Positive Rates

Understanding the numerous variables (clear weather versus rain, dawn/dusk versus mid-day, optimal camera placement and installation), these questions require information based on false positive responses. The request was framed as such because Mr. Kane indicated before the West Virginia Legislature that Flock's accuracy rate for Hot List alerts was "99.99%"—yet testified that number was derived from "investigations based on surveys and things like that with customers[.]" These questions also require data for 2017-2025, by year, not a summary from July 2026.

11. **For each year since Flock Safety's founding, how many false "Hot List" positives have been generated by:**
    a. **Flock Safety's Falcon license plate reader; and**
    b. **Flock Safety's Sparrow license plate reader.**

12. **Based on the aforementioned false positive data, what was the accuracy rate of the Falcon license plate reader for all license plate "Hot List" hits in 2025?**

13. **Based on the aforementioned false positive data, what was the accuracy rate of the Sparrow license plate reader for all license plate "Hot List" hits in 2025?**

IV. Internal Oversight & Employee Access Controls

14. **For each corporate division of Flock Safety, approximately how many employees have access to all customer data?**

The question was not which corporate divisions have access to all customer data, or whether it resulted in "unrestricted ability to conduct customer searches for personal or investigative purposes." It was how many employees, by division, have such access—which your letter apparently refers to as "elevated technical access."

15. **How often does Flock Safety audit its employees' access of customer data? What do the audits consist of? Do such audits comprehensively review every search, or only perform spot checks?**

We did not ask whether Flock "treat[s] every employee access as presumptively suspicious," or whether "it [would] 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." We are simply seeking to ascertain whether Flock applies the same standards to

itself that it recommends for law enforcement agencies. Mr. Kane testified before the West Virginia Legislature:

> We are very confident, not only in our audit logs and our Audit Assist tool, but also **working with departments to develop policies to ensure regular audits are actually occurring**. And so I think a combination of **the policies *as well as* the advancements in the technology** ensure that if anyone were to seek to abuse this, they're gonna get caught. And so we strongly encourage it. **Can't just be relying upon the technology.** There has to be a good policy in place to ensure **regular oversight of all queries** that their department may be conducting on Flock.

Your letter reads:

> Flock's oversight model . . . 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.

It strongly sounds as though Flock is simply "relying upon the technology"—precisely what Mr. Kane testified was not sufficient for law enforcement agencies. Please correct us if we are mistaken, such as if Flock's "periodic privilege reviews" include any manual review of queries the employee has made.

16. **Since Flock Safety's founding, how many employees have ever been found to have improperly accessed customer data?**

V. Data Governance & Infrastructure

19. **How long are metadata, derivative data, analytics, insights, intelligence, and extracted data from customer products retained by Flock Safety for research purposes?**

This question did not ask for "a single number of days as the 'research retention period' for all metadata and derivative data." It was presumed that various data would have different retention schedules. Please provide them.

20. **Please list all contracts Flock Safety has ever had with entities outside of the United States to conduct third-party review of Flock Safety data, metadata, derivative data, analytics, insights, intelligence, or extracted data.**

This requires identifying the non-U.S. vendor referenced in your letter, the contract dates, and any other such contracts, their parties, and their dates.

22. Please provide your most recent SOC 2 Type II compliance audit.

This is important to ensure the "multiple snapshots of operational databases so that data can be recovered in the event of a system failure" are also completely disposed of upon the end of a retention period. But to "provide" the audit does not mean providing a hyperlink for customers to which Flock can "facilitate access."

Please provide complete responses to the outstanding items, with appropriate numbering to the corresponding request, by September 17, 2026, so we are not forced to consider compulsory process in this matter. To arrange for delivery of documents, please contact Committee on Government Organization staff at 304-340-3192 or government.organization@wvhouse.gov.

Finally, we appreciate the offer of a verbal briefing with "appropriate technical personnel." We will schedule such a briefing once you have responded in full to the outstanding items above.

Cordially,

Delegate Tristan Leavitt

Delegate Ryan Browning

Delegate Patrick Lucas

Chairman Chris Phillips

cc: Chairman JB Akers, West Virginia House Committee on the Judiciary
Speaker Roger Hanshaw, West Virginia House of Delegates
President Randy Smith, West Virginia Senate