

United States Senate

WASHINGTON, DC 20510-3203

October 5, 2026

Garrett Langley
Chief Executive Officer
Flock Group Inc.
1170 Howell Mill Rd NW, Suite 210
Atlanta, GA 30318

Dear Mr. Langley:

I write to share my concern regarding the rapid expansion of Flock Safety's automated license plate reader (ALPR) network and the severe risks it poses to the privacy, security, and constitutional rights of Americans.

While law enforcement agencies rely on technology to assist in criminal investigations, the mass collection, retention, and sharing of location data on innocent people fundamentally threatens the Fourth Amendment right to be free from unreasonable searches. Flock has essentially built a private, nationwide surveillance tool.

I am particularly alarmed by the data-sharing capabilities facilitated by your "National Lookup Tool," which allows agencies to search data collected far outside their own jurisdictions. For Americans, this presents a unique and immediate threat.

The ability of federal agencies and federal law enforcement to utilize Flock's network to track individuals exercising their fundamental rights is unacceptable. The pushback we have seen from various municipalities which are pulling flock cameras over data sharing concerns, demonstrates that the public does not consent to this level of unwarranted surveillance.

Furthermore, recent reports indicating that Flock cameras are vulnerable to hacking with malicious actors allegedly extracting stored media and decryption keys directly contradict your company's claims regarding data security and encryption. Coupled with documented instances of law enforcement personnel abusing ALPR systems for personal reasons, such as stalking, the lack of rigorous oversight is glaring. At a minimum, personal data not tied to a crime should be deleted from Flock's servers.

Please provide written responses to the following questions by October 16, 2026:

Data Collection and Retention

1. What is the exact volume of data (including images, videos, and metadata) currently stored on Flock servers that originated from cameras located within New York State?
2. What is your data retention policy, and are there any exceptions that allow data to be held longer than the stated default period?
3. Do Flock cameras capture, categorize, or store images of pedestrians, cyclists, or individuals outside of vehicles? If so, what is the justification for this collection?

Data Sharing

4. What percentage of your law enforcement customers are currently enrolled in the National Lookup Tool?
5. What specific, systemic safeguards are in place to prevent out-of-state agencies from utilizing the National Lookup Tool to track data generated by Flock cameras?

6. What federal agencies accessed data generated by Flock cameras, either directly or through local law enforcement partnerships?

Oversight and Misuse

7. What auditing measures does Flock employ to detect unauthorized or inappropriate searches by users before they are publicly exposed?

Data Security

8. In light of recent reports that hackers accessed decryption keys and stored media on Flock devices, what immediate mitigations have been deployed to secure the physical hardware?

Artificial Intelligence

9. Does Flock use Artificial intelligence to enhance images?
10. Can you detail how you are using artificial intelligence generally?

Law abiding Americans should not have to sacrifice their right to privacy simply by driving down a public street. I look forward to your prompt response to these critical questions.

Sincerely,



Charles E. Schumer
United States Senator