

Benn Jordan - Testimony:

Over the summer of 2025, I started learning about some of the weaknesses in the security and efficacy of the ALPR industry's ecosystem and hardware. I found that Flock, at the time, did not require their clients to use multifactor authentication.

This led me to find Flock law enforcement accounts for sale by a Russian vendor on a Dark Web marketplace, which was referenced in Senator Wyden and Representative Krishnamoorthi's letter urging the FTC to investigate Flock as a national security risk in November of 2025.

I then met and worked with Jon "GainSec" Gaines, who had discovered, detailed, and published 55 security vulnerabilities related to Flock. Some of these vulnerabilities are published through MITRE, who manages security vulnerabilities for the Department Of Homeland Security.

The most alarming of Jon's reported vulnerabilities was in the most common model of Flock's ALPR camera. I publicly demonstrated that by pushing the button on the camera 3 times, I was able to access all of the data or reprogram the device however I wanted in under a minute. A backdoor. Malware. I've even played Doom on a Flock camera.

In addition to this, Jon and myself found insufficiently protected sensitive information stored on Flock cameras including photos, license plate data, logs, API keys, passwords, and communications.

In December of 2025, Through a specialized search engine, I found unprotected administrative interfaces for over 60 newly deployed Flock Condor cameras that had AI-enabled pan-tilt-zoom features. This allowed me to remotely view, delete, and modify 30 days of streaming camera footage from cameras across the country in potentially sensitive areas like forest trails, people's front porches, and playgrounds, as well as zoom in on people's mobile phone screens.

Another security researcher, Joshua Michael, independently found a misconfigured Flock development demo via a Google search that included ArcGIS API keys with virtually unlimited limits on usage. ArcGIS stores enormous amounts of data from local governments ranging from the live GPS location of police vehicles to aerial drone feeds.

To give you an example of why this is so problematic: Last year it was discovered that Flax Typhoon, a Chinese state-backed hacking group, had accessed this system and maintained a hidden backdoor for over a year. Since this attack was likely the result of misconfigurations by a 3rd party, it can't be fixed by a file scan or security patch.

Flock has repeatedly claimed that their service utilizes end-to-end encryption. Both Jon and myself have verified the lack of end-to-end encryption in a variety of different ways, but the most alarming consequence of this is in Dunwoody, GA, where FOIA requests show that Flock employees had viewed cameras on their network over 1000 times, including the ones in sensitive areas like the interior of a Jewish community center and a playground.

Until recently, Flock's response to my videos and media stories about our research had primarily been defensive or in denial of many of the reported vulnerabilities. But in light of recent events, they have invited myself and other researchers to review their hardware and platform. While there hasn't been enough time for a thorough review before this hearing, it does appear that they're taking security a lot more seriously than they were a year ago.

There is something that Flock's executive leadership, myself, and the majority of Americans seem to agree on. We all want clear privacy guard rails that puts safe limits to the government's use of this technology. Even a multibillion dollar startup like Flock now seems to understand that existing in the Wild West has far more consequences than benefits.

I have been one of Flock's harshest critics for years, but everything I just stated about them is a symptom of a much larger problem. What I've been asking for, around the country, is for privatized government surveillance vendors to require independent security testing and inspections. I cannot legally open a restaurant or a barber shop without the health inspector and fire marshall making sure it's safe. Yet there is not a single city or police department in this country that requires this from a 3rd party company tracking their citizens.

I want to use my time here to ask our legislators to take this rare bipartisan agreement to view Flock as a canary in a coal mine and understand that this doesn't go away by removing one company from the equation. Axon and Motorola are actively rolling out the same reckless features that we're shaming Flock for, and you can expect these same vulnerabilities will continue to happen over and over again when innocent people's data is traded between private companies and police without any safeguard or protection.

Some members of this committee are in support of the Combating Organized Retail Crime Act, which has broad definitions that could lower the security posture of sensitive civilian data to the standards used by big box stores. After reading the bill, I immediately imagined a scenario where the Home Depot and Target data breaches affecting hundreds of millions of Americans also included their location data and sensitive information related to ongoing investigations.

To be as concise as possible: From a security perspective, it would be absurd to be concerned with the scenarios playing out with Flock while supporting bills like CORCA or the extension of FISA 702. That would be the equivalent of feeding a monster in an attempt to defeat it.

An effective solution to many of the problems we're hearing about today, would be using this momentum to make clear, effective, and unified federal privacy laws on par with the GDPR and, literally, every other developed country on the planet. ALPRs are used all over the world, but viewing license plates as personal data with modern privacy guard rails would have prevented nearly every single problem we're learning about in this hearing.

This is an opportunity for Congress to build the overdue framework to protect the privacy of Americans for generations to come.