# 30 seconds with a stick' | Researchers claim Flock cameras are easy to hack, have significant security vulnerabilities

https://www.9news.com/article/tech/researchers-claim-flock-cameras-are-easy-to-hack/73-6c805b4a-7b64-4d71-828e-961dda84b8e5

Channel 9 News-Denver, CO

Author: Spencer Soicher
Published: 7:48 PM MST November 19, 2025
Updated: 7:48 PM MST November 19, 2025

A researcher said he was quickly able to take control of a device. A cybersecurity content creator said he found a police login for an account on the dark web.

AURORA, Colo. — The Aurora Police Department has launched a drone program in partnership with Flock Safety. Aurora already uses Flock's automated license plate reading (ALPR) cameras, which cybersecurity researchers are now reporting are extremely easy to hack and are vulnerable to security concerns.

The drones are part of Aurora's new Real Time Information Center, which combines license plate readers, city cameras and the drone program into one location. APD and police departments all over the country tout the cameras as a way to solve and deter crime. But the launch comes as researchers have discovered what they describe as severe security vulnerabilities in Flock's camera systems, including the ability to manipulate footage and a lack of mandatory multi-factor authentication for police users.

Jon Gaines, a cybersecurity researcher, published a white paper recently that prompted Flock to issue public statements on its website. Gaines, who says he purchased Flock cameras on eBay, began testing them for vulnerabilities. Gaines said he was able to take control of the devices in under a half minute.

"It would be about 30 seconds, with a stick," Gaines said.

Gaines demonstrated the security flaws using Flock's compute box, which serves as the brain behind the camera system. He said the devices lack proper security best practices.

"The stuff that is running on the devices themselves is lacking," Gaines said, pointing out that his research is designed to help stop future bad actors.

"The goal is to give a better perspective over all of the industry, and not just use this as an indication of the security posture of the industry. But from my peers and colleagues, there's definitely an indication that this is bad, and I would say it quickly overflowed to the point where it's not an indication of the industry," he said.

He said he was quickly able to gain control of the device and was able to plant images on it. He also found images on the device, he said, of the factory where the camera was manufactured. He described a hypothetical worst-case scenario involving the security flaws.

"I can wirelessly connect to this device and plant footage that will result in, let's say, a hit coming up on the hotlist and the cops showing up to somebody who is not aware that, you know, the cops were called on them," Gaines said.

Benn Jordan, a YouTuber and researcher, featured a few of the 51 vulnerabilities discovered by Gaines in a recent video on his channel. Jordan said he focused on the most severe issues for his video, which now has over half a million views in just a few days.

Jordan identified the lack of mandatory multi-factor authentication as particularly concerning. He said he found Flock police login credentials for sale on dark web marketplaces, though he did not purchase them for legal reasons.

"There is a national security risk," Jordan said. "Like this actually needs to be dealt with because I was finding accounts for sale on the dark web."

Jordan described the absence of required multi-factor authentication as a fundamental security failure.

"Any tech-minded person probably knows that not having multi-factor authentication on a camera that's logging the location of everybody is just unfathomably bad," Jordan said.

He also felt that gaining unauthorized access to the cameras requires minimal technical skill.

"It's extraordinarily easy, like 12-year-olds could do it," Jordan said.

Another researcher, Joshua Michael, offered the same harsh assessment of Flock's security measures.

"I've seen high school projects with better security," Michael said.

Flock responded to the research by stating that 97% of its customers now use either Flock multi-factor authentication or customer single sign-on. The company said it began requiring multi-factor authentication by default for all new users in November 2024. According to Flock, the remaining customers have been urged to enable multi-factor authentication, but have declined for reasons specific to them.

Aurora Police Deputy Chief Phillip Rathbun said the department was aware of vulnerabilities disclosed in May. Both Aurora and Denver say they require multi-factor authentication.

Both Aurora and Denver Police said they require two-factor authentication for Flock logins, despite no company mandate requiring it.

Jordan believes that no matter who is running a system like this, the issues will persist.

"It's up to the communities to be the ones to force some type of regulation to make sure that these things are up to security standards," he said. "Because as I said in my video, if Flock disappeared tomorrow morning, there'd be seven more companies trying to do

the exact same thing, and they're all just trying to make money as quickly as possible. That's what businesses do.

"I feel like sometimes people think of this company as if communities had no way to communicate with each other. Like we were just like in the medieval times before Flock came along or before Axon, any of these companies came along and gave us the ability to communicate with other police departments. We've been doing this since the beginning. It's not that hard."

Submit A Whistleblower Complaint
(https://www.wyden.senate.gov/whistleblower-complaint)

November 03, 2025

# Wyden, Krishnamoorthi Urge FTC to Investigate Surveillance Tech Company on Negligently Handling Americans' Personal Data

## Congressional investigation reveals 35 accounts of Flock customers were stolen

***Washington, D.C.*** — U.S. Senator Ron Wyden, D-Ore. and Representative Raja Krishnamoorthi, D-Ill., today called for a federal investigation into surveillance technology company Flock Safety, for failing to implement cybersecurity protections and needlessly exposing Americans' personal data to theft by hackers, foreign spies, and criminals.

Flock does not require its law enforcement customers to use multi-factor authentication (MFA), a cybersecurity best practice. The methods of MFA that Flock supports can be circumvented by hackers. In addition, Flock does not natively support phishing-resistant MFA, which is recognized by the federal government as the gold-standard of cyberprotection, and is required of federal agencies.

The letter notes that passwords for at least 35 Flock customer accounts have reportedly been stolen by hackers, according to a public website operated by the cybersecurity company Hudson Rock. Phishing-resistant MFA can protect accounts from hackers, even when user passwords have been stolen or phished.

**"Flock has received vast sums of taxpayer money to build a national surveillance network,"** Wyden and Krishnamoorthi wrote in their letter to FTC Chair Andrew Ferguson. **"But Flock's cavalier attitude towards cybersecurity needlessly exposes Americans to the threat of hackers and foreign spies tapping this data. Accordingly, we urge the FTC to hold Flock accountable for its negligent cybersecurity practices."**

Flock's failure to provide real privacy protections poses a serious threat that could result in bad actors gaining unauthorized access to law-enforcement-only parts of Flock's website and harvest billions of Americans' license plates collected by taxpayer-funded cameras nationwide. There have been at least four cases, including against Uber, Cheff, Drizly, and Blackbaud, where the FTC reached settlements with companies for failing to require MFA, which the FTC argued violated federal law.

Flock is the largest surveillance camera operator in the United States, providing services to 5,000 police departments, 1,000 businesses, and numerous homeowners associations across 49 states. The company's surveillance cameras capture personal data which can reveal the movements of Americans, including trips to doctors and therapists, support group meetings for alcohol or drug addiction, and places of worship and protests.

Last week, Wyden slammed Flock for its ineffective protections for Oregonians against abuses by federal agencies and out-of-state law enforcement.

The text of the letter is here.

###

Electronic Frontier Foundation

# How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists

**https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists**

BY DAVE MAASS AND RINDALA ALAJAJI
NOVEMBER 20, 2025

It's no secret that 2025 has given Americans plenty to protest about. But as news cameras showed protesters filling streets of cities across the country, law enforcement officers—including U.S. Border Patrol agents—were quietly watching those same streets through different lenses: Flock Safety automated license plate readers (ALPRs) that tracked every passing car.

Through an analysis of 10 months of nationwide searches on Flock Safety's servers, we discovered that more than 50 federal, state, and local agencies ran hundreds of searches through Flock's national network of surveillance data in connection with protest activity. In some cases, law enforcement specifically targeted known activist groups, demonstrating how mass surveillance technology increasingly threatens our freedom to demonstrate.

Flock Safety provides ALPR technology to thousands of law enforcement agencies. The company installs cameras throughout their jurisdictions, and these cameras photograph every car that passes, documenting the license plate, color, make, model and other distinguishing characteristics. This data is paired with time and location, and uploaded to a massive searchable database. Flock Safety encourages agencies to share the data they collect broadly with other agencies across the country. It is common for an agency to search thousands of networks nationwide even when they don't have reason to believe a targeted vehicle left the region.

Via public records requests, EFF obtained datasets representing more than 12 million searches logged by more than 3,900 agencies between December 2024 and October 2025. The data shows that agencies logged hundreds of searches related to the 50501 protests in February, the Hands Off protests in April, the No Kings protests in June and October, and other protests in between.

The Tulsa Police Department in Oklahoma was one of the most consistent users of Flock Safety's ALPR system for investigating protests, logging at least 38 such searches. This included running searches that corresponded to a protest against deportation raids in February, a protest at Tulsa City Hall in support of pro-Palestinian activist Mahmoud Khalil in March, and the No Kings protest in June. During the most recent No Kings protests in mid-October, agencies such as the Lisle Police Department in Illinois, the Oro Valley Police Department in Arizona, and the Putnam County (Tenn.) Sheriff's Office all ran protest-related searches.

While EFF and other civil liberties groups argue the law should require a search warrant for such searches, police are simply prompted to enter text into a "reason" field in the Flock Safety system. Usually this is only a few words–or even just one.

In these cases, that word was often just "protest."

Crime does sometimes occur at protests, whether that's property damage, pick-pocketing, or clashes between groups on opposite sides of a protest. Some of these searches may have been tied to an actual crime that occurred, even though in most cases officers did not articulate a criminal offense when running the search. But the truth is, the only reason an officer is able to even search for a suspect at a protest is because ALPRs collected data on every single person who attended the protest.

**Search and Dissent**

2025 was an unprecedented year of street action. In June and again in October, thousands across the country mobilized under the banner of the "No Kings" movement—marches against government overreach, surveillance, and corporate power. By some estimates, the October demonstrations ranked among the largest single-day protests in U.S. history, filling the streets from Washington, D.C., to Portland, OR.

EFF identified 19 agencies that logged dozens of searches associated with the No Kings protests in June and October 2025. In some cases the "No Kings" was explicitly used, while in others the term "protest" was used but coincided with the massive protests.

**Law Enforcement Agencies that Ran Searches Corresponding with "No Kings" Rallies**

- Anaheim Police Department, Calif.
- Arizona Department of Public Safety
- Beaumont Police Department, Texas
- Charleston Police Department, SC
- Flagler County Sheriff's Office, Fla.
- Georgia State Patrol
- Lisle Police Department, Ill.
- Little Rock Police Department, Ark.
- Marion Police Department, Ohio
- Morristown Police Department, Tenn.
- Oro Valley Police Department, Ariz.
- Putnam County Sheriff's Office, Tenn.
- Richmond Police Department, Va.
- Riverside County Sheriff's Office, Calif.
- Salinas Police Department, Calif.
- San Bernardino County Sheriff's Office, Calif.
- Spartanburg Police Department, SC
- Tempe Police Department, Ariz.
- Tulsa Police Department, Okla.
- US Border Patrol

For example:

- In Washington state, the Spokane County Sheriff's Office listed "no kings" as the reason for three searches on June 15, 2025 [Note: date corrected]. The agency queried 95 camera networks, looking for vehicles matching the description of "work van," "bus" or "box truck."
- In Texas, the Beaumont Police Department ran six searches related to two vehicles on June 14, 2025, listing "KINGS DAY PROTEST" as the reason. The queries reached across 1,774 networks.
- In California, the San Bernardino County Sheriff's Office ran a single search for a vehicle across 711 networks, logging "no king" as the reason.
- In Arizona, the Tempe Police Department made three searches for "ATL No Kings Protest" on June 15, 2025 searching through 425 networks. "ATL" is police code for "attempt to locate." The agency appears to not have been looking for a particular plate, but for any red vehicle on the road during a certain time window.

But the No Kings protests weren't the only demonstrations drawing law enforcement's digital dragnet in 2025.

For example:

- In Nevada's state capital, the Carson City Sheriff's Office ran three searches that correspond to the February 50501 Protests against DOGE and the Trump administration. The agency searched for two vehicles across 178 networks with "protest" as the reason.

- In Florida, the Seminole County Sheriff's Office logged "protest" for five searches that correspond to a local May Day rally.
- In Alabama, the Homewood Police Department logged four searches in early July 2025 for three vehicles with "PROTEST CASE" and "PROTEST INV." in the reason field. The searches, which probed 1,308 networks, correspond to protests against the police shooting of Jabari Peoples.
- In Texas, the Lubbock Police Department ran two searches for a Tennessee license plate on March 15 that corresponds to a rally to highlight the mental health impact of immigration policies. The searches hit 5,966 networks, with the logged reason "protest veh."
- In Michigan, Grand Rapids Police Department ran five searches that corresponded with the Stand Up and Fight Back Rally in February. The searches hit roughly 650 networks, with the reason logged as "Protest."

Some agencies have adopted policies that prohibit using ALPRs for monitoring activities protected by the First Amendment. Yet many officers probed the nationwide network with terms like "protest" without articulating an actual crime under investigation.

In a few cases, police were using Flock's ALPR network to investigate threats made against attendees or incidents where motorists opposed to the protests drove their vehicle into crowds. For example, throughout June 2025, an Arizona Department of Public Safety officer logged three searches for "no kings rock threat," and a Wichita (Kan.) Police Department officer logged 22 searches for various license plates under the reason "Crime Stoppers Tip of causing harm during protests."

Even when law enforcement is specifically looking for vehicles engaged in potentially criminal behavior such as threatening protesters, it cannot be ignored that mass surveillance systems work by collecting data on everyone driving to or near a protest—not just those under suspicion.

**Border Patrol's Expanding Reach**

As U.S. Border Patrol (USBP), ICE, and other federal agencies tasked with immigration enforcement have massively expanded operations into major cities, advocates for immigrants have responded through organized rallies, rapid-response confrontations, and extended presences at federal facilities.

USBP has made extensive use of Flock Safety's system for immigration enforcement, but also to target those who object to its tactics. In June, a few days after the No Kings Protest, USBP ran three searches for a vehicle using the descriptor "Portland Riots."

USBP has made extensive use of Flock Safety's system for immigration enforcement, but also to target those who object to its tactics.

USBP also used the Flock Safety network to investigate a motorist who had "extended his middle finger" at Border Patrol vehicles that were transporting detainees. The motorist then allegedly drove in front of one of the vehicles and slowed down, forcing the Border Patrol vehicle to brake hard. An officer ran seven searches for his plate, citing "assault on agent" and "18 usc 111," the federal criminal statute for assaulting, resisting or impeding a federal officer. The individual was charged in federal court in early August.

USBP had access to the Flock system during a trial period in the first half of 2025, but the company says it has since paused the agency's access to the system. However, Border Patrol and other federal immigration authorities have been able to access the system's data through local agencies who have run searches on their behalf or even lent them logins.

**Targeting Animal Rights Activists**

Law enforcement's use of Flock's ALPR network to surveil protesters isn't limited to large-scale political demonstrations. Three agencies also used the system dozens of times to specifically target activists from Direct

Action Everywhere (DxE), an animal-rights organization known for using civil disobedience tactics to expose conditions at factory farms.

Delaware State Police queried the Flock national network nine times in March 2025 related to DxE actions, logging reasons such as "DxE Protest Suspect Vehicle." DxE advocates told EFF that these searches correspond to an investigation the organization undertook of a Mountaire Farms facility.

Additionally, the California Highway Patrol logged dozens of searches related to a "DXE Operation" throughout the day on May 27, 2025. The organization says this corresponds with an annual convening in California that typically ends in a direct action. Participants leave the event early in the morning, then drive across the state to a predetermined but previously undisclosed protest site. Also in May, the Merced County Sheriff's Office in California logged two searches related to "DXE activity."

As an organization engaged in direct activism, DxE has experienced criminal prosecution for its activities, and so the organization told EFF they were not surprised to learn they are under scrutiny from law enforcement, particularly considering how industrial farmers have collected and distributed their own intelligence to police.

The targeting of DxE activists reveals how ALPR surveillance extends beyond conventional and large-scale political protests to target groups engaged in activism that challenges powerful industries. For animal-rights activists, the knowledge that their vehicles are being tracked through a national surveillance network undeniably creates a chilling effect on their ability to organize and demonstrate.

**Fighting Back Against ALPR**

ALPR systems are designed to capture information on every vehicle that passes within view. That means they don't just capture data on "criminals" but on everyone, all the time—and that includes people engaged in their First Amendment right to publicly dissent. Police are sitting on massive troves of data that can reveal who attended a protest, and this data shows they are not afraid to use it.

Our analysis only includes data where agencies explicitly mentioned protests or related terms in the "reason" field when documenting their search. It's likely that scores more were conducted under less obvious pretexts and search reasons. According to our analysis, approximately 20 percent of all searches we reviewed listed vague language like "investigation," "suspect," and "query" in the reason field. Those terms could well be cover for spying on a protest, an abortion prosecution, or an officer stalking a spouse, and no one would be the wiser–including the agencies whose data was searched. Flock has said it will now require officers to select a specific crime under investigation, but that can and will also be used to obfuscate dubious searches.

For protestors, this data should serve as confirmation that ALPR surveillance has been and will be used to target activities protected by the First Amendment. Depending on your threat model, this means you should think carefully about how you arrive at protests, and explore options such as by biking, walking, carpooling, taking public transportation, or simply parking a little further away from the action. Our Surveillance Self-Defense project has more information on steps you could take to protect your privacy when traveling to and attending a protest.

For local officials, this should serve as another example of how systems marketed as protecting your community may actually threaten the values your communities hold most dear. The best way to protect people is to shut down these camera networks.

Everyone should have the right to speak up against injustice without ending up in a database.