



**KNOW
WHO IS
WATCHING**

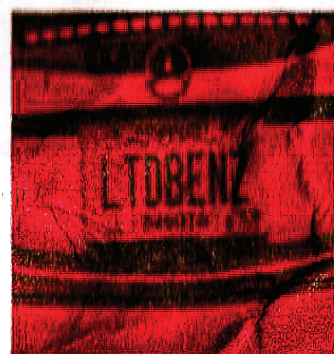
-Ryan Zielie-

You were recorded today.

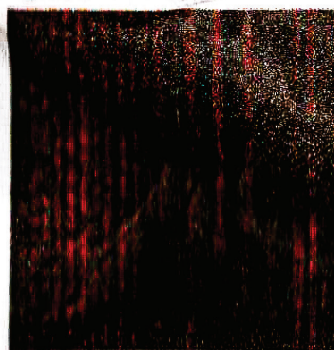
You were recorded today. Not because you did anything wrong. Not because anyone suspected you of anything. You were recorded because you drove down a road.

Flock records everyone, including YOU.

There was no warning. No sound. No notification. Nothing in the environment changed. The road looked like a road. The neighborhood looked like a neighborhood. You had no reason to think anything was happening...but something was.



Your license plate was photographed. The image was processed.



Your plate number, the time, and your exact location were converted into a data entry and stored in a database.



It can be searched, shared, and accessed by thousands of law enforcement agencies.



Without a warrant, without your knowledge, and without any suspicion that you did anything wrong.



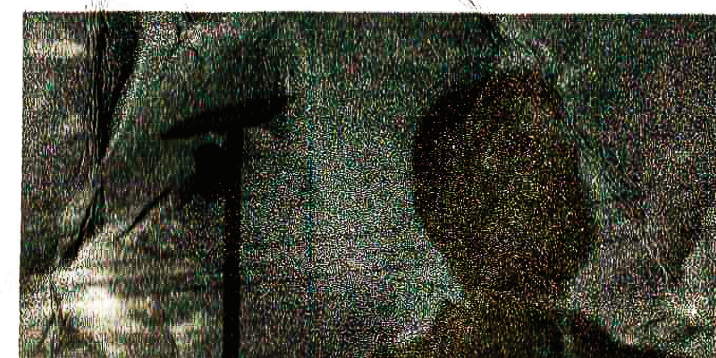
You drive to work, Its logged.

You go to pick up your kids, Its logged.

You go to the doctor or the grocery store, all logged.

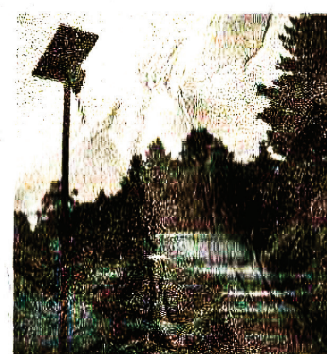
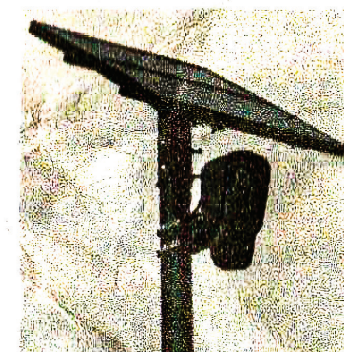
You weren't targeted. You were just there. and still you're logged.

You were recorded today,



Flock Safety performs over 20 billion license plate scans every month.

flocksafety.com



What is Flock?

Flock Safety is a \$7.5 billion surveillance company. Their cameras line American roads, neighborhood entrances, and intersections across 49 states. Most people have never heard of it.

The cameras are small and solar powered. They don't look like

surveillance equipment. They blend into existing infrastructure. That unobtrusiveness is intentional. When your vehicle passes within range, the camera captures an image automatically. No human presses a button. No one decides whether you're worth recording. The system records everything.

In 7 years, Flock built the largest private surveillance network in American history. Valued at \$7.5 billion.

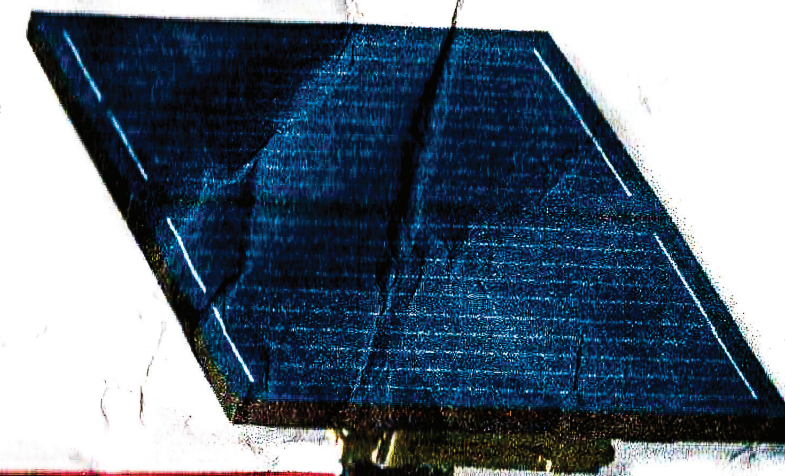
flocksafety.com



Your plate number, time, location, vehicle make, model, and color are packaged into a data entry and uploaded to Flock's network. Over days and weeks, repeated scans of the same vehicle form a picture. Where you go. When you go there. What your patterns look like.

One scan is a data point. Ten scans is a pattern. A hundred scans is a record. The system doesn't just capture moments. It accumulates them. Over time it knows your routine better than you do.

You didn't choose to be part of this network. There was no opt-in. No terms of service. No notification that your movements were being logged. The system was simply installed, and you became part of it the moment you drove past it.



How it works.

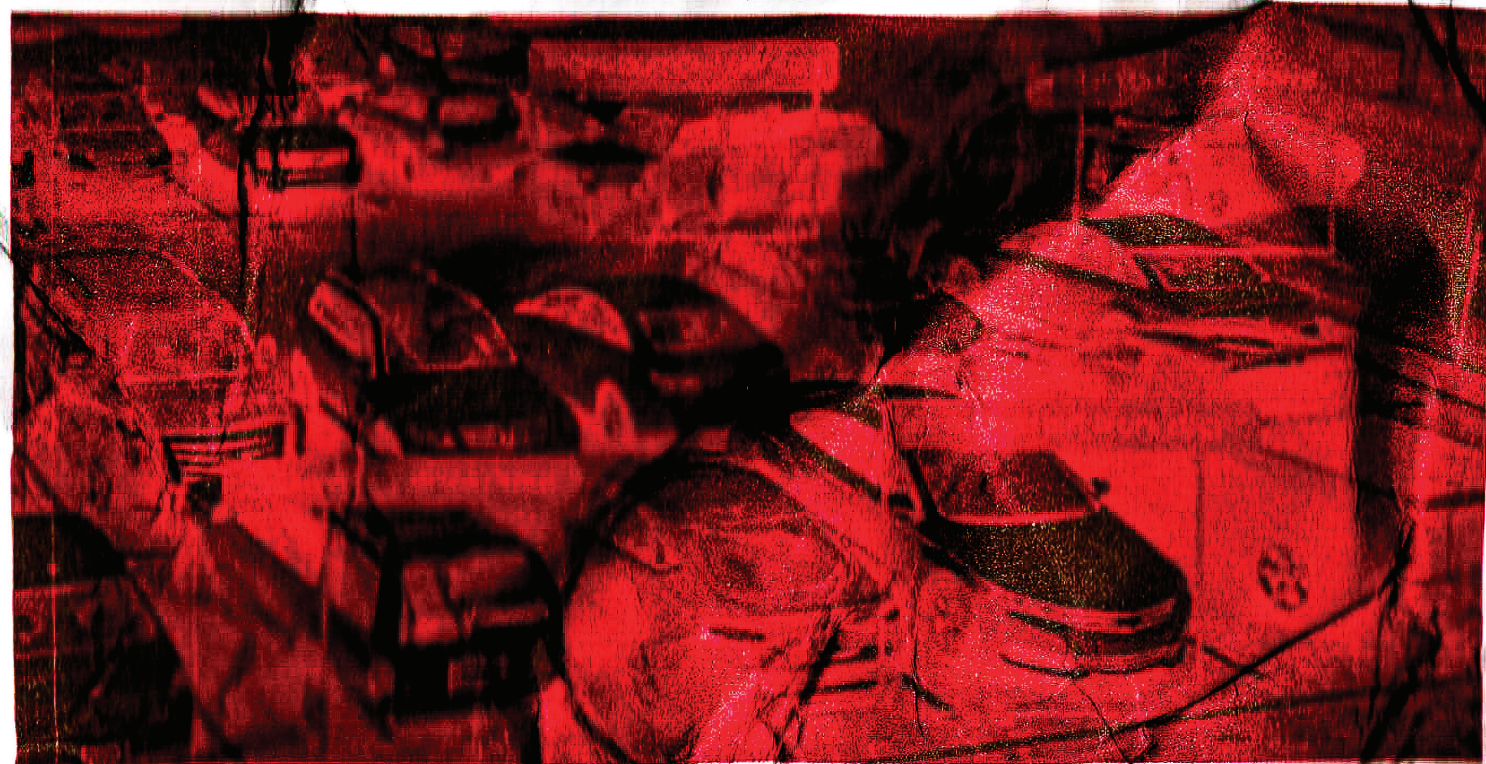
The process is fast, automatic, and requires almost no human involvement. Your vehicle enters the camera's field of view. An image is captured. Software reads your plate and converts it to text. Time and location are logged. The entry is stored and indexed in a searchable database. This happens in seconds.

The camera does not care who you are. It does not assess whether you look suspicious or whether you have done anything wrong. It records everyone equally because that is the only way the business model works. More data means a more valuable network. You are not a person to this system. You are a data point.

That data does not stay local either. A scan recorded in your neighborhood can be searched by an officer in another state entirely. You have no way of knowing who has looked at your records, when, or why. There is no notification. There is no log you can access. The information flows in one direction.

In a single month in 2025, San Jose's Flock database was searched 3,965,519 times. The vast majority of those searches were conducted without a warrant.

eff.org



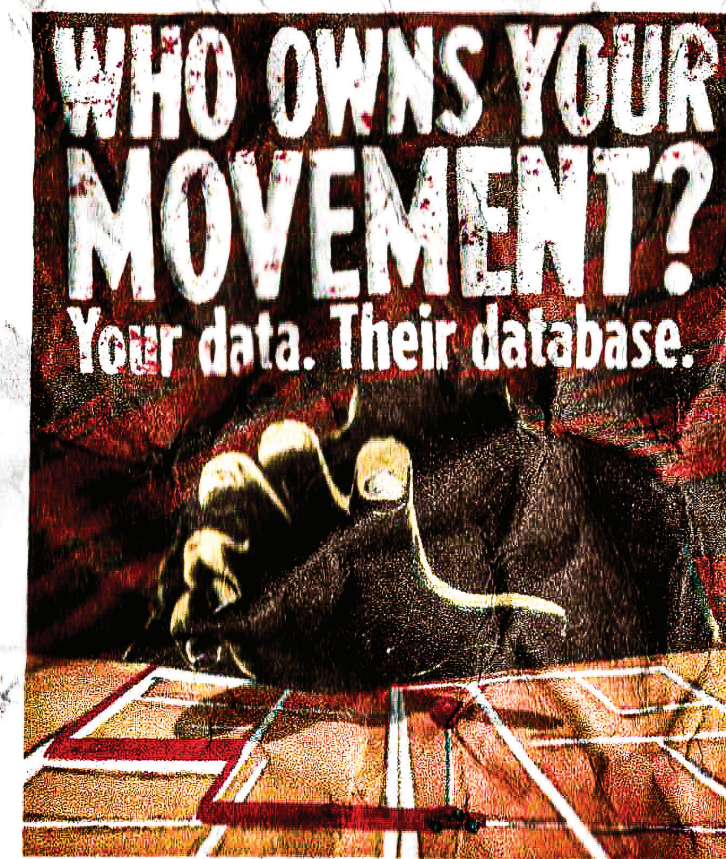
How it works. |

For years, American politicians and media have pointed to China as a cautionary tale. The surveillance state. Cameras on every corner. Citizens tracked by their government without consent. It has been held up as proof of authoritarianism, as evidence of a system incompatible with freedom.

Those same politicians represent districts covered by Flock cameras. Those same media outlets operate in cities where every vehicle that passes a major intersection is logged, stored, and made searchable by thousands of agencies without a warrant. The infrastructure they warned about exists here. It was just built by a private company with a friendly name.

The difference between a surveillance state and a surveillance market is not freedom. It is branding. China's system is operated by the government and people know it exists. America's system is operated by a \$7.5 billion corporation and most people have never heard of it. It is difficult to argue that ignorance makes it more acceptable.

You cannot claim to stand against surveillance while funding it, installing it, and granting it access to your data. The outrage was never about the cameras. It was about who owned them.



There is a reason Flock was built by a private company and not the government. The government would have faced immediate constitutional challenges. A private company can collect the same data, build the same network, and sell access back to law enforcement without the same legal scrutiny. Flock didn't circumvent the system. It found the gap and built a \$7.5 billion business inside it. They installed cameras on public roads without permits. They didn't ask. They just put them up.

Size and scale.

90,000 cameras.

49 states.

5,000+ communities.

7,000+ agencies with
search access.

20,000,000,000 scans.
Every month.

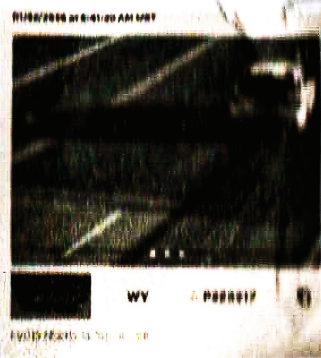
In Oakland, 293 cameras scanned 1.4 million vehicles in a single month. Those scans produced 232 arrests over 17 months. The rest of that data, belonging to people never connected to any crime, was collected, stored, and retained anyway.

In a 30-day period in 2025, law enforcement ran over 450,000 searches of Flock's nationwide database. Most involved people never charged with anything.

Size and scale. |

If Flock's 20 billion monthly scans were printed as individual receipts and stacked, the pile would reach the moon and back.

Error and...



In a 2021 study, surveillance research firm IPVMI found a 10% error rate in Flock camera output. One in ten reads was inaccurate. At 20 billion scans per month that's a significant volume of bad data circulating through a system used to make real decisions about real people.

After IPVMI published their error rate findings, Flock stopped selling to them entirely. Their findings were never publicly refuted with independent data.

flocksafety.com



Misread plates have led to wrongful stops. People have been pulled over at gunpoint because an automated misread matched a flagged vehicle. They were innocent. The camera was wrong.



A 10% error rate in a database this large is not a minor technical problem. It is a structural one. And the people who bear the consequences of those errors are not the people who built the system.

oversight.

There is no federal law regulating automated license plate reader systems in the United States. No national standard for data retention. No warrant requirement before searching records. No limit on how many agencies can access a single network. No federal accountability when the system is misused.

Some communities have said no. Austin, Evanston, and Eugene cancelled or refused to renew Flock contracts after residents organized. The EFF and ACLU filed lawsuits and state audits were launched.



The technology expanded faster than the rules governing it and in that gap is where most of the documented abuses have occurred.



Illinois has state privacy protections and yet, In 2025, Border Patrol accessed Illinois Flock data in violation of those protections. The Illinois Secretary of State launched a formal audit. Those laws exist and yet, Flock's network architecture made them easier to route around.

eff.org



This affects us all.



Had an Abortion.

Those are not the words of a privacy advocate or a civil liberties organization. Those are the words of a Texas law enforcement officer, typed directly into Flock Safety's required audit log field as the stated reason for a multi-state database search.

In 2025, a Texas officer used Flock's nationwide network to track a woman suspected of self-administering an abortion. The search crossed state lines. It pulled location data from cameras in Washington state. It was conducted without a warrant. The reason for the search was logged in the officer's own words because Flock requires officers to enter a justification before running a query. That field, designed as an accountability measure, became the only evidence the search ever happened.

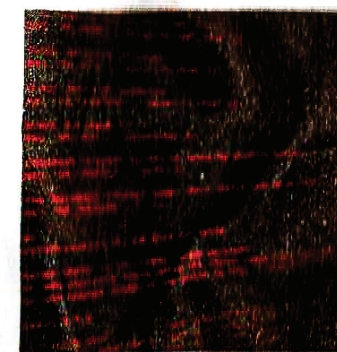


The woman had not been charged with a crime. The search was not part of an active criminal investigation in the traditional sense. It was a officer using a surveillance network to locate a woman based on a medical decision she made about her own body.



Search For Female.

This is not a hypothetical about what these systems could be used for. This is documentation of what they were used for. The infrastructure existed. The access was available. Someone decided to use it this way.



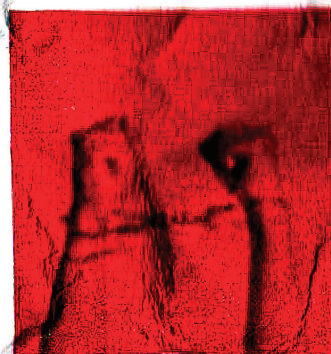
Flock's network does not know what it is being used for. It does not evaluate the reason an officer enters before running a search. It processes the query and returns the results. The system worked exactly as designed. That is the problem.

The audit log field exists so officers can be held accountable for their searches. In this case it was the only reason we know this search happened at all. Without it, it would have been invisible.

jsis.washington.edu



Multiple protesters



In 2025, the Electronic Frontier Foundation analyzed over 12 million searches logged by more than 3,900 law enforcement agencies across Flock's network. What they found went far beyond stolen cars and criminal investigations.

Hundreds of searches were directly tied to political demonstrations. Officers ran plates at protests organized under the names 50501, Hands Off, and No Kings. The searches were not triggered by criminal activity at the protests. They were triggered by the presence of vehicles near a demonstration.

The First Amendment protects the right to assemble. It does not protect your license plate from being recorded, stored, and searched because you parked near a protest. Those are two different things and Flock's network exists in the gap between them.

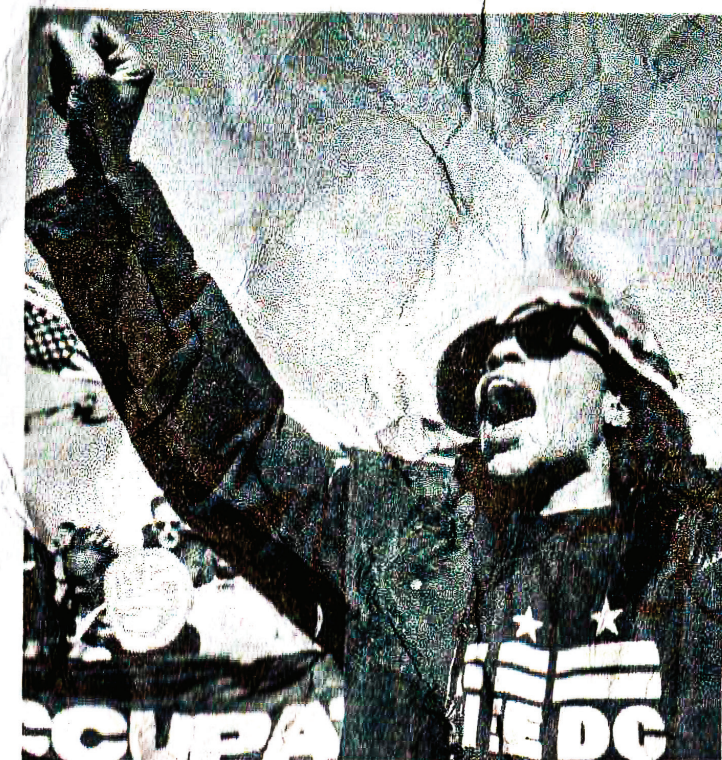


were logged.

There is a term for what happens when surveillance makes people afraid to exercise their rights. It is called a chilling effect. When people know they are being watched at a protest, some of them stop going. The demonstration gets smaller.

You do not have to be arrested to be surveilled. You just have to show up.

eff.org



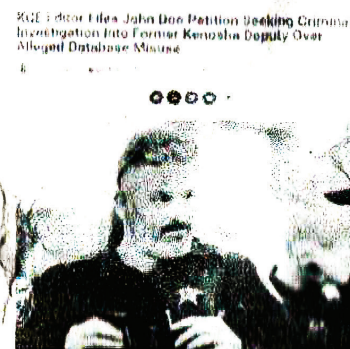
The message gets quieter. The surveillance does not need to result in an arrest to be effective. The knowledge that it exists is enough.



Officers Used Flock To Stalk Women.

At least 14 documented cases exist of officers using Flock and other ALPR systems to track romantic partners, ex-partners, and in at least one case, a complete stranger. The bulk of these incidents occurred since 2024, the same period when Flock dramatically expanded into thousands of new communities. Nearly all of the officers involved were criminally charged and lost their jobs, but most cases were not caught by Flock's internal systems. They were reported by the victims.

In Milwaukee, an officer tracked a woman he was dating and her ex-partner nearly 180 times over two months. His misconduct was only discovered after his victims looked up their own plate numbers on HaveIBeenFlocked.com, a site that collects Flock audit data made public by some local governments. In Florida, a sheriff's deputy tracked a woman he met on a TV set and eventually pulled her over. In Kansas, a police chief tracked his ex-girlfriend and her new partner over 200 times. These are the cases that got caught.



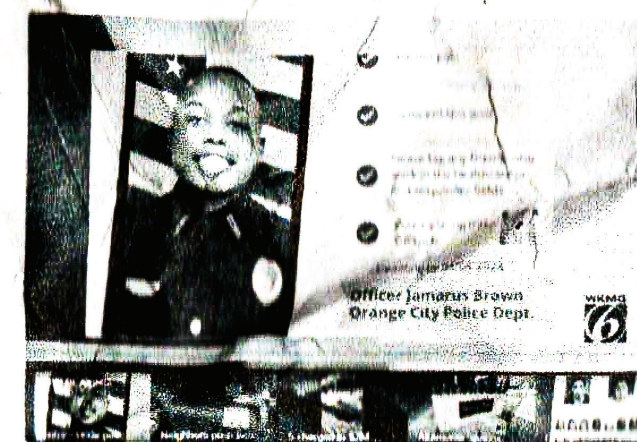
Florida police officer allegedly stalked woman's travels using license plate readers

HaveIBeenFlocked.com lets you look up whether your plate has been searched. Several stalking cases were discovered this way, not by Flock, not by police departments, but by the victims themselves.

ij.org

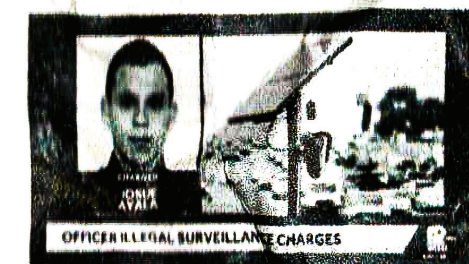
officer accused of stalking woman using license plate readers

Jamarus Brown, 29, faces charges of stalking and improper computer access



license plate readers to stalk and harass people

The website that started the investigation into Officer Josue Ayala



Flock's safeguards did not catch these officers. The victims did. In December 2025, after multiple stalking cases became public, Flock quietly updated their audit log system to anonymize all searches, making future abuse significantly harder to detect. The response to officers stalking women through the network was not to restrict access. It was to hide who was searching. The 14 documented cases are almost certainly an undercount, as officers frequently log vague or inaccurate search reasons and some misconduct gets resolved quietly.



13 Officers Accused



Alexander Vanny

In June 2024, Vanny was arrested on suspicion of forcible rape, kidnapping to commit rape, and forced oral copulation against a female sheriff's department volunteer, posting a \$1 million bond before those charges were ultimately not pursued to sentencing.

While out on bail he continued committing crimes against his former fiancée. He secretly followed her on a date, waited outside her home, and set up an audio recording device outside her bedroom window to record her having sex with another man. He then forced his way into the apartment and challenged the man to a fight. When she attempted to call 911 he damaged her phone. On a separate occasion he followed her to a bar, demanded she leave with him, and when she refused he forcibly threw her into his truck and drove her 17 miles to his home without her consent. He placed tracking devices on her car to monitor her movements, violated the restraining order she filed, and continued carrying a personal firearm in defiance of that order. He

also used department systems including Flock to track her friends. He was convicted of stalking, possession of child pornography, unauthorized use of protected electronic data, malicious destruction of a wireless device, witness intimidation, illicit eavesdropping, using a concealed camera to invade privacy, illegal use of a tracking device, interference with a traffic control device, and possession of a firearm in violation of a protective order.

He was sentenced to six years in state prison on February 6, 2026.

Sources: ABC7 KABC June 25 2024, KESQ February 6 2026, Institute for Justice ij.org



Kyle Rector*

Bonner Springs, Kansas, 2025
Used plate readers to track his estranged wife and two men he suspected were her new romantic partners.
Charged with multiple crimes, March 2026.

Michael McSherry

Westmoreland County, Pennsylvania, 2021
Pleaded guilty to stalking after using readers to track his estranged wife and other family members.
(Photo Credit: KDKA)



Victor Heiar

Kechi, Kansas, 2023
Pleaded guilty to computer crime and stalking after using Flock cameras to track his estranged wife.

Lee Nygaard*

Sedgwick, Kansas, 2023
Resigned after using Flock cameras to track his ex-girlfriend and her new boyfriend more than 200 times over several months.



*Cases marked have not resulted in a guilty plea or conviction at time of publication.
Source: Institute for Justice, ij.org

13 Officers Accused



Jarmarus Brown*
Orange City, Florida, 2024
Used ALPRs to stalk his girlfriend and her family members more than 100 times over seven months. Arrested and charged 2025.

Thadius Gordon*
Shelby County, Tennessee, 2024. Relieved of duty after using an ALPR database to track his ex-wife's location more than 100 times.



Roberto Cedeno*
Louisville, Kentucky, 2025
Charged with nine felonies after using the city's ALPR system to track an ex-partner and her friends hundreds of times over two months.

Josue Ayala*
Milwaukee, Wisconsin, 2025
Used Flock to track a woman he was dating and her ex-partner nearly 180 times over two months. Resigned 2026 after being charged with misconduct.



Frank McGrath*
Kenosha County, Wisconsin, 2025. Resigned with severance pay after using Flock to monitor a deputy he was romantically involved with.

Cristian Morales*
Menasha, Wisconsin, 2025
Placed on leave and charged with misconduct after his ex-girlfriend filed a complaint alleging he used Flock to track her.



Lamar Roman*
Monroe County, Florida, 2026
Used an ALPR system to track and eventually pull over a woman he met while working security on a TV set. Arrested and charged.
"I Saw a shiny object..."

Robert Josett
Costa Mesa, California, 2023
Used Flock to track his mistress and her other romantic interests. Pleaded guilty to multiple criminal charges, April 2026.



*Cases marked have not resulted in a guilty plea or conviction at time of publication.
Source: Institute for Justice, ij.org

[REDACTED]



[REDACTED]

[REDACTED]



[REDACTED]

Flock Safety's audit logs contain the full record of every search ever conducted on its network. Law enforcement agencies have repeatedly fought public records requests to keep those logs sealed. What they are willing to show you is that the system exists. What they are fighting to keep hidden is what it has been used for.

Now you know.

You were recorded today. You were recorded yesterday. You will be recorded tomorrow. Every road you drive, every neighborhood you pass through, every routine Tuesday morning commute is being logged, stored, and made searchable by thousands of agencies across the country.

You did not consent to this. You were not asked. The system was installed quietly, justified with crime statistics, and expanded without public debate. By the time most people find out it exists, they are already in the database. The facts in this publication are not hypothetical. A woman was tracked across state lines because of a medical decision she made about her own body. Protesters were logged for

showing up. Officers used the network to stalk women they were obsessed with. Border Patrol accessed data in states that had laws specifically prohibiting it. These things happened. They are documented. They will happen again because the infrastructure is still there and the oversight is not.

Awareness is not enough on its own. But it is where everything starts. The communities that pushed back did so because someone told them what was happening and they decided it was not acceptable. Austin cancelled their contract. Evanston cancelled theirs. Eugene cancelled theirs. Lawsuits were filed. Audits were launched. The system can be challenged. It has been.

You were recorded today.
Now you know.
What happens next is up to you.

Sources:

Electronic Frontier Foundation
eff.org

ACLU of Massachusetts
aclum.org

University of Washington Center for
Human Rights
jsis.washington.edu

The Oaklandside
oaklandside.org

Flock Safety
flocksafety.com

Institute for Justice
ij.org

ABC7 KABC
abc7.com

KESQ News Channel 3
kesq.com

WDRB Louisville
wdrb.com

WHAS11 Louisville
whas11.com

Fox35 Orlando
fox35orlando.com

Click Orlando
clickorlando.com

Fox6 Milwaukee
fox6now.com

WISN Milwaukee
wisn.com

Kenosha County Eye
kenoshacountyeye.com

Wikipedia / Flock Safety entry
wikipedia.org

Norfolk, Virginia Circuit Court
ruling, June 2024

HaveIBeenFlocked.com

deflock.org

This project was produced independently. It is not affiliated with any of the above organizations. All facts cited are sourced and verifiable.

You were recorded today.

Flock Safety operates 90,000 cameras across 49 states, performing over 20 billion scans every month. Their network has been used to track a woman across state lines for having an abortion, to surveil protesters exercising their First Amendment rights, and to give Border Patrol access to data in states with laws specifically designed to prevent it. At least 13 documented officers used it to stalk women they were obsessed with.