

Public Interest | Perspective

They're Watching Everything You Do. Unless They Don't Want To.

Michael Kirk Moore

MD, Plastic Surgeon, Freedom Wellness Spa, Freedom Surgical & Aesthetics, Utah, USA. www.freedomsurgicalutah.com

Submitted: 12 August 2026

Approved: 23 August 2026

Published: 24 August 2026

Address for correspondence: drmoore@psiutah.com

How to cite this article: How to cite this article: Moore MK. They're Watching Everything You Do. Unless They Don't Want To. G Med Sci. 2026; 7(1):60-69.

<https://www.doi.org/10.46766/thegms.pubi.26120802>

Copyright: © 2026 Michael Kirk Moore. This is an Open Access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The surveillance state has arrived. It's just not being used to find the truth - it's being used to control you. But don't worry, the people running it can be trusted. They've assured us.

KEYWORDS

Surveillance, Flock Safety Cameras, Body Cameras, Public Safety

INTRODUCTION

We've been told how this works.

A crime is committed. Law enforcement deploys its tools - the cameras, the databases, the license plate readers, the cell tower dumps - to find the person who did it. The technology serves the investigation. The evidence leads to the suspect. Justice is served. This is the social contract. This is what we pay for. This is what we're supposed to believe in.

And we do believe in it. We have to. Because the alternative - that the technology comes first, that the surveillance net is cast first, and the crime is found later, or invented, or ignored depending on who the target is - is too ugly to look at directly.

So, let's look at it directly.

MILWAUKEE: FIND THE PERSON, INVENT THE CRIME

The Milwaukee Police Department has 31 Flock Safety cameras. There are over 200 across the county. These cameras photograph every license plate that passes, log the time and location, and dump it all into a searchable database. Officers are supposed to use this system for "bona fide law enforcement purposes". They're required to enter a reason for each search. They're trained on the policy. They've been told: *this is for investigations, not for you*.

And thank God we have those policies. Because without them, who knows what might happen?

Well, here's what happened anyway.

Former Officer **Josue Ayala** used the Flock system to search his ex-girlfriend's license plate 55 times. He searched her new boyfriend's plate 124 times. Combined: **179 searches** over two months in spring 2025. Each time, he typed "investigation" into the reason field. He was on duty. He was protecting and serving. He was stalking his ex.

The victims discovered this because one of them went to *HaveIBeenFlocked.com* - a website built by private citizens, not the government, not the police department, not the Flock corporation - that lets you check whether your plate has been run through these databases. Let that sink in. The only reason these victims know they were stalked is because some civic-minded programmers built a tool that the system itself never provided. The system doesn't want you to know you're being watched. It wants you to assume it's all for your protection.

Ayala cut a deal. He resigned. He pleaded guilty to a misdemeanor - misconduct in public office. The prosecutor agreed to recommend a fine at sentencing. Let me repeat that: **a fine**. For 179

counts of using government surveillance equipment to stalk two people. If you or I put a tracking device on an ex-girlfriend's car, we'd be looking at felony stalking charges. But when a cop does it with taxpayer-funded equipment while on the clock? That's a fine. Maybe.

But this is where the story achieves a level of irony that would be funny if it weren't so wretched.

The detective assigned to investigate Ayala's misconduct was **Tehrangi Chapman** - 22-year veteran, Internal Affairs Division. Chapman was the one reviewing the audit trails. Chapman saw exactly what happens when an officer abuses the Flock system. Chapman saw the 179 searches, the fake "investigation" labels, the two traumatized victims. Chapman was the accountability mechanism. The system working as designed.

And then, according to a criminal complaint filed just days ago, Chapman did the same damn thing.

Twenty searches on two victims. Logged as "test" and "training". And - because why stop at license plate readers - Chapman also planted a physical GPS tracking device on one victim's vehicle without their knowledge or consent. When that victim found the device and confronted Chapman, they tried to make an anonymous report to MPD. They were, according to prosecutors, "visibly shaken" and "upset that their identity was discovered during the investigation".

Chapman now faces felony misconduct in public office and misdemeanor misuse of a GPS device. He's been suspended for four months. He faces up to three and a half years.

So, the scorecard for Milwaukee's Flock camera program, which we have all been assured exists only for legitimate criminal investigations and is governed by strict departmental policies:

- **Officer #1** stalks his ex 179 times. Resigns. Gets a fine.
- **Detective #2** investigates Officer #1, then gets caught doing the same thing — plus a GPS tracker. Faces felony charges.
- The department responds by "increasing audits" and "trimming down access."

The system works. The policies are robust. The oversight is vigilant. The people in charge can absolutely be trusted not to abuse their positions of authority. They've told us so. Repeatedly.

UTAH: FIND THE CRIME, THEN FIND THE PERPETRATOR - UNLESS YOU DON'T FEEL LIKE IT

Now let's look at how this technology is deployed when it actually matters - when there's a real crime, a real victim, and a real need to find the perpetrator.

Tyler Robinson stands accused of assassinating Charlie Kirk at Utah Valley University (UVU) in September 2025. The highest-profile murder case in Utah history, and certainly the highest profile assassination since JFK in 1963. Death penalty on the table. Preliminary hearing just wrapped - a full week of testimony.

The prosecution presented grainy, spliced campus surveillance footage, sometimes not even in chronological order. DNA evidence - a screwdriver, a towel, possible contributor matches. Videotaped testimony from Robinson's former roommate about an alleged confession note. Photographs of the rifle. Engraved bullet casings. A Chick-fil-A receipt.

Here's what they didn't present.

No Flock camera data. Utah is blanketed with these things. They're on I-15, on University Parkway, on every major intersection in Utah County. If Robinson drove to UVU that day - and the prosecution's own

narrative has him parking in a nearby neighborhood, caught on a doorbell camera - his vehicle should have triggered multiple Flock captures. License plate. Time stamp. Location. A digital breadcrumb trail from his apartment to the campus. None of this was presented at the hearing.

No cell phone tower pings. The prosecution has Robinson on campus for hours before the shooting. They showed surveillance footage of someone they say is him - walking around, buying Chick-fil-A, changing clothes, making contact with Kirk's staff. Hours of alleged presence. And yet: no cell tower data. No location pings. No digital confirmation that Robinson's phone was anywhere near UVU during the time in question. Tyler was even 'seen' on camera holding his cellphone. In any modern investigation, this is standard. It was notably absent.

No mention of the Panguitch debit card transaction. According to what's been reported, Robinson allegedly had a witnessed debit card transaction in Panguitch, Utah — a small town roughly 200 miles south of Provo — between 9:00 and 9:50 p.m. on the night of the shooting. That's nearly a four-hour drive from UVU. If that transaction is real and verified, it raises serious questions about the timeline. The FBI was notified of this witnessed visit, but never followed up. Was this even disclosed to the defense? Why has it not been followed up on? At the preliminary hearing, it was never mentioned. Not once.

HOW MANY CAMERAS ARE WE TALKING ABOUT?

Let's put some numbers on this, because "Utah is blanketed with these things" isn't rhetoric — it's math.

Provo Police Department: 23 Flock cameras installed in April 2023. Twenty-three cameras covering roughly 640 miles of city roadways. That's

the official number from the city's own transparency portal.

Orem Police Department: Flock cameras operational as of 2025. The exact count isn't publicly listed - Orem is less transparent than Provo on this - but the department has been confirmed as a Flock customer.

Utah County Sheriff's Office: Flock cameras operational as of 2025. Again, no public count disclosed.

BYU Police Department: Automated license plate readers operational.

And the surrounding departments: Lone Peak PD (12 cameras), Pleasant Grove, Springville, Salem, Saratoga Springs, Spanish Fork, Highland (7 cameras) - every single police department in Utah County is running Flock or equivalent ALPR systems.

Conservative estimate: **well over 60 Flock cameras in Utah County alone**, all feeding into a shared, searchable database with 30-day retention. That's not counting the cameras operated by UDOT, by private businesses that share feeds with law enforcement, or by neighboring counties whose data is accessible through Flock's networked architecture.

The UVU campus sits at the intersection of University Parkway and I-15 - one of the most heavily trafficked and heavily surveilled corridors in the state. There are Flock cameras on University Parkway. There are Flock cameras on the I-15 on-ramps and off-ramps within a mile of campus. There are Flock cameras on Geneva Road, on 800 North, on Bulldog Boulevard. A vehicle approaching UVU from any direction will pass multiple cameras.

If Tyler Robinson drove to UVU on September 10, 2025 - and the prosecution's own narrative,

backed by doorbell camera footage from a nearby neighborhood, says he parked his vehicle and walked to campus - then his license plate was captured. Multiple times. By multiple cameras. At multiple locations. With time stamps and GPS coordinates.

Where is that data?

The prosecution didn't present it. The defense apparently hasn't received it. And at a preliminary hearing where the state was supposed to demonstrate probable cause - the lowest evidentiary bar in the criminal justice system - nobody asked.

THE BODY CAMERA THAT CONVENIENTLY DIED

Then there's the body camera. And this one is almost too perfect.

UVU Police Officer Chris Bagley was the first officer to reach the roof of the Losee Center after the shooting. He ran up a public staircase. He spotted a red-and-black screwdriver on the roof - a piece of evidence that would later become central to the prosecution's DNA case. He observed what he described as a "sniper pad" disturbance in the gravel - the imprint of someone lying in a firing position. He was the first set of official eyes on what the state alleges was the sniper's nest.

And his body camera stopped recording. Right as he reached the roof.

Bagley's testimony, under questioning from defense attorney Kathryn Nester, was that his battery died. "I think my battery died. I don't know", he said. He had approximately 27 minutes of footage from that day. He did not recharge his body camera because, he said, "it was too chaotic".

Let's walk through what Axon body cameras actually record, because the audit trail capabilities of these

devices are extensive - and the public deserves to know what questions haven't been asked yet.

Axon body cameras - Provo PD and UVU PD both use Axon systems, confirmed by public records - generate a comprehensive device audit trail that logs, at minimum:

- **Every power-on and power-off event**, with date and time stamps
- **Battery percentage** at the time of each event
- **Recording start and end events**, with time stamps
- **GPS coordinates** added to recordings
- **When the camera was docked or undocked**
- **When video was accessed or streamed** using Axon View or Evidence Sync
- **Sleep mode entry and exit** (a distinct event from power-off)
- **Firmware version** and device status changes
- **Remaining storage capacity** at each event
- **A loud audible notification when battery reaches 10%**, and then an even more obnoxiously loud notification when it reaches 5%.
- **Function button presses, volume changes, stealth mode toggles, and indicator light changes**

This audit trail is exportable as both a PDF and a CSV file. It shows the entire life of the device for any selected date range. It cannot be altered by the officer. It is stored on Axon's servers, not on the camera itself. Every event, every action, every change is logged - including battery percentage at the moment of shutdown.

So, when Officer Bagley says "I think my battery died. I don't know" - the audit trail knows. It knows exactly what the battery percentage was when the camera shut off. It knows whether the camera was powered down manually or shut off due to low battery. It knows whether sleep mode was activated. It knows the GPS coordinates of the camera at the

moment it stopped recording. It knows whether anyone accessed or streamed the footage after the fact. It knows everything.

And Axon body cameras, per their own specifications, are designed to operate for a full shift. A standard Axon Body 3 or Body 4 camera provides 12 to 14 hours of battery life under normal operation. Bagley's camera recorded 27 minutes of footage before dying on the roof of the most important crime scene in Utah history.

Twenty-seven minutes. At the beginning of a shift. On the roof of the Losee Center. At the exact moment the first officer reached the sniper's nest.

The audit trail for that device - which the defense should be demanding in discovery, and which should have been presented or at least acknowledged at the preliminary hearing - would answer every question:

- What was the battery percentage when Bagley started his shift?
- What was the battery percentage when the camera shut off on the roof?
- Was the camera manually powered down or did it shut off due to low battery?
- If low battery, why was a camera with 14-hour battery life dead after 27 minutes?
- If manually powered down, who did it and why?
- Where are the GPS logs showing the camera's location throughout the shift?
- Was the footage accessed, reviewed, or altered after the fact?

None of this was presented at the preliminary hearing. None of this appears to have been provided to the defense. The officer's explanation - "I think my battery died. I don't know" - was accepted without follow-up.

Now, let's compare this to another Utah prosecution. **Kouri Richins**. Convicted of murdering her husband

in Park City. Her trial was a festival of surveillance-state evidence. Cell phone records - including sensor data showing she was holding the phone to her ear during the 911 call. GPS data. Digital forensic analysis of deleted text messages. Financial records. Body camera footage. A private investigator who logged 936 hours and over \$100,000 in billables. The state threw every piece of technological evidence they had at her. They convicted her.

So, here's the question that any reasonable person should be asking:

Why does one Utah defendant get buried in digital evidence - cell towers, GPS, deleted texts, financial forensics - while another defendant, in a case with national implications and the death penalty, gets a prosecution built on a roommate's recorded statement, some inconclusive ballistics, and a body camera that mysteriously died after 27 minutes on the most important roof in the state?

The technology exists. It's deployed. It's operational. We know this because:

- A Wayne County triple-homicide suspect was tracked across southern Utah and into Colorado using Flock cameras and GPS - just months ago. The system worked. The breadcrumbs led to the arrest.
- Kouri Richins was convicted on a mountain of digital evidence collected from the same kinds of systems that are apparently silent in the Robinson case.
- Milwaukee police officers can apparently search anyone's license plate 179 times without breaking a sweat - the data is there, it's accessible, it's comprehensive.

So, either the 60-plus Flock cameras that blanket Utah County all happened to be looking the other way on September 10, 2025 and the Axon body camera with 14-hour battery life just happened to die after 27 minutes at the exact moment the first

officer reached the sniper's nest - or the data exists and the prosecution chose not to present it.

You can draw your own conclusions about why.

THE FOURTH AMENDMENT: STILL ON THE BOOKS, IF THAT'S ANY COMFORT

Let's talk about what Flock cameras actually are, because the courts are working very hard to pretend, they're something else.

These are not traffic cameras. They are not red-light cameras. They are automated license plate readers that photograph every single vehicle that passes - not just suspect vehicles, not just stolen vehicles, not just vehicles associated with open investigations. Every vehicle. Every plate. Every time. They log the image, the plate number, the time, the GPS coordinates. They store this data - typically for 30 days, sometimes longer. They share it across jurisdictions, creating a searchable, networked database of vehicle movements across entire metropolitan areas.

In Wichita, Kansas, a defendant recently challenged the warrantless use of Flock data under the Fourth Amendment. The court acknowledged that he had standing to challenge the search. The court acknowledged that the Fourth Amendment protects against unreasonable searches. The court then ruled that nine Flock captures of his vehicle over the course of a single day did not constitute a search because - and this is the legal reasoning, I am not making this up - it wasn't *enough* surveillance to reveal "the whole of his movements".

So, the constitutional protection isn't based on whether you're being tracked without a warrant. It's based on *how many times* you're being tracked without a warrant. A few times? Perfectly fine. A lot of times? Maybe a problem. The threshold is undefined. The courts will let you know when

you've crossed it. Probably after you've already been convicted.

In Norfolk, Virginia - 176 Flock cameras - a federal judge just tossed a lawsuit challenging the system, ruling that the plaintiffs "failed to demonstrate that Norfolk's Flock cameras capture enough data to reveal the whole or virtual whole of their or other citizens' movements".

Notice the circular logic. The cameras don't violate the Fourth Amendment because there aren't *enough* of them yet to track your "whole movements". But every year, more cameras are installed. Every year, the net tightens. Every year, the database grows. And every year, the courts say: *still not enough. Check back later.*

Meanwhile, in Milwaukee, two officers used these same cameras to stalk romantic partners. One did it 179 times. The other did it 20 times and added a GPS tracker for good measure. The "bona fide law enforcement purpose" these searches were logged under was a lie. The oversight mechanisms failed. The audit trails caught them only because someone - a private citizen - built a website to check.

The Fourth Amendment says: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"*.

It does not say: *"Unless the search is done with a camera instead of a GPS tracker."*

It does not say: *"Unless the search only captures some of your movements, not all of them."*

It does not say: *"Unless the officer logs the search as 'training' and hopes nobody checks."*

It does not say: *"Unless the body camera battery just happens to die at the crime scene."*

But that's where we are.

THE REAL PURPOSE OF THE SURVEILLANCE STATE

The sales pitch for Flock cameras - and for the broader surveillance infrastructure they represent - is always the same. *Public safety. Crime-solving. Protecting communities. Finding the bad guys.*

And sometimes that's true. The Wayne County triple-homicide suspect was caught with Flock data. Real crime, real victims, real perpetrator. The system worked as advertised.

But the Milwaukee cases reveal what happens when the system is working as *designed*, not as advertised. The design is simple: give people with badges and passwords access to a database of everyone's movements, tell them to behave, and hope for the best. The design assumes that the people with access will be trustworthy. The design assumes that "investigation" means investigation and "training" means training. The design assumes that the human beings operating the surveillance apparatus will be held in check by... what, exactly? Their own conscience? The audit trail they know how to falsify? The internal affairs detective who's doing the same thing they are?

The Robinson hearing reveals the other side of the coin. When the surveillance state has data that might complicate the prosecution's narrative - cell tower pings that don't place the defendant at the scene, 60-plus Flock cameras that somehow didn't capture his vehicle, a debit card transaction 200 miles away, a body camera that died after 27 minutes on the most important roof in Utah - that data becomes mysteriously irrelevant. Not exculpatory, exactly. Just... not presented. Not followed up on. Not disclosed.

This is the three-tiered reality of the surveillance state:

Tier one: The technology is deployed aggressively against defendants the state wants to convict. Every camera, every ping, every deleted text message is excavated and presented as evidence of guilt. Kouri Richins gets the full digital autopsy.

Tier two: The technology is deployed recreationally by the people who operate it — to stalk ex-girlfriends, to track colleagues, to satisfy personal curiosity, all logged as "investigation" or "training." Milwaukee's finest can't stop running plates on their romantic interests.

Tier three: The technology is deployed selectively - or not deployed at all - when the evidence might point away from the state's preferred narrative. The cameras that blanket the Wasatch Front are suddenly silent. The cell towers that ping every phone in the county are suddenly offline. The body camera with a 14-hour battery dies at minute 27 on the sniper's roof. The database that tracked a triple-homicide suspect across state lines is suddenly empty.

This is not a bug. This is the feature. The surveillance state exists to serve power, not truth. It exists to build cases the state wants to build and to ignore evidence the state wants to ignore. It exists to give cops a tool to stalk their exes and to give prosecutors a tool to bury exculpatory leads. The "public safety" framing is the marketing copy. The reality is what you see in Milwaukee and Provo.

SO, WHAT DO WE DO ABOUT IT?

The Founders understood this. They didn't write the Fourth Amendment because they were worried about red-light cameras. They wrote it because they understood that power, unchecked, will always expand. That surveillance, once normalized, will

always be abused. That the people operating the machinery of the state are human beings with human weaknesses - jealousy, obsession, ambition, laziness, malice - and that no policy manual, no audit trail, no "bona fide law enforcement purpose" checkbox will stop them from using the tools they're given for purposes they're not supposed to pursue.

We've been told to trust the system. Trust the policies. Trust the oversight. Trust the people in charge.

In Milwaukee, the oversight detective was doing the same thing as the officer he was investigating.

In Utah, the surveillance state that convicted Kouri Richins can't seem to find any Flock data or cell tower pings on Tyler Robinson - and the body camera on the roof of the crime scene died after 27 minutes.

In federal courts across the country, judges are ruling that photographing every license plate on every road doesn't violate the Fourth Amendment - as long as there aren't *too many* cameras. Yet.

The system is not correcting itself. The system is not capable of correcting itself. The system is doing exactly what systems do: expanding, entrenching, protecting its own, and deploying its power selectively - heavily against some, lightly against others, not at all when inconvenient.

We are supposed to believe that law enforcement uses these tools to find the perpetrator after a crime has been committed. That's the social contract. That's the promise. And in a functioning republic, that's how it would work.

THIS IS NOT A DEMOCRACY ANYMORE

Tucker Carlson has been saying it plainly, and he's right: we don't live in a democracy. Not in any meaningful sense.

A democracy is a system where the government acts in the interests of the governed. Where our elected leaders make laws that benefit the people who sent them there - not themselves, not their donors, not the surveillance contractors pitching the next camera network. Where the institutions exist to serve the public, not to manage it. Where the technology serves the investigation, not the other way around.

What we have instead is a managerial state. A surveillance apparatus. A legal system that deploys its full technological weight against some defendants while mysteriously finding its hands empty against others. A police force where officers use license plate readers to stalk their ex-girlfriends, and the detective assigned to investigate them turns out to be doing the exact same thing. A public health bureaucracy that spent two years telling you to mask your toddler while Nancy Pelosi got her hair done maskless in a closed salon. An intelligence community that classifies everything and discloses nothing. A federal government that spent three years trying to imprison a doctor for giving patients a choice, then walked away mid-trial when the facts started coming out.

Nothing is being done for our benefit. That's not an opinion - it's the definition of the absence of democracy. When the government ceases to act in the interests of the governed, the governed no longer live in a democracy. They live in something else. Something that still holds elections and still flies the flag and still uses the old vocabulary but is no longer answerable to the people it pretends to serve.

The Founders gave us a remedy for this. It's in the Declaration of Independence - the document that created this country:

"Whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new

Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness."

That's not radical. That's not fringe. That's the founding document of the United States of America. The right to overthrow a government that no longer serves the people isn't some internet conspiracy - it's the entire premise of this country. It's the escape hatch the Founders built into the system because they knew - from hard experience with the British Crown - that power doesn't self-correct. *Power corrupts and absolute power corrupts absolutely.*

We're not there yet. But we're closer than most people care to admit. When police officers stalk citizens with surveillance tech and just get fines. When prosecutors bury exculpatory evidence while building death penalty cases. When the courts rule that photographing every vehicle on every road doesn't violate the Fourth Amendment because it only captures a *few* of your movements - for now. When the same government that tried to put me in prison for 35 years suddenly decides, mid-trial, that it was all "in the interests of justice" to walk away.

That's not justice. That's not democracy. That's power protecting itself and using every tool at its disposal to do so.

The Flock cameras are just the most visible piece of it. They're the part you can see from your car window. But behind them is an entire architecture of surveillance, classification, selective prosecution, and narrative management that has nothing to do with public safety and everything to do with control.

The question isn't whether the system is broken. The question is whether enough Americans still remember what it feels like to be free - and whether they're willing to demand it back.

Noli Parere

ABOUT THE AUTHOR

Dr. Michael Kirk Moore is an ex-board-certified plastic surgeon in Utah. In 2023, he was indicted on federal charges related to his COVID-19 vaccine clinic. All charges were dismissed by Attorney General Pam Bondi in July 2025. His forthcoming book is OATH: Truth, Medicine, and the Price of Integrity.