



A WORKSHOP FOR FEDERAL DEFENDERS · ASHEVILLE, NORTH CAROLINA

Law Enforcement Use of AI

How these systems build the case against your client, and how to take that case apart.

Lars Daniel · Director of Digital Forensics, Rimkus · Forbes contributor

Lars Daniel



Expert Testimony

- Qualified and testified in State, Federal, and international courts. Testified as an expert in computer, cell phone, digital, photo, video and audio forensics.

Journalist

- Writing for Forbes on digital evidence, artificial intelligence, and the impact of technology in law, risk, and insurance.

Author

- *Digital Forensics For Legal Professionals, 2011*
- *Digital Forensics Trial Graphics, 2016*
- *The Trucking Defense Guide to Cell Phone Forensics, 2025*

Educator

- 400+ speaking engagements

Forbes

CLM

ATTORNEY
AT LAW
MAGAZINE

dri
Lawyers
Representing
Business.™



NEWS
NATION

Quimbee

Attorney Credits®

LEXVID



Federal Bar
Association

myLawCLE



AI For Humans

- Preparing your defendant for testimony.
- Preparing witnesses for testimony.
- Preparing experts for testimony.



 correct

Training note. You just conceded that the company knew it needed to act sooner but chose not to until after the plaintiff was injured. This is a direct admission of prior knowledge and inaction, which the attorney will use to prove the company prioritized budget over safety. The defense is to reframe the timing. "We recognized the need to accelerate the program, and we made that business decision based on our resources at the time. It does not mean we ignored known risks before this incident." The principle is to separate the business decision of timing from the moral implication of ignoring safety.

 Back on the record. You said the company recognized the need to act sooner only after this crash. So before this nurse was hurt, the company knew it needed to act sooner but chose not to?

We recognized the need to accelerate the program, and we made that business decision based on our resources at the time. It doesn't mean we ignored the known risks before this incident.

 You said the company made a business decision based on resources at the time. So the company weighed the cost of thirty-four dollars a truck against the risk to the public, and decided the risk was acceptable until this crash proved otherwise?



 Take all the time you need. The record will wait.







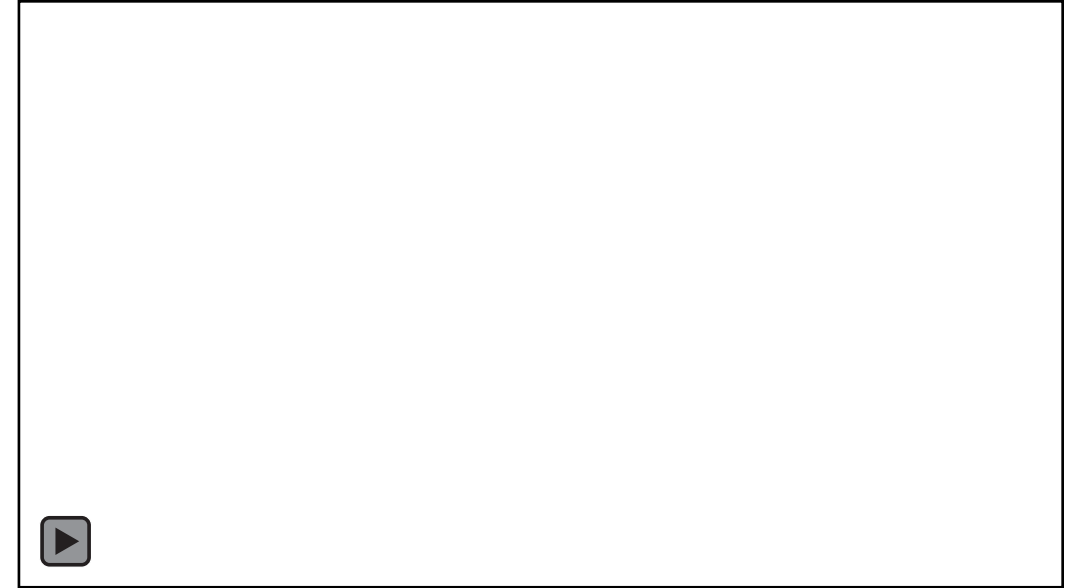
Four girls, face down, at gunpoint

A Sunday afternoon in Aurora, Colorado. Brittney Gilliam is taking four girls to get their nails done. Her daughter, her sister, and her nieces. The youngest is six.

A license plate camera reads her SUV and matches it to a stolen motorcycle from Montana. A motorcycle.

Minutes later, four girls are face down in a parking lot, in handcuffs, at gunpoint. The city later settled for 1.9 million dollars.

A machine made a mistake. The humans around it treated the mistake as truth.



The stop, as it aired. CBSN Denver, 2020. 46 seconds, embedded.

Sentinel Colorado on the 1.9 million dollar settlement. CBSN Denver footage, 2020.

“I saw a shiny thing”

Six years later. Last week, 404 Media published the investigative file on Lamar Roman, a Monroe County, Florida officer who spotted a woman near the Bad Monkey production set in the Keys and decided to find her.

He ran her plate and added it to a license plate reader hot list, so the camera network would alert him whenever her car moved. Asked why, his answer, as quoted in the records: “I mean, I saw a shiny thing, teasing and all that.”

He was charged with stalking and fired, and per the reporting he entered a plea deal. The cameras did exactly what they were built to do. They found her.



404 Media, Aug. 19, 2026. Quotes and case details per the investigative records the outlet obtained.

They do not think like you do

- **You work one client at a time. They work a billion data points at a time.**

Your unit of analysis is one case, one set of facts, one person whose liberty is on the line. The people building these systems think in populations and probabilities, and that difference in units explains most of what follows.

- **The ideology has a name: the TESCREAL bundle.**

Two scholars, Timnit Gebru and Emile Torres, named the cluster of ideologies that dominates this corner of Silicon Valley. Strip the philosophy vocabulary and the core idea is simple: the moral weight sits with the future at maximum scale, and technology is the engine that gets us there.

- **In that frame, one person is a rounding error.**

Never out of cruelty, always out of arithmetic. When the unit of concern is all of humanity forever, one wrongful arrest does not move the number.

- **It explains every design choice you are about to see.**

Safeguards that ship turned off. Audit tools nobody is required to use. A demo culture that treats live cameras as sales material. None of it is surprising once you know the frame.

The money behind the cameras

Thiel, 2009: "I no longer believe that freedom and democracy are compatible."

Thiel, 2014: "Competition is for losers."

- **He co-founded Palantir. His fund invests in Flock.**

Palantir holds roughly 140 million dollars in ICE contracts, including a 30 million dollar immigration tracking platform. His venture firm, Founders Fund, joined Flock Safety's investor list in the March 2025 round, and Flock was last valued around 7.5 billion dollars.

- **Nobody at that table measures wrongful stops.**

The customers being satisfied are investors measuring scale and agencies measuring clearance rates. The person the system got wrong is not on anyone's dashboard, which means the checking falls to this room.

WATCH HIM SAY IT

Should the human race survive?

- *Douthat: you would prefer the human race to endure, right? A pause. Douthat again: you're hesitating.*
- **His venture firm is among Flock Safety's investors. This is the worldview behind the cameras, in his own words.**

NYT, Interesting Times with Ross Douthat, 2025, excerpt at the exchange. Coverage per Complex and The Nation.



WHY THIS MATTERS IN A COURTROOM

A system built to optimize aggregates produces evidence that treats your client as an aggregate.

That is why the safeguards ship turned off. That is why the audit tools are optional. Friction costs money, and your client's case is friction.

The correction mechanism they did not design for is the one sitting in this room.

PART ONE OF FIVE

Flock and the plate dragnet

The abuse record, the discovery request, and the cross. This one touches more of your cases than anything else in the hour.

A private, searchable record of where cars go

- **The cameras photograph every plate that passes.**

Flock sells license plate readers to about 5,000 communities. Every passing car is photographed, stamped with time and location, and loaded into a searchable database, whether or not anyone is suspected of anything.

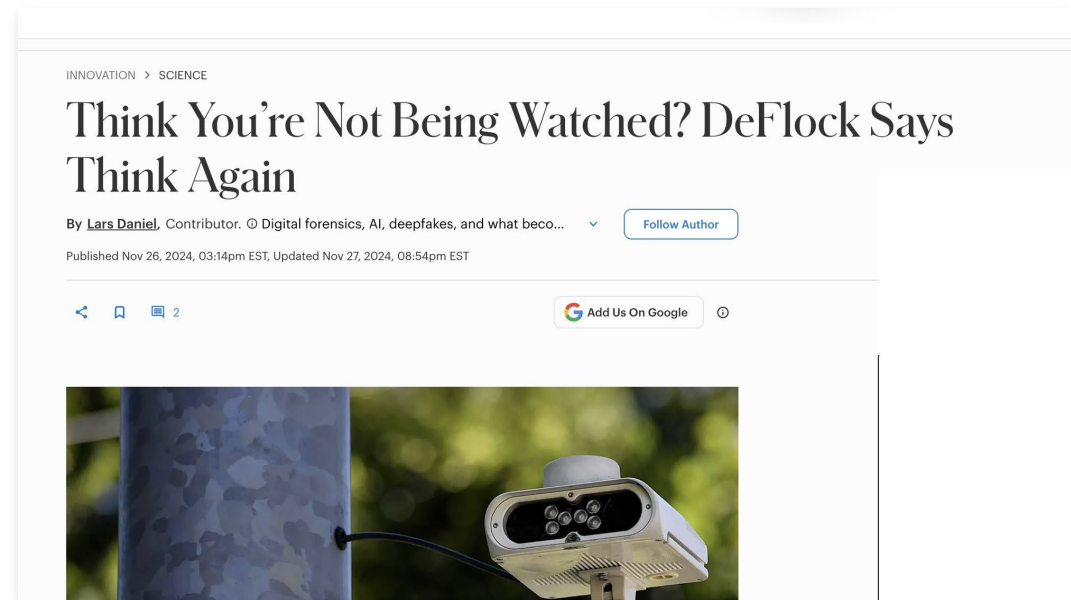
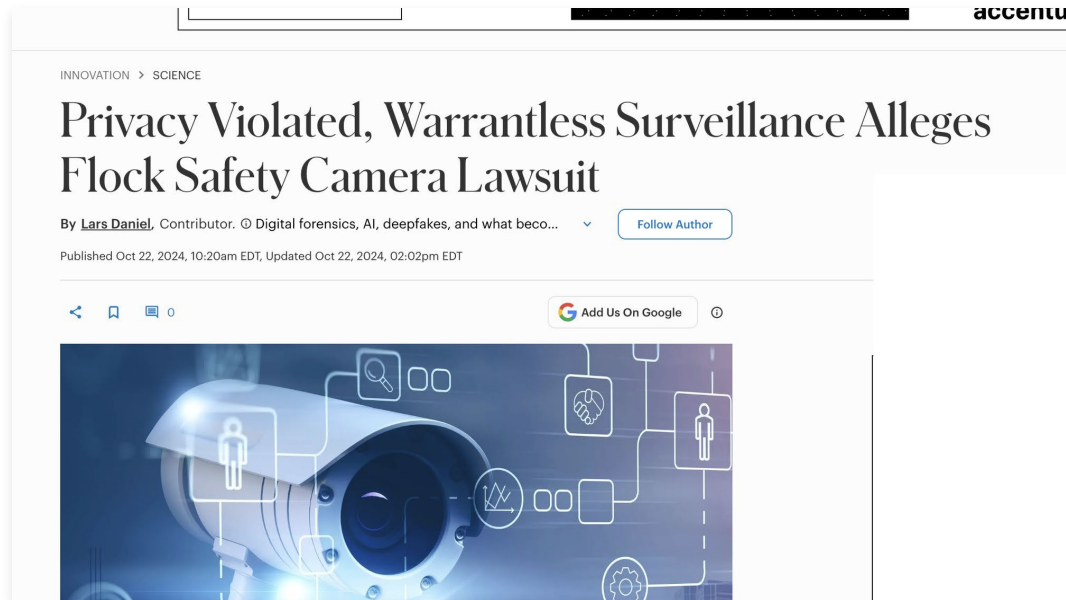
- **One search can sweep the whole country.**

The networks connect to each other. A single officer at a single desk can reach thousands of camera networks across the country with one query.

- **Nobody in the database is a suspect. Everybody is in it.**

This is ambient surveillance of ordinary driving. Your client is in the database right now. So are you, and so is the judge who will hear the motion.

I have been writing this down for a while



Flock's response, printed in my October 2024 column: there is no reasonable expectation of privacy in a license plate on a public road, and photographing one is not a Fourth Amendment search. The doctrine is moving against it.

Lars Daniel, Forbes, Oct. 22, 2024 and Nov. 26, 2024. The Flock statement appears in the October piece.

EDITORS' PICK | INNOVATION > SCIENCE

Woman Wrongfully Jailed 5 Months After AI Facial Recognition Error

By [Lars Daniel](#), Contributor. © Digital forensics, AI, deepfakes, and what beco...

Follow Author

Published Apr 01, 2026, 12:58pm EDT, Updated Apr 03, 2026, 04:22pm EDT

Add Us On Google

This voice experience is generated by AI. [Learn more.](#)

CAM 3.17/w5



CAM 4.17/w5



General

Lightbox

History

Library

Search

Network

Workspaces

History

Project

Address

Unlinked

Jailed more than five months on a facial recognition match. The charges fell apart in minutes.

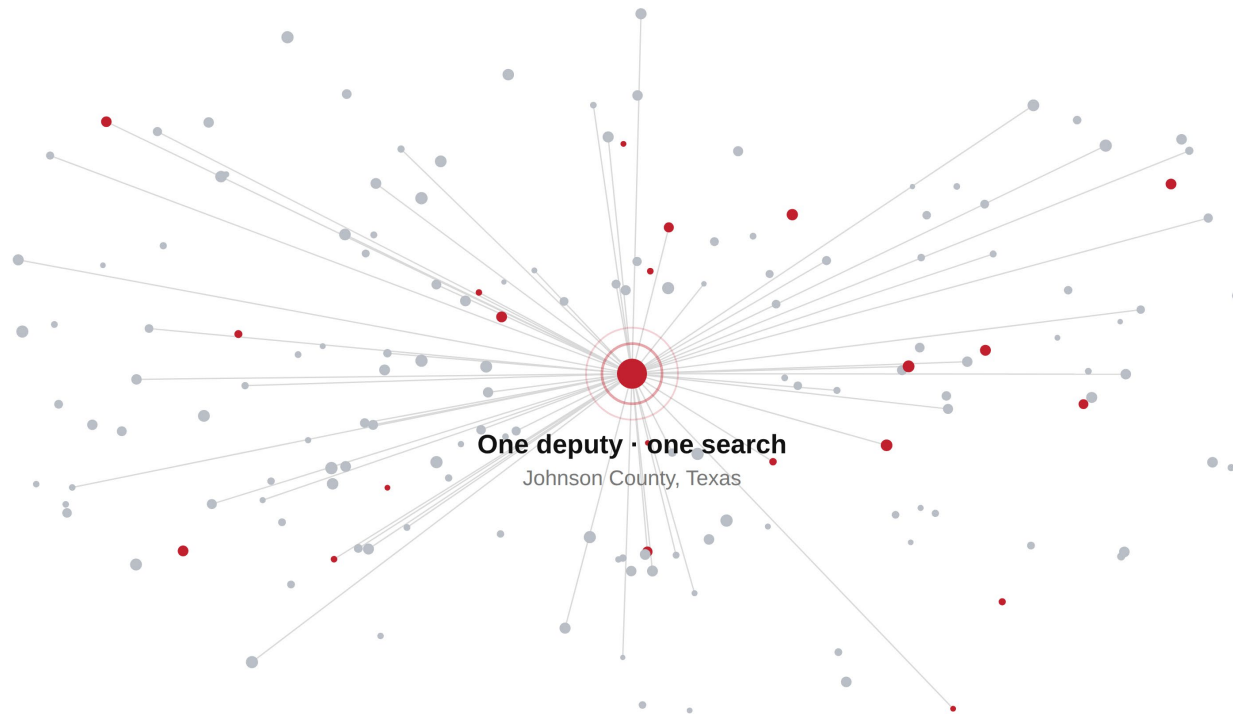
 RIMKUS

THE ABUSE RECORD

None of what follows is hypothetical.
All of it was found in the system's own logs.

Documented by journalists, auditors, and courts. The same logs exist in your cases.

83,345 cameras across 6,809 networks



The reason the deputy typed into the log:

“had an abortion, search for female”

The sheriff and Flock later described it as a missing person case. Court records said otherwise. The typed reason survived because the log cannot be edited after the fact.

Rogue officers on a nationwide network



- **Milwaukee: 170 searches on one woman in two months.**

Officer Josue Ayala used the network to track a woman he dated, and her ex boyfriend. One officer, one hundred seventy queries.

- **Wisconsin, Georgia, Florida: exes, girlfriends, stalking arrests.**

Five unauthorized searches on an ex in Menasha. A police chief arrested for stalking in Braselton. An officer arrested for tracking his girlfriend in Orange City.

- **The Washington Post count: at least 50 officers.**

Charged with or accused of misusing these camera systems, coast to coast. Every case here was proven from the system's own audit logs.

Every one of these cases was proven from the audit logs.

The Marshall Project, Mar. 7, 2026. The Washington Post, Aug. 2, 2026. Arrest records per public reporting.

WHAT THE COVERAGE SAYS, WORD FOR WORD



- *“The problem with 20 billion plates a month is this: cops have access to these records... They’ve been abusing access to databases like these for years to stalk exes, pursue sexual conquests, and harass protesters and critics.”*
- *“What has been implemented by Flock to date has almost exclusively been tools and guardrails law enforcement agencies can opt in to. None of this is on by default.”*
- **One officer looked up a woman and her teenage daughter about 600 times over eight months. Another drew a \$618 fine for 69 unauthorized searches. That is about nine dollars per illegal search.**

Techdirt, Aug. 10, 2026, quoted verbatim. Kechi, Kansas sentencing per The Wichita Eagle: Lt. Victor Heiar, who told his estranged wife, you were spotted.

Watch the reporting for yourself



CNN's segment on growing police misuse of Flock's license plate reader cameras: the scope of the network, the documented misuse cases, and the company's response, reported on national television.

Embedded 95 second excerpt. Plays in the slide.

CNN, via the network's posted segment. Full version linked in the handout.

Local cameras, federal purposes, no process

- **The typed reason fields said ICE.**

Reporters pulled audit logs and found local police running Flock searches with reasons that said ICE or immigration. Federal enforcement moved through local cameras and local officers, without federal process.

- **Illinois audited and found violations of state law.**

The Secretary of State's audit found a federal border agency with pilot access it should not have had, and out of state agencies running immigration and abortion related searches through Illinois cameras, against Illinois law.

- **Flock's own chief executive conceded the compliance architecture did not exist.**

When the auditors pressed, the company's own leadership admitted the controls were not built. Those are his words in the record, not mine.

- **Sanctuary policies can leak through the cameras.**

If you practice in a sanctuary jurisdiction, the sharing your city voted to ban may be happening anyway through the network. The sharing configuration is discoverable, and it is worth demanding.

The error arrives at gunpoint

- **27 documented wrongful stops. About two thirds at gunpoint.**

The Institute for Justice went looking and documented twenty seven wrongful stops built on plate reader errors since 2018. Most of them were felony stops, guns drawn, for database mistakes.

- **Sherwood, Arkansas: one misread digit.**

The camera misread a single character, and a couple ended up on the ground at gunpoint with their six week old in the back seat.

- **San Diego: the wrong red Alfa Romeo.**

This one was not even a plate misread. Flock's vehicle signature feature matches cars by appearance, a machine learning guess about what the car looks like. It matched the wrong car, and a passenger spent about a month in jail over the holidays.

- **I am not aware of any published validation or error rate for vehicle signature matching.**

As an examiner, that absence matters. A match type with no published error rate is an opinion wearing a uniform, and it comes back in the cross examination.

These stops have names attached

Brittney Gilliam, Aurora, CO, 2020

Four girls, ages six to seventeen, handcuffed face down at gunpoint. The reader matched their SUV to a stolen motorcycle from Montana. The city settled for 1.9 million dollars.

Denise Green, San Francisco

Ordered out at gunpoint and made to kneel. The reader turned a three into a seven. She settled for 495,000 dollars.

Jason Burkleo, Atherton, CA

Ordered onto his stomach at gunpoint. The reader turned an H into an M.

Jaclynn Gonzales, Espanola, NM

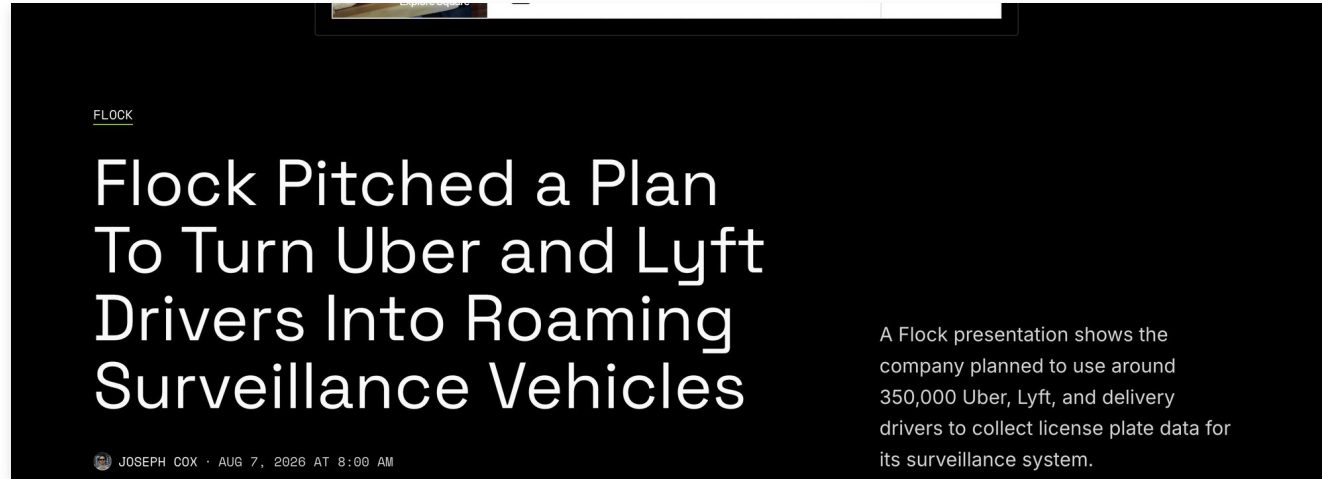
Held at gunpoint, and her twelve year old sister was put in the back of a patrol car. The reader turned a two into a seven.

Brian Hofer, 2019

Detained with his brother on Thanksgiving. The car had been stolen, recovered, and never cleared from the hotlist. Settled for 49,500 dollars.

Isoke Robinson, Detroit

Handcuffed while her two year old son sat in a patrol car. Her car was impounded for three weeks over a vehicle type match.



- Person level search products are being layered on top of the plate network.
- The cameras spread to HOAs, retailers, malls, and now gun ranges.
- The House Oversight Committee opened an investigation. The ACLU published Privacy for Profits in July 2026.

"A Flock presentation shows the company planned to use around 350,000 Uber, Lyft, and delivery drivers to collect license plate data for its surveillance system."

Flock employees watched a children's gymnastics room to make a sales pitch

- **Flock employees opened cameras inside a children's gymnastics room.**

In Dunwoody, Georgia, company staff accessed the city's cameras inside a children's gymnastics room at the Marcus Jewish Community Center of Atlanta, plus a pool, a playground, and a school, and used the live views as sales demonstrations for other police departments.

Flock's blog: "Although the camera was only viewed during a routine demo, we understand that this is a sensitive location."

A Flock spokesperson: "No one is spying on children in parks."

- **The city renewed the contract anyway.**

Flock's concession was that future demos would use, in its words, more public locations, like retail parking lots. When the government says this system is tightly controlled, remember that the vendor's own sales staff could open a camera inside a children's gym.

Two years, seven independent sources

2024, Forbes	A federal lawsuit alleges warrantless surveillance by the Flock network. My column, October 22.
2025, 404 Media	A Texas deputy searches 83,345 cameras for a woman who had an abortion.
2025, 404 Media	Local police run Flock lookups for ICE. The reason fields say so.
2025, Illinois SOS	The state audit finds violations of Illinois law and access that should not have existed.
2026, Marshall Project	Rogue officers coast to coast. One ran 170 searches on a woman he dated.
2026, Washington Post	At least 50 officers charged with or accused of misusing camera systems.
2026, Wichita Eagle	A Kansas lieutenant is sentenced for stalking his estranged wife through police cameras.
2026, Inst. for Justice	27 documented wrongful stops, about two thirds at gunpoint.
2026, 404 Media	Flock pitches 350,000 rideshare cars as roaming plate scanners.

Full ledger with links in the companion handout. Every row is independently sourced.

Every abuse on that ledger was discovered the same way.

Someone read the logs.

Flock's own spokesperson: "Audit logs represent a key accountability feature, because they can't be changed after the fact."

The vendor has already vouched for the records you are about to request.

What to request about your client

- Produce a complete export of the Flock audit log for every search that returned the defendant's license plate or vehicle, including the date and time of each search, the name and agency of the user who ran it, the stated reason entered at the time of the search, and the networks and camera counts included in its scope.
- Produce every detection image of the defendant's vehicle relied on in this investigation, including the full frame photograph, the plate crop, the read confidence, and any vehicle signature attributes the system assigned.
- Produce the complete hotlist history for the defendant's plate, including who entered it, when, on what stated basis, and every later update or removal.
- Produce any analytics the system generated about the vehicle, including travel patterns, frequent locations, and convoy or association analysis.
- Produce the retention schedule and any deletion records that apply to these detections.

Bullet form here. The companion handout carries this as numbered requests with definitions.

What to request about the system and the officers

- Produce every Flock search run by each officer involved in this investigation during the ninety days surrounding the stop or arrest, including every query and every stated reason. The abuse cases were all proven from exactly this kind of pattern evidence.
- Produce the agency's policies and standard operating procedures for license plate reader use, all training records for the officers involved, and the roster of personnel authorized to run searches.
- Produce the network sharing configuration, including which outside agencies and which private networks, such as HOA, retail, and gun range cameras, feed data into or receive data from the agency's system, together with the written sharing agreements.
- Produce the agency's contract with Flock, the applicable terms of service, and any correspondence with Flock concerning this case.
- Produce any error reports, misread reports, or internal audits of system misuse conducted in the last three years.

The ninety day window is a starting point. Adjust to the facts of the case.

The requests that usually go unmade

- State whether any person level search, people lookup, or vehicle association product offered by the vendor was used in connection with the defendant, any witness, or any vehicle in this case, and produce the queries and results.
- Produce records of every non law enforcement access to the relevant cameras or detections, including access by vendor employees for demonstrations, testing, or support, and state whether such access is logged.
- Produce the camera placement map and coverage area for every camera that produced a detection in this case, together with maintenance records and any misread or calibration reports for those cameras.
- State whether any search relevant to this case was run through a mobile application or a personal device, and produce those access logs.
- **Produce all detections of the defendant's vehicle during the charged period, including detections inconsistent with the government's theory of the defendant's movements.**

The last request is the exculpatory one. The network that tracked your client can also alibi your client.

What the logs can show

- A stated reason that does not match the case timeline points you to the lead's true origin. That is the foundation for a Franks challenge, and it is how parallel construction gets proven.
- Searches on your client that predate any documented suspicion mean the investigation started somewhere the report does not say.
- An officer's unrelated searches, the ex girlfriends and the neighbors and the celebrities, are impeachment material that arrives ready made from the record.
- Agency wide reason fields that say ICE, or that say nothing at all, undercut any testimony that this is a trusted and well governed tool.
- **And sometimes the most useful entry is the blank one. An unexplained nationwide search of your client is its own exhibit.**

How was it used?

- What reason did you type into the system when you searched this plate? Is that reason accurate?
- How many cameras, and how many other agencies' networks, did that one search reach?
- Who placed my client's plate on the hotlist? When? Based on what information?
- Before the stop, what did you do to confirm the camera's read against the actual plate on the actual car?
- When was the hotlist entry last verified against the underlying database?
- Where does your report say this investigation began? Where does the search log say it began?

Each question is keyed to a field in the audit log export. Ask what the record can contradict.

Can it be trusted?

- How many Flock searches did you personally run last month? On which cases?
- What training have you received on this system? Who else in your department can run searches?
- What is the system's error rate for plate reads? What is its error rate for vehicle signature matches?
- Whose camera captured this detection? The city's, an HOA's, a business's? Under what written agreement?
- Has your department ever audited these logs for misuse? Would your own search history survive that audit?
- The log says the reason for this search was one thing. You have testified to another. Which one is false?

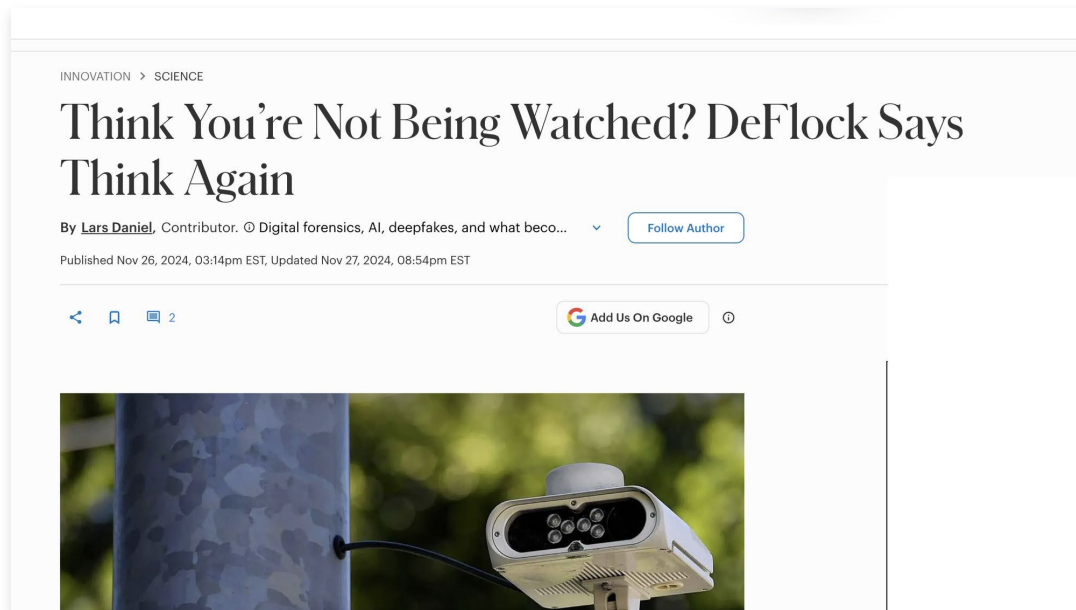
Pair with the Institute for Justice study and the misuse record for foundation.

Access, absence, and the questions nobody expects

- Who, besides law enforcement, can view these cameras? Has the vendor's own staff ever accessed them? Would you know?
- Has any agency outside this jurisdiction ever searched for my client's plate? Have you checked?
- Can you tell this jury every person who has viewed the detections of my client's vehicle in this case?
- Did the network capture my client's plate anywhere else during the charged period? Did you look?
- When a search returns nothing, is that logged? Did any search for my client's vehicle come back empty?
- Did you run any of these searches from the mobile app? On whose phone?

The absence questions matter as much as the presence questions. A dragnet that did not see your client is evidence too.

Know where the cameras are



- DeFlock, at deflock.me, is a crowdsourced map of license plate reader locations. Check your client's alleged route against real camera positions before you accept the government's version of where the car was seen.
- **Have I Been Flocked, at haveibeenflocked.com, searches published Flock audit logs and shows whether a plate has been searched, by which agency, and when. Run your client's plate before you accept the government's story.**
- The EFF's Atlas of Surveillance shows what your jurisdiction owns. The ACLU and the Institute for Justice carry the policy record and the litigation, including the Norfolk appeal in this circuit. DeFlock also keeps the scoreboard of communities that dropped the cameras: 95 in late July.



Scan now: haveibeenflocked.com

deflock.me. haveibeenflocked.com. eff.org. aclu.org. ij.org. My DeFlock column: Forbes, Nov. 26, 2024. CBS News on Have I Been Flocked, Aug. 2026.

Ninety five communities and counting

- **47 cancelled. 25 rejected. 22 deactivated. 1 ban.**

Ninety five communities have now pushed the cameras out or kept them out, per DeFlock's running tally. The outright ban is Ypsilanti, Michigan.

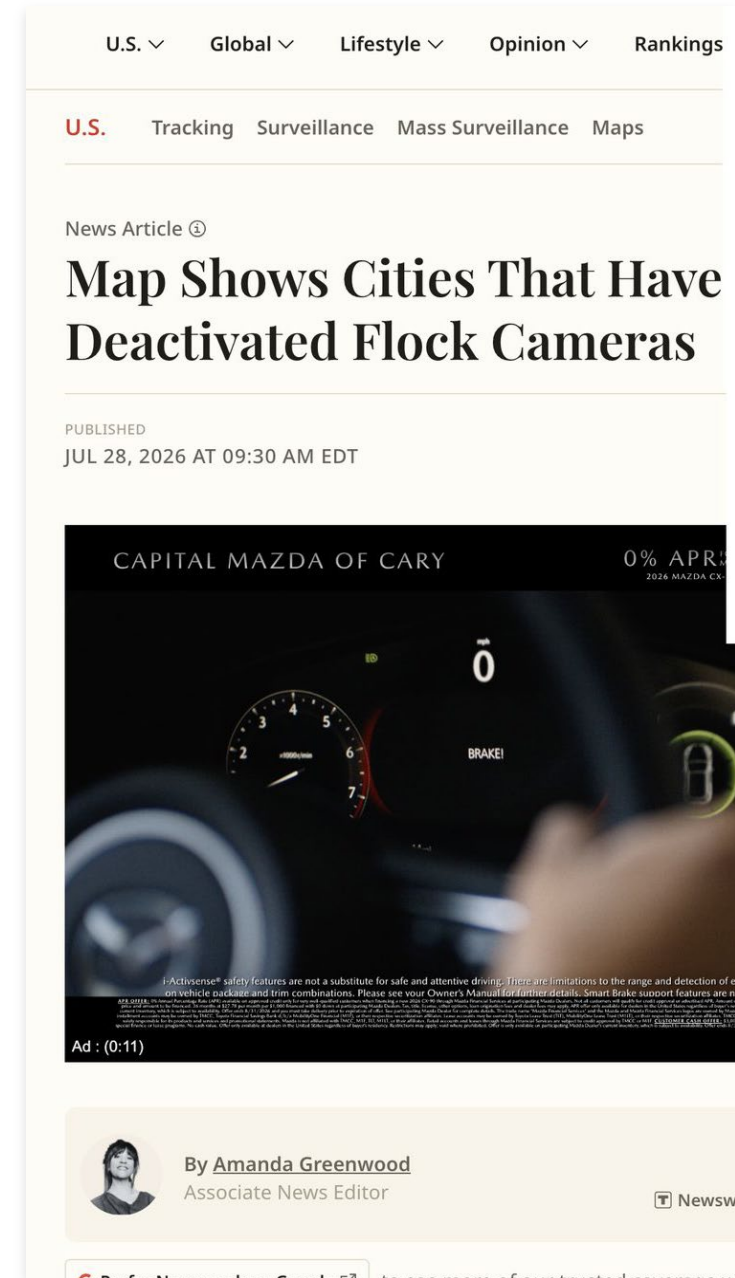
El Cerrito's mayor pro tem: "Ultimately my biggest concern is the federal government could access the data."

Appleton's mayor: system integrity concerns "have eroded our trust."

- **Austin organizers forced a cancellation.**

These are elected officials and organized residents reading the same abuse record you just saw, and reaching the same conclusion.

Newsweek, July 28, 2026, quotes verbatim, tally per DeFlock. Austin coverage, 2025 to 2026.



Virginia is pushing back, town by town

- **Five Virginia localities have dropped the cameras in nine months.**

Staunton took its cameras offline in December. Charlottesville voted to end its contract the same month. Harrisonburg ended its contract in July, Elkton voted unanimously to cut ties after residents organized, and Floyd County's cameras deactivate when its contract expires in August.

- **About 3,000 Flock cameras remain, across more than 150 Virginia localities.**

The dragnet is still the default. The exits are still the exception, and the network your client drove past is probably intact.

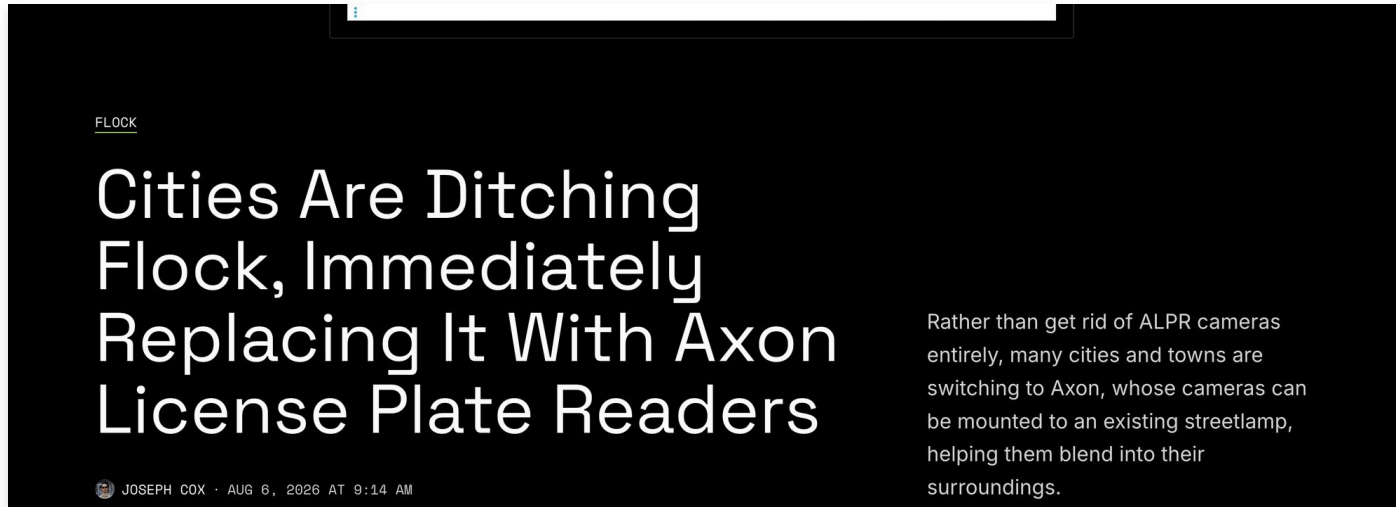
Melissa Corrigan, a veteran, to VCIJ: "This is technology that we saw being developed in the Middle East when we were over there, and now they're using it on us."

- **Virginia's 2025 ALPR law requires federal agencies to get a search warrant for this data.**

My understanding, and your judgment controls: when Flock returns from Virginia cameras appear in a federal case, ask how the data crossed from the local network into federal hands, and under what authority. If the answer is a shared login, the statute has something to say about it.



The cameras come down. The dragnet stays.



"Rather than get rid of ALPR cameras entirely, many cities and towns are switching to Axon, whose cameras can be mounted to an existing streetlamp, helping them blend into their surroundings."

- **One vendor now holds the whole evidence pipeline.**

Cities dropping Flock are switching to Axon, whose cameras mount on existing streetlights and blend in. Axon also sells the body cameras, the AI report writer, and the fusion platform, so the same company now touches nearly every piece of evidence in the case.

- **Your discovery request survives the rebrand.**

The fix that lasts is policy: retention limits, audit log access, and sharing bans that bind whoever owns the cameras. Change the vendor name in the caption and serve the same requests.

DEMAND THE RECORD. *The dragnet will change vendors. The audit log demand goes with it.*

404 Media, Aug. 6, 2026, quoted verbatim: Cities Are Ditching Flock, Immediately Replacing It With Axon License Plate Readers.

PART TWO OF FIVE

The report wrote itself

Axon's Draft One drafts the official narrative from body camera audio. The officer edits and certifies it. Then the original draft is destroyed.

02

Infrastructure already, and growing

- **600 departments. 600,000 reports.**

Draft One listens to the body camera audio and a language model writes the police narrative. It sells for about 199 dollars per officer per month and arrives bundled inside body camera contract renewals, which means departments adopt it as a line item, without a validation study.

- **Axon booked about 750 million dollars on its AI line.**

Report writing is the growth product. Some of those six hundred thousand reports are sitting in discovery folders in this room, marked or unmarked.

- **The officer edits and certifies the machine's draft.**

The machine drafts, the human signs. That certification is where your cross examination begins, because it is the only human commitment in the whole pipeline.

“We don’t store the original draft and that’s by design... the last thing we want to do is create more disclosure headaches for our customers.”

An Axon senior product manager, on video, reported by the EFF in July 2025.

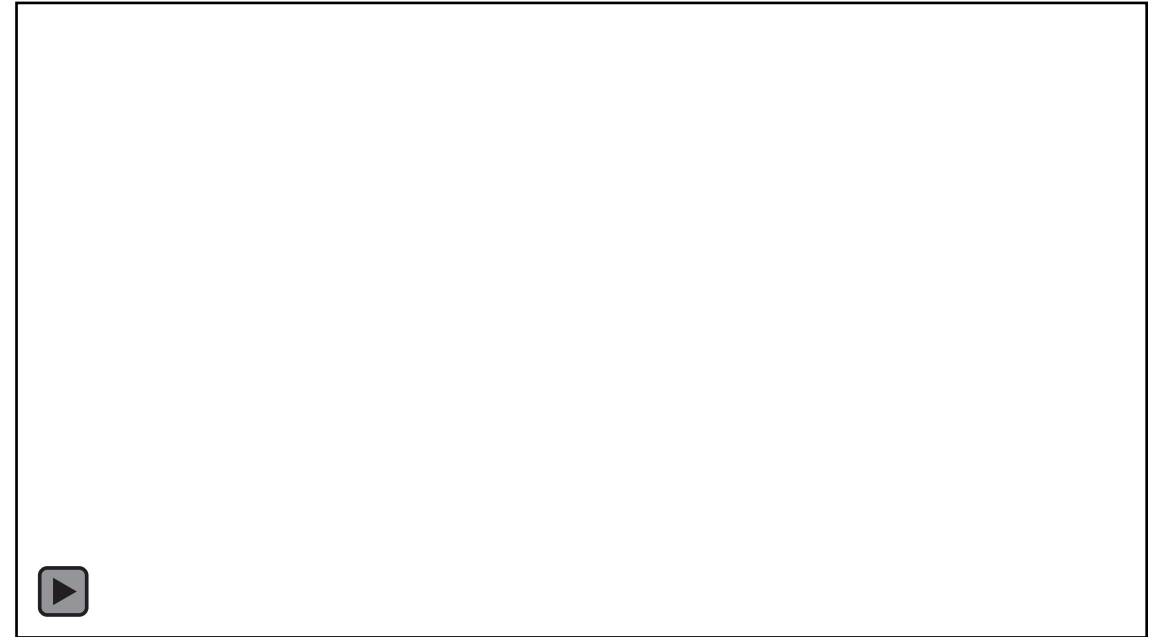
An honest mistake and a fabrication now look identical

- **No record survives of machine text versus human edits.**

When a report turns out to contain a false statement, the one document that would tell you whether it was an honest mistake, a machine hallucination, or a deliberate fabrication is the original draft. That draft is destroyed at export, on purpose, as a feature.

- **The news is covering it.**

This segment runs about two minutes and puts the question in plain language: who actually wrote this report? It is a fair introduction for a judge who has never heard of the product.



Embedded segment, about two minutes. Plays in the slide.

Pulled from agencies' own files, July 2026

- **Officers who were only on the radio appear in reports as on scene.**

A King County prosecutor reviewing these reports found the AI placing officers at scenes they never visited. A witness list built from that report starts wrong, and the error surfaces on the stand, where it reads as dishonesty.

- **Wrong names and wrong plates in final reports.**

Officers described fixing so many errors that a thirty second entry took three minutes, and the mistakes appeared even where the body camera audio was perfectly clear.

- **A teenager typed a SpongeBob quote. The AI report flagged him for pattern tracking.**

Richmond, California. A student typed the cartoon's line, Gary, there is a bomb strapped to my chest. A classmate reported it, the responding officer confirmed it was a harmless joke, and the AI written report still logged the incident as retained for future pattern tracking. A cleared misunderstanding became a standing surveillance entry on a minor.

- **Axon solicited promotional quotes mid pilot.**

While agencies were still supposedly evaluating the product, the vendor was collecting marketing endorsements from them. The evaluation and the marketing were the same event.

The report said the officer turned into a frog

- **Draft One heard a Disney movie and wrote it into the report.**

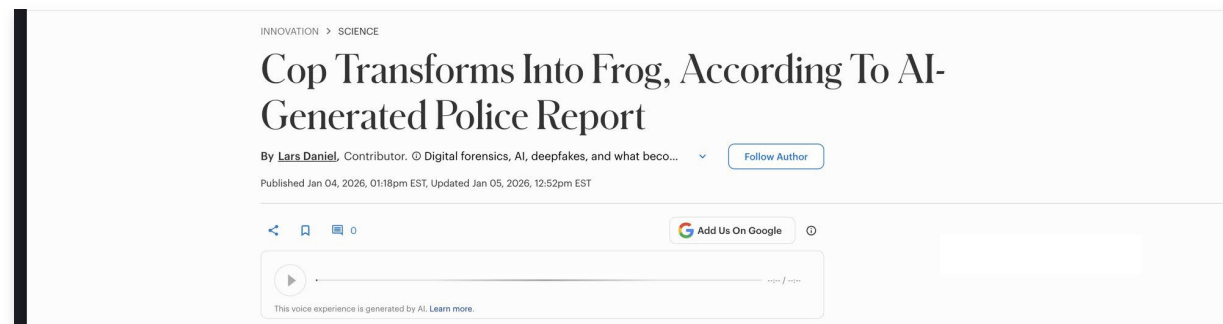
Heber City, Utah. The Princess and the Frog was playing in the background, the tool folded the audio into the narrative, and the police report said the officer shape shifted into a frog.

- **It was caught because TV cameras were in the room.**

The department happened to be demonstrating the product for local television, and a man turning into a frog is hard to miss. A sergeant there says the tool saves him six to eight hours a week, and that is the real trade: hours saved against errors that only get caught when they are absurd.

- **The absurd error gets caught. The subtle one gets sworn.**

A wrong street name does not announce itself. A smoothed over uncertainty does not announce itself. An officer placed at a scene he never visited does not announce itself. After the draft is destroyed, nothing separates those errors from what the officer actually saw.



My column: Forbes, Jan. 4, 2026. The time estimate is Sgt. Rick Keel's, per the same reporting.



No time saved, and the scope is creeping

- **The only randomized study found no time savings.**

Manchester, New Hampshire ran the one controlled test, and it found no measurable time saved. About half the officers believed it saved them time anyway, which tells you how closely they were checking. Manchester and Anchorage both dropped the product.

- **Policies say minor incidents only. Utah says otherwise.**

One Utah department produced more than 900 AI reports, including kidnapping and assault cases. The scope creeps because nothing in the tool stops it.

- **The AI disclosure footer is a setting, and departments turn it off.**

Lafayette, Indiana and Fort Collins, Colorado disabled the one line that tells a reader a machine drafted the report. Police chiefs cannot tell you which of their own reports the machine wrote, which means the prosecutor cannot tell, and neither can you, unless you demand the usage records.

No court has litigated an AI drafted report yet

- **King County prosecutors banned AI drafted reports.**

Their stated reason was blunt: they could not vouch for the accuracy. That is the government's own lawyer talking about the government's own paperwork.

- **California now requires marking, audit trails, and draft retention.**

SB 524, signed October 2025, requires AI reports to be marked, audit trails kept, and the first draft preserved. The vendor will comply in California, which settles the feasibility argument everywhere. When an agency in your district says the draft cannot be preserved, the answer is that Axon already built that for California.

- **Utah requires disclosure on the face of the report.**

SB 180, with officer certification on top.

- **The first litigated AI report case will come out of a room like this one.**

What to request when a report may be AI drafted

- Send a preservation letter on day one demanding that Axon and the agency preserve the AI draft, the prompts, the audit logs, the Draft One usage data, and the model and version identifiers for every report in the case. Axon has represented that materials exist internally that agencies do not export.
- Request the Draft One audit trail for each report, including who generated the draft, when, from what audio, what edits were made, and who certified the final version.
- Request the agency's Draft One usage records sufficient to identify every report in this case, and every report by the involved officers, that was machine drafted.
- Request the department's Draft One policy, the disclosure footer configuration, and all training records for the involved officers.
- **Where the agency claims the draft no longer exists, request the retention policy and the date and mechanism of destruction, in writing.**

Model the requests on California SB 524. It is the documented, vendor feasible standard.

The certification is the pressure point

- Which sentences in this report did you write, officer?
- What did the machine's draft say before you edited it?
- You certified this report as accurate. What did you compare it against?
- How long did you spend reviewing the draft before you certified it?
- Does this report disclose, anywhere on its face, that a machine drafted it?
- If the draft would show the machine invented that detail, where is the draft?

My understanding as an expert: Smith v. Arizona limits witnesses narrating machine work they did not do, and destroyed drafts raise spoliation questions. Your call to make.

A model cannot be sworn.

It cannot be questioned, and it cannot be held to account.

Six hundred thousand of these reports already exist. Some are in your case files, unmarked. The window to demand the drafts closes at export, every single day.

DEMAND THE RECORD. *The draft, the prompts, the audit trail. The preservation letter goes out on day one.*

PART THREE OF FIVE

Push button forensics

Tools simple enough that pushing a button passes for expertise. That sentence is from my column. The problem is older than AI, and AI makes it worse in a specific way.

03

The field has been warning about this for years

- **The field calls it button pushing.**

Brett Shavers, a former undercover officer turned respected examiner, has spent years writing about it: run the tool, accept the output, call it an examination. That is the discipline's own standing complaint about itself.

- **More than 2,000 agencies own mobile forensic tools.**

Upturn's Mass Extraction study found agencies in all fifty states running tens of thousands of phone extractions, many for minor offenses, with kiosk models pushing the work to patrol officers and written policies rare. Two thousand agencies do not employ two thousand qualified examiners.

- **Challenging the unqualified operator quotes the field's own literature.**

When you challenge the operator in your case, you are never inventing a defense theory. You are reading the field's own warnings back to it, and that is a comfortable place to cross examine from.

Specialist tool, then field tool, then anyone can run it



The error rate surfaces years later, in defense counsel's cases. Every time.

Two dollar drug kits fed tens of thousands of guilty pleas. The Massachusetts breath test scandal put tens of thousands of tests out of evidence. Rapid DNA moved lab science to the booking desk.

The rule of my discipline has never changed.

**The tool's output is where the work starts.
It is never where the work ends.**

Findings get verified against the device and the records around it. AI does not change that rule. It just makes unverified output more fluent.

The AI powered nerve center

- **March 2026: the AI powered nerve center.**

Cellebrite launched Guardian Investigate worldwide and called it exactly that. Agentic AI as a force multiplier. Investigators ask questions of the evidence and the system builds the timelines. Nearly every phrase on this slide is the vendor's own marketing.

- **The pitch is speed around the laboratory.**

Evidence flows in real time instead of waiting for device returns from labs, and intelligence packages come together in hours rather than months. Listen to what is being removed: the laboratory, the examiner, the verification step. Faster is the feature, and the examiner is the delay.

- **7,000 customers. 3 million investigations a year.**

That is the scale this ships into, without a published validation study behind the AI features.

Cellebrite launch release, Mar. 18, 2026, with its Feb. 2025 generative AI assistant announcement. Quoted phrases are the vendor's.

Investigative leads, not conclusions

- **April 2026: Magnet AI.**

Natural language search plus machine generated summaries, with a citation feature. The company's own label is careful: investigative leads, not conclusions, with verification left, in its words, firmly in the hands of human judgment.

- **Credit where due. Hold the company to its own label.**

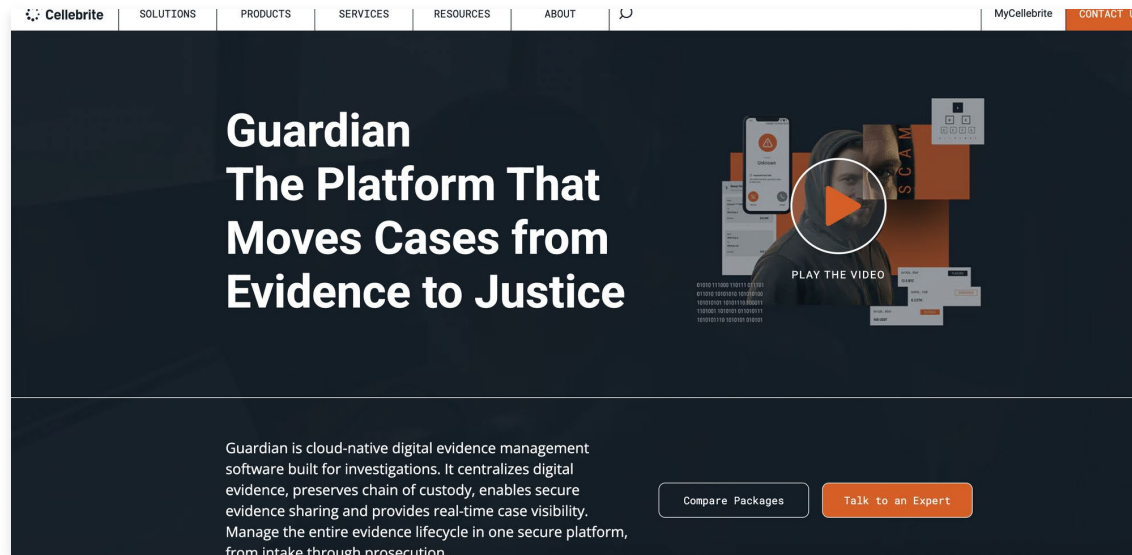
Those are good words, and they are quotable. When a witness swears to a conclusion, the vendor's own language says the tool produces leads. One of them is overselling, and either answer helps you.

- **It ships inside the platform built for people who are not examiners.**

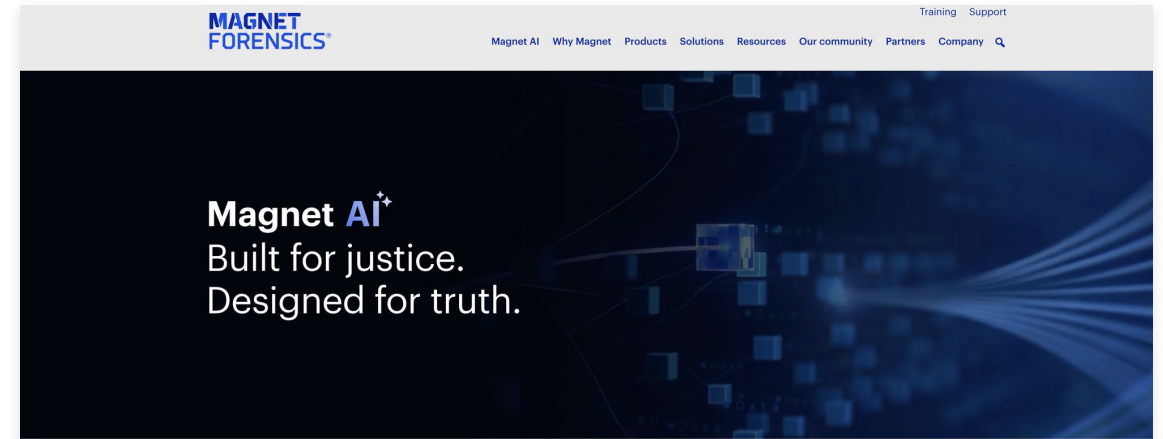
Magnet AI lives in Magnet Review, the product made so detectives, prosecutors, and reviewers can work the evidence without an examiner. And since the Grayshift merger, the same company sells GrayKey, the box that opens the phone, and now the AI that reads what comes out. The full pipeline, one vendor.

Magnet AI announcement, Apr. 21, 2026, Magnet User Summit. Magnet and Grayshift merged in 2023.

What the vendors say the AI can do



Cellebrite: an AI powered nerve center. Ask questions of the evidence.

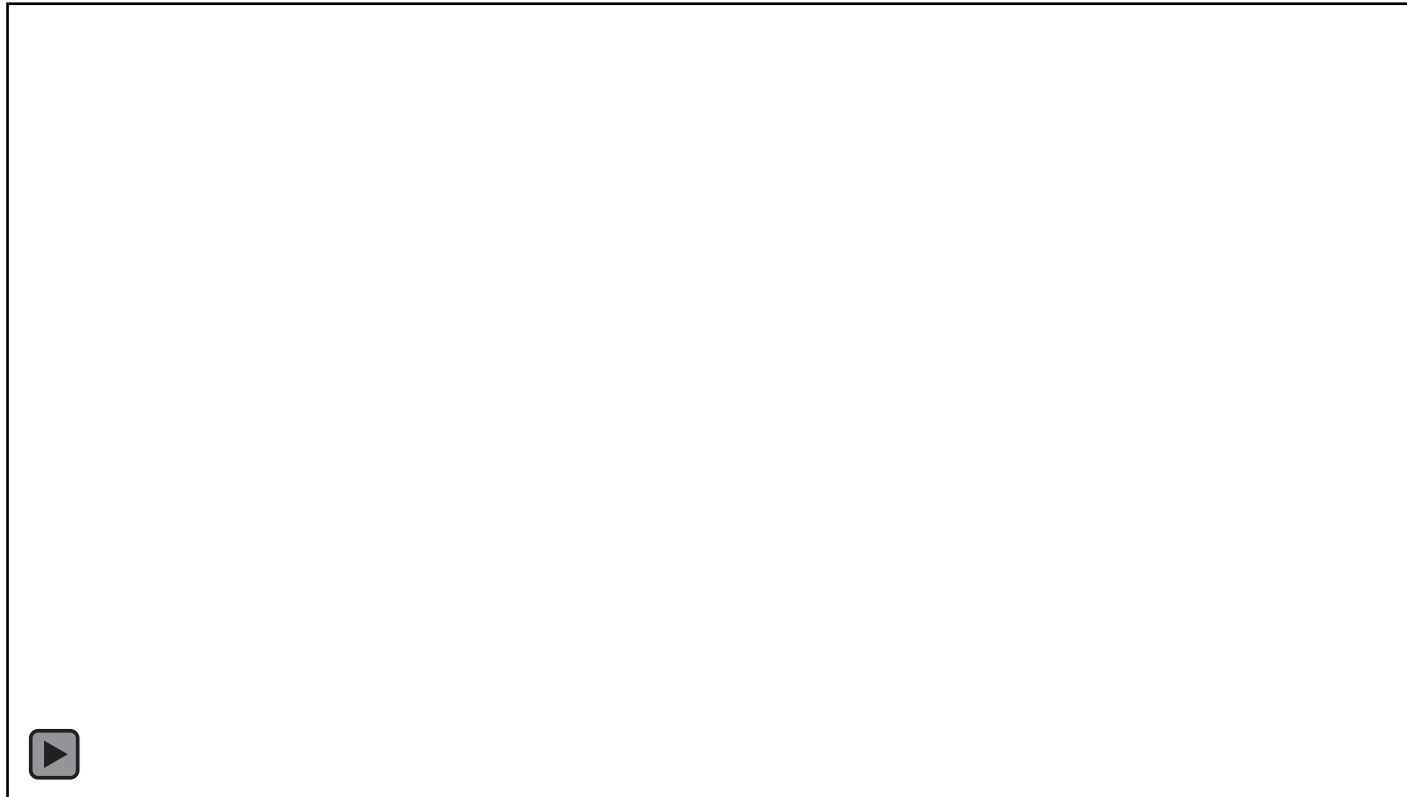


Magnet: natural language search, machine generated summaries, investigative leads.

Save these pages. Whatever the witness says the tool did, the company's own marketing says what it sells.

Cellebrite launch materials, Mar. 2026. Magnet AI announcement, Apr. 2026. Captured from the vendors' own pages.

Cellebrite's own demo: ask, and the timeline builds itself



Cellebrite Guardian promotional demo. About two minutes, embedded.

- **Watch what the demo shows.**

Evidence uploads, an AI chat panel that answers questions, timelines that assemble themselves, suspect movements drawn onto a map, task lists that fill in.

- **Watch what never appears.**

A validation step. An error rate. An examiner checking any of it against the actual device. The workflow makes answers easy and never makes anyone earn one.

Cellebrite Guardian promotional video, published by the vendor.

An expert asked ChatGPT to write his opinion. The prompts surfaced.

- **Watson Grinding, Houston, 2020. Three dead. A 61 million dollar case.**

An explosion killed three people and damaged about two hundred homes. One defendant is 3M, and plaintiffs allege the facility's gas detection system was not properly serviced. An expert witness defending 3M produced a report on the company's standard of care.

His prompts, per the court documents: "create an exceptional expert witness report defending the standard of care at 3M." And: "show how 3M is 0% at fault for the explosion."

- **He handed the machine the conclusion.**

He did not ask what the evidence showed. He typed the verdict into the prompt box and asked the machine to build support for it. The prompts were discoverable, and the deposition went the way you would expect.

- **Expect the police version of this.**

The forensic tools we just walked through invite the same shortcut. An investigator can ask the evidence what happened, or can ask the system for the case against your client. The difference lives in the prompts, and prompts are records. Request them.

Research assistant or opinion writer. Pick one.

- **The right way: AI as a research assistant.**

Use it to search the literature, surface what you might have missed, and pressure test your own reasoning. Then verify every line against the record, because the opinion is yours, and every word of the report has to survive without the machine in the room.

- **The wrong way: AI as the opinion writer.**

Hand it the conclusion and ask it to build the support. That is what the 3M expert did: he typed the verdict into the prompt box, and the machine dressed it up. At that point the tool is leading the expert by the nose.

- **The difference is the direction of the questions.**

Ask what the evidence shows, and the tool serves the expert. Tell it what to prove, and the expert serves the tool.

- **Every prompt is a record of which direction the questions ran.**

How I use these tools in my own practice, and the line an expert cannot cross.

Make them produce the prompts

- State whether any artificial intelligence or generative AI system, including ChatGPT or any AI feature embedded in a forensic or investigative tool, was used in the preparation of any report, analysis, or opinion in this case, and identify each system and version used.
- Produce every prompt, query, or instruction submitted to any such system in connection with this case, together with every output received, including drafts, summaries, timelines, and proposed conclusions.
- Identify which portions of each report or opinion were generated, in whole or in part, by an AI system, and produce the earlier drafts showing what the machine wrote and what the human changed.
- Produce logs, account histories, or usage records sufficient to show when each AI interaction occurred, and state whether any prompts or outputs have been deleted.
- **Where the response is that no prompts were retained, request the date and manner of their deletion, in writing.**

Modeled on the 3M record. The prompts were discoverable there, and they are discoverable here.

Whose opinion is this?

- Did you use any AI tool at any point in forming your opinions or preparing your report?
- Which tool? What did you type into it?
- Did the AI draft any sentence that appears in this report? Which ones?
- What did you ask it to do: analyze the evidence, or support a conclusion you already had?
- Did you keep your prompts? If they are gone, who deleted them, and when?
- What did the AI get wrong, and how would you know?
- **If the AI led and you followed, whose opinion is on the stand?**

A yes opens prompt production. A no is testable against usage records and billing.

If the witness is not a digital forensics expert, challenge them. Every time.

A witness who cannot explain how the tool works has no business swearing to what the tool produced. That was true before AI. It is more urgent now, because the output got more fluent and the operator pool got bigger.

AI did not change the rule. It multiplied the number of witnesses the rule applies to.

The traps an examiner is trained to catch

- **Extraction type is a menu click.**

Logical, file system, and full file system extractions pull very different data from the same phone. Choose wrong and you can miss the deleted messages entirely, or destroy the only chance to collect them, and the operator may not know it was a choice.

- **Time zones convict people.**

The classic conviction grade misread. A timestamp read in the wrong zone puts a person somewhere they never were, at a time that fits the government's story.

- **Cached is not viewed.**

A file existing on a phone and a human being having looked at that file are two different facts. Whole cases live inside that difference.

- **Sync bleed blends people together.**

Account syncing writes one person's activity onto another person's device. A family shares an account and one person's searches surface on everyone's phones. I have worked cases that turned on exactly this, and so has every examiner who does this work.

A finding that cannot be reproduced is not a finding

- **Ask the same model twice, get different answers.**

An AI output is a probability dressed up as an answer, and probability is not proof. A finding another examiner cannot reproduce from the same data is not a finding, and that rule is older than any of these products.

- **The version that generated the lead may not exist at trial.**

The models update quietly under the hood. By the time you litigate, the exact tool that produced the lead may be gone, which leaves nothing to validate and nothing to reproduce.

- **Rule 702 puts the reliability burden on the proponent.**

My understanding as someone who testifies under it: since the 2023 amendment, the party offering the expert must show a reliable method, reliably applied to this evidence. A tool that cannot repeat itself, run by an operator who cannot explain it, struggles with both halves of that sentence.

Quoted lines from my column, Forbes, Aug. 12, 2026. Fed. R. Evid. 702, as amended in 2023.

Ask the practitioners. Then look at who was asked.

- **Magnet and Brett Shavers are surveying where digital investigations break down.**

Credit where due. They are asking the people who do the work before the product roadmap hardens, and that is the right order of operations. It is rare enough that I wrote a Forbes column saying so.

- **Read the survey population.**

Law enforcement leaders, examiners, investigators, and prosecutors. No defenders. No defense experts. The half of the adversarial system whose job is testing these findings in court was not asked where they break.

- **Watch for the survey results.**

When the results publish, they will be a map of where digital examinations break down, written by the people who run them. Read it like a deposition outline. Every failure point the field admits to is a question you get to ask in your next case.

- **You are the room where these tools get tested.**

Nobody at that table pictures you as part of the quality control system. You are the quality control system, and the testing only happens if you do it.

What to request when AI touched the examination

- Identify the forensic tools used in this case, including the exact software version and configuration, and state which AI features were enabled during acquisition, processing, or review.
- Produce every AI generated summary, insight, ranked lead, and timeline created in connection with this case, together with every prompt or question an operator typed into the tool. These exist as records inside the platforms, including citation logs and dashboards.
- Identify the extraction type performed on each device, who selected it, and why. Produce the operator's activity log showing what was actually done, in what order.
- Produce all validation materials for the AI features relied on, including error rates and the agency's standard operating procedures. Produce the training records and certifications of each operator.
- **Preserve and produce a forensic image sufficient for independent re-examination by a defense expert.**

The re-examination request is the reproducibility rule turned into a demand. Same data, independent examiner.

Did the human do the work, or push the button?

- Which of these findings did you reach yourself, and which did the software suggest to you?
- What did you verify against the device itself, without the tool?
- If your colleague ran the same analysis tomorrow, would it produce the same result?
- What training do you have in digital forensics, apart from the vendor's course on operating this tool?
- What extraction type did you choose, and why that one?
- What did you ask the tool for? Produce every prompt you typed.
- **The vendor describes these outputs as investigative leads, not conclusions. You swore to a conclusion. Which is it?**

A vendor certificate is not a discipline. Operating the tool is not understanding the tool.

The software takes no oath.

Every machine generated lead ends the same way: a human raises a right hand and swears to findings someone's life turns on. The question in every case is whether that human did the work.

The tools are already in seven thousand agencies. The validation studies do not exist yet. The people testing these findings in the meantime are the people in this room.

DEMAND THE RECORD. *The tool, the version, the AI features, and an image for re-examination.*

PART FOUR OF FIVE

No warrant. We bought it.

Mobile advertising IDs turn every free app into a location beacon. Law enforcement buys the data instead of getting a warrant. You have seen this play before, with cell site simulators.

04

Every free app is a location beacon with a name

- **Every phone carries an advertising ID.**

It is a durable identifier that exists so the ad industry can recognize your device. It is the name your phone answers to in the advertising economy.

- **Free apps broadcast it thousands of times a day.**

Every free app pushes that ID into advertising auctions, with your precise location attached. That is how a free flashlight app pays its bills.

- **Brokers reassemble the exhaust into a life.**

Data brokers sit under the auctions, collect the exhaust, and rebuild it into a device history: where the phone sleeps, where it works, where it worships, where it parks.

- **Law enforcement subscribes. No warrant.**

Resellers package the histories and agencies subscribe. The government's position is that no warrant is needed because the data is, quote, commercially available.

- **You can spot the shape in discovery.**

A suspiciously precise location fix with no warrant return behind it, no carrier records, and no named source. When you see that shape, you are probably looking at bought data.

The cell site simulator playbook

- **Stingrays forced phones to reveal themselves. The paperwork said otherwise.**

A cell site simulator impersonates a tower and makes every nearby phone check in. Police used them for years without warrants, while reports credited the location to other sources.

- **Baltimore: about 4,300 uses, almost none disclosed to courts.**

A detective testified to the number under oath. Thousands of deployments, and the courts hearing those cases almost never knew.

- **Agencies signed FBI nondisclosure agreements.**

The concealment was contractual. Reporting documented prosecutors dropping cases and cutting charges rather than reveal the tool in a courtroom. The government walked away from convictions to keep a surveillance method secret.

- **The paper trail was built so courts would never see it.**

It took defense lawyers years of refusing to accept location evidence with no explained origin to drag it into the light. Remember the method, because it works again.

MAIDs are the same play with better cover

- **Fog Reveal: about 7,500 dollars a year.**

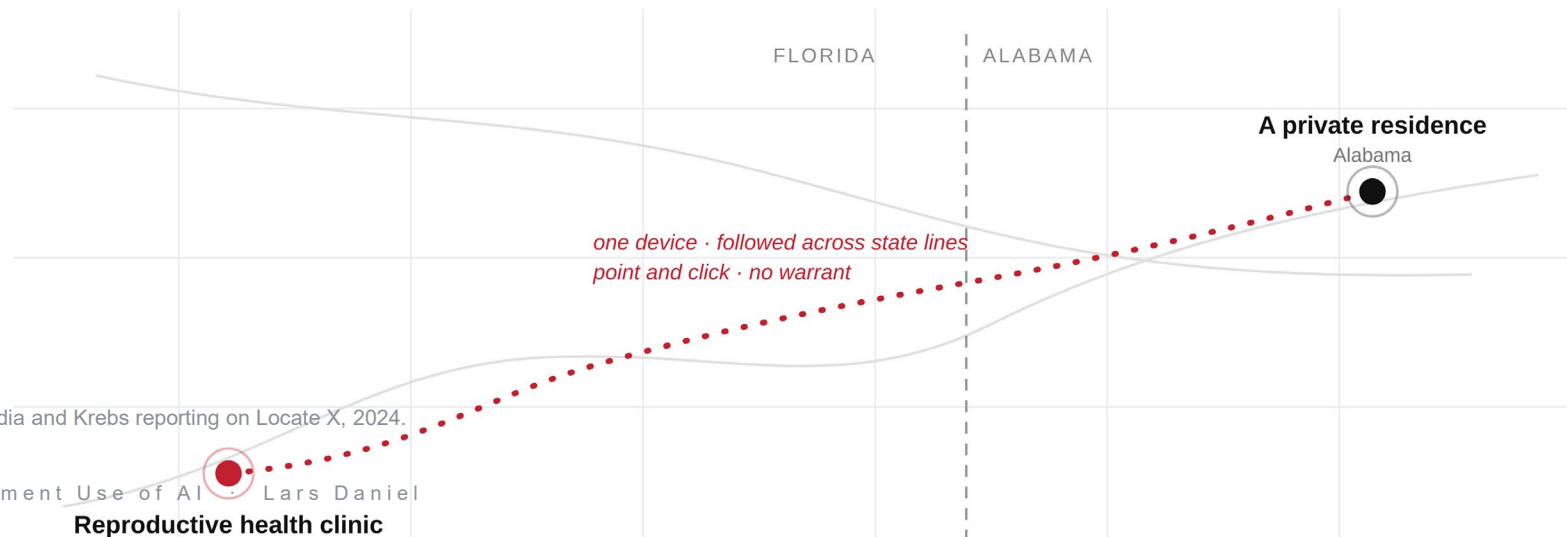
A commercial subscription that maps phone locations from advertising data, stingray capability at small town prices. The AP investigated and found its use rarely, if ever, appears in warrant applications, and officers were coached to call it, simply, a law enforcement database.

- **Locate X tracked a phone from a Florida clinic to an Alabama home.**

In a sales demonstration, Babel Street's tool followed a device from a reproductive health clinic across state lines to a house. Point and click, no warrant. And the contract language reportedly forbids disclosing the tool in legal proceedings, which means the secrecy now ships inside the license.

- **A stingray needed a van. This is a browser tab.**

The concealment moved from an FBI nondisclosure agreement to a commercial license, and the reach went from one neighborhood to the whole country. Same play, better cover.



AP investigation of Fog Reveal. 404 Media and Krebs reporting on Locate X, 2024.

After the geofence ruling

- **Chatrie: a geofence is a search.**

In June the Supreme Court held that acquiring location history through a geofence is a Fourth Amendment search. It closed the two escape hatches: short duration is no defense, and clicking allow in an app is not consent to police acquisition. My understanding as an examiner, and your judgment controls: getting this data from a provider now generally requires a warrant.

- **The Court reserved tower dumps, keyword warrants, and bought data.**

Those questions were left open on purpose, and the surveillance market read the reserved list as a product roadmap. When the front door acquired a warrant requirement, the government went shopping at the side doors.

- **The market moved immediately.**

A tower dump in Nevada swept 1,686 phones from a single tower, and the court called it an unconstitutional general search, saved only by good faith. ICE bought Penlink's Webloc, commercial geofencing built on advertising data, for about five million dollars. Preserve the purchased data question in every one of these cases, because it is the next fight.

Quote the FTC back to the prosecution

- **The FTC already condemned this data.**

The Federal Trade Commission brought enforcement actions against the location brokers themselves, Gravy Analytics, Venntel, and Mobilewalla, finding the data was collected without meaningful consent, including from sensitive places like health clinics and churches.

- **Commercially available? The government's own agency found the commerce unlawful.**

When the prosecution calls this commercially available data, quote the FTC back to them. The federal government's own consumer protection agency found the commerce itself was illegal.

- **A MAID is not a person.**

Devices get shared. Advertising IDs get reset. Locations get spoofed, and ad fraud pollutes the stream badly. Tying an advertising ID to a specific human being at a specific moment is expert work, and the error sources are documented in the industry's own literature. If the government's case leans on a MAID trail, that trail can be examined, and it should be.

Name the tools, then demand the origin

- State whether any of the following were used in this investigation: Fog Reveal, Locate X, Webloc, Tangles, or any commercial telemetry, advertising intelligence, or data broker service. Generic requests miss laundered leads. The euphemisms are the point, so name the products.
- For each use, produce the queries run, the date ranges, the geographic areas drawn, the results returned, and the subscription or license agreement under which the tool was accessed.
- Identify the origin of the initial lead in this case, including the first tool, database, or source that associated the defendant or any device with the offense, and the date of that association.
- **Produce all materials concerning any nondisclosure obligation, license term, or policy limiting disclosure of any investigative tool used in this case.**
- If the represented origin of the lead conflicts with the tool records, that conflict is the Franks hearing.

Franks v. Delaware, 438 U.S. 154 (1978). The stingray record is the argument for why origin demands are reasonable.

Where did this case actually begin?

- What was the first piece of information that pointed you to my client? What was its source?
- Did any commercial location tool or data broker service touch this investigation? Would your agency's subscription records agree with that answer?
- The affidavit says the lead came from a database. What database? Who queried it, and what did the query say?
- How does an advertising ID become my client? Who made that association, and with what training?
- **Is there any agreement that limits what you can say in this courtroom about the tools you used?**
- If the answer to the last question is yes, everyone in the room should want to see it.

Ask the origin questions in every location case. The honest answers are short. The evasive ones are shorter.

The stingray era ended for one reason.

Defense lawyers refused to accept location evidence with no explained origin.

Do it again. The tools changed. The refusal still works.

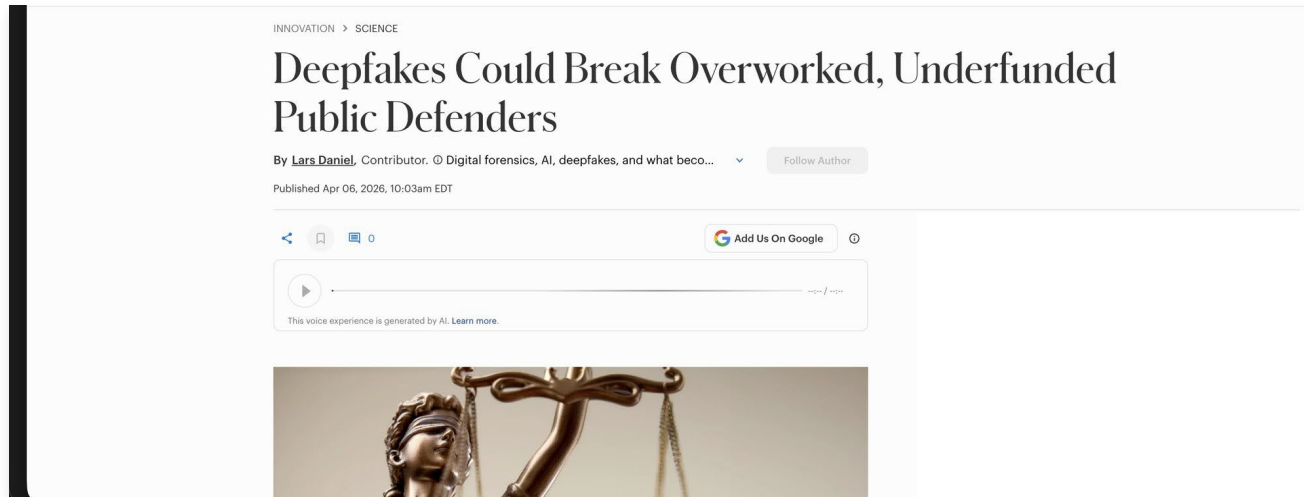
DEMAND THE RECORD. *Name the tools. Demand the origin of the lead. Read the license terms.*

Deepfakes could break public defense

Everything so far was about AI building the case against your client. This last piece is about what AI fakery does to true evidence, and it lands hardest on your side of the aisle.

The economics of authentication, pointed at the least funded side of the courtroom.

05



Fraud is not new.
and neither is this.

MAY 2024



**Fraud is not
new.**

BUT THIS IS





How Evidence Gets Compromised

Fraud Vectors

Fabricated

Fake spills, injuries, and conditions generated entirely from scratch

Altered

Wet floor signs removed, lighting changed, details erased from real photos

Enhanced

Real minor damage amplified to look catastrophic — the hardest to detect

SAS UK (Feb 2026): "With just a few prompts, fraudsters can create, enhance, or erase visual evidence."

October 2024

How Hurricane Helene Deepfakes Flooding Social Media Hurt Real People

By [Lars Daniel](#), Contributor. © Lars Daniel covers...

[Follow Author](#)

Published Oct 04, 2024, 12:27pm EDT
Updated Oct 05, 2024, 04:26pm EDT



**My first article
on deepfakes**

VOGUE JAPAN

January 2026

- The error occurred when the magazine's photo editors employed **AI-powered retouching tools**, which introduced the digital mutation while attempting to enhance the image.
- The mistake went unnoticed through **Vogue's editorial process** and was published to their official website.

VOGUE
JAPAN

FASHION BEAUTY CELEBRITY LIFESTYLE RUNWAY HOROSCOPE VII



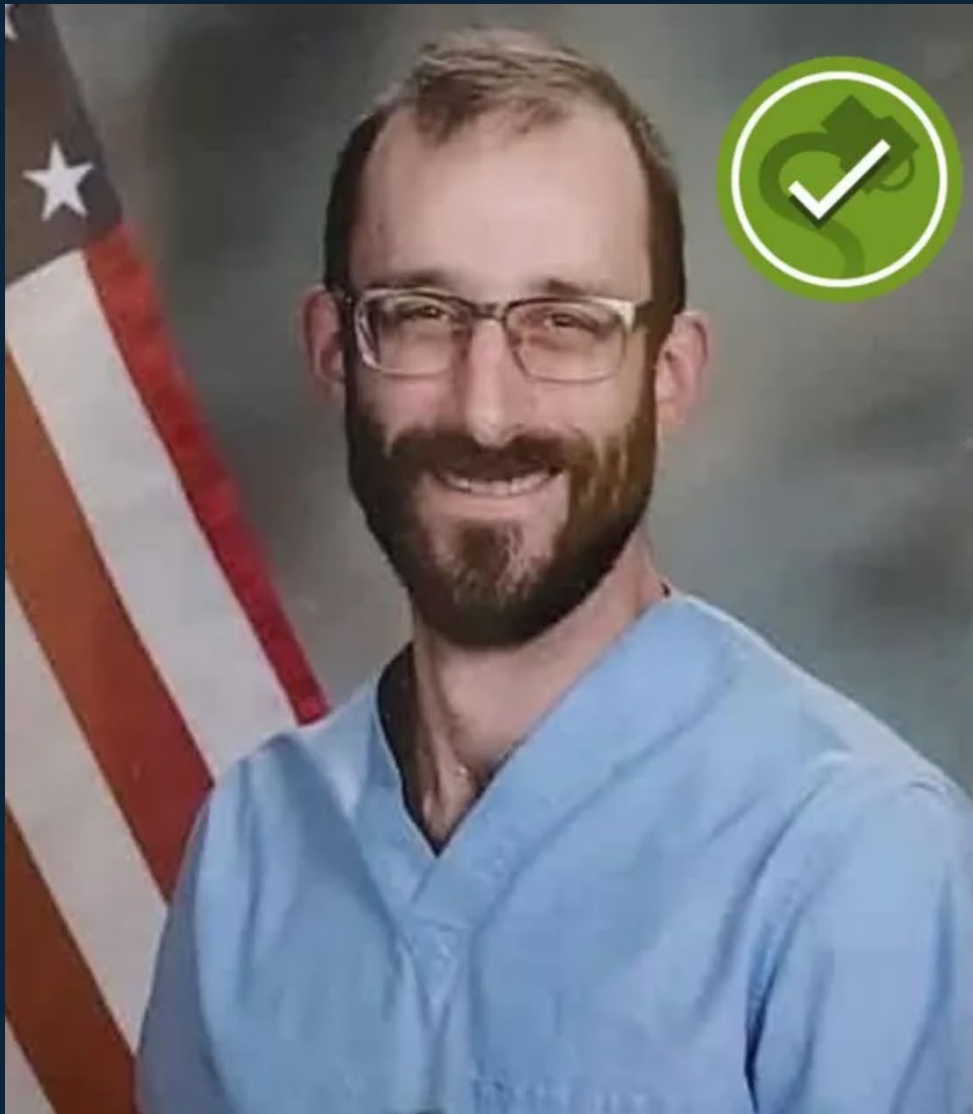
Shirt ¥370,000, Skirt ¥410,000 (both reference prices), Neckband 130,000 (estimated prices) / All DIOR (Christian

ALEX PRETTI INCIDENT

- During a high-profile protest shooting, a bystander image was shared millions of times showing an agent who appeared headless.
- The image, cited on the **Congress floor**, was not a deepfake but an AI "upscaling" hallucination. Forensic scrutiny reveals the pixel errors that escaped political notice.



The Setup: Viewed from a distance, the image appears legitimate, mirroring the initial perception of staff and press.



The news network, formerly known as MSNBC, featured what it later called an "AI-enhanced" image on the cable news network's TV channel, website and YouTube channel...the network ***obtained the image from the internet without the knowledge someone had altered it.***



**No solution
anytime soon.**

Forbes December 8 2025 \$1/week F

INNOVATION > SCIENCE

Deepfakes Are Entering U.S. Courtrooms—Judges Say They’re ‘Not Ready’

By [Lars Daniel](#), Contributor. ⓘ Lars Daniel covers digital... Follow Author

Forbes January 10 2026 ek F¹

EDITORS' PICK | INNOVATION > SCIENCE

AI Didn't 'Unmask' The Minneapolis ICE Shooter — It Invented A Face

By [Lars Daniel](#), Contributor. ⓘ Lars Daniel covers digital evidence and forensics in life and law. Follow Author

Forbes February 22 2026 week F¹

INNOVATION > SCIENCE

'Seeing Is Believing' Is Dead: AI Deepfakes Have Broken Visual Evidence

By [Lars Daniel](#), Contributor. ⓘ Lars Daniel covers digital evidence and forensics in life and law. Follow Author

Published Feb 22, 2026, 04:41pm EST, Updated Feb 23, 2026, 04:20pm EST

and
because
it's **worse**
than you
think.



<https://lucy.decart.ai/>





~~**HYPOTHETICAL**~~

**It's
probably
already
happening
to
you.**



Overserved?



Modern Metadata Myths

Original From Phone



Modern Metadata Myths

Sent From iPhone Photos Using Gmail



THE MISSING STUFF

Date/Time Original	:	2026:01:24 20:27:36
Create Date	:	2026:01:24 20:27:36
Offset Time	:	-06:00
Offset Time Original	:	-06:00
Offset Time Digitized	:	-06:00

Make	:	Apple
Camera Model Name	:	iPhone 16 Pro Max
Orientation	:	Rotate 90 CW
X Resolution	:	72
Y Resolution	:	72
Resolution Unit	:	inches
Software	:	26.2
Modify Date	:	2026:01:24 20:27:36
Host Computer	:	iPhone 16 Pro Max

The government's evidence arrives with its authentication built in

- **Body camera video arrives pre authenticated.**

It rides in on infrastructure that was bought to authenticate it: cloud platforms with tamper evident audit trails, cryptographic file fingerprints, custody documentation, and an officer available to swear to it. Nobody pays an authentication cost at trial, because the department paid it up front when it signed the contract.

- **Surveillance, dispatch, jail calls: same road.**

A records custodian signs a certification and the exhibit walks in. My understanding as an expert who works under these rules: the federal rules were amended so certified records from an electronic process can come in on paper, without a live fight. In practice, the government's digital evidence self authenticates.

- **Your evidence has no infrastructure behind it.**

A video on your client's cousin's phone. A witness recording. A screenshot that crossed WhatsApp and lost its metadata in transit. No custodian, no audit trail, and when the government shrugs and says it could be fake, answering costs a forensic examination that mostly nobody will fund.

- **The deepfake era prices that gap.**

Their exhibits keep their presumption. Yours pay the liar's dividend, and the tax is collected almost entirely from your side of the aisle.

Once fabrication is possible, denying real evidence gets cheap

- **Saying it could be a deepfake costs nothing.**

The scholars who named the liar's dividend saw it coming in 2019: as the public learns any recording can be faked, the value of denying a real one goes up. The words cost nothing, prove nothing, and still plant doubt in a jury that has seen the fakes on their own phones.

- **The authenticity challenge is a cost weapon.**

Raising one costs an afternoon of drafting. Answering one properly costs preservation, examination, an expert report, maybe a deposition. At some price point, the rational side settles on economics instead of merits.

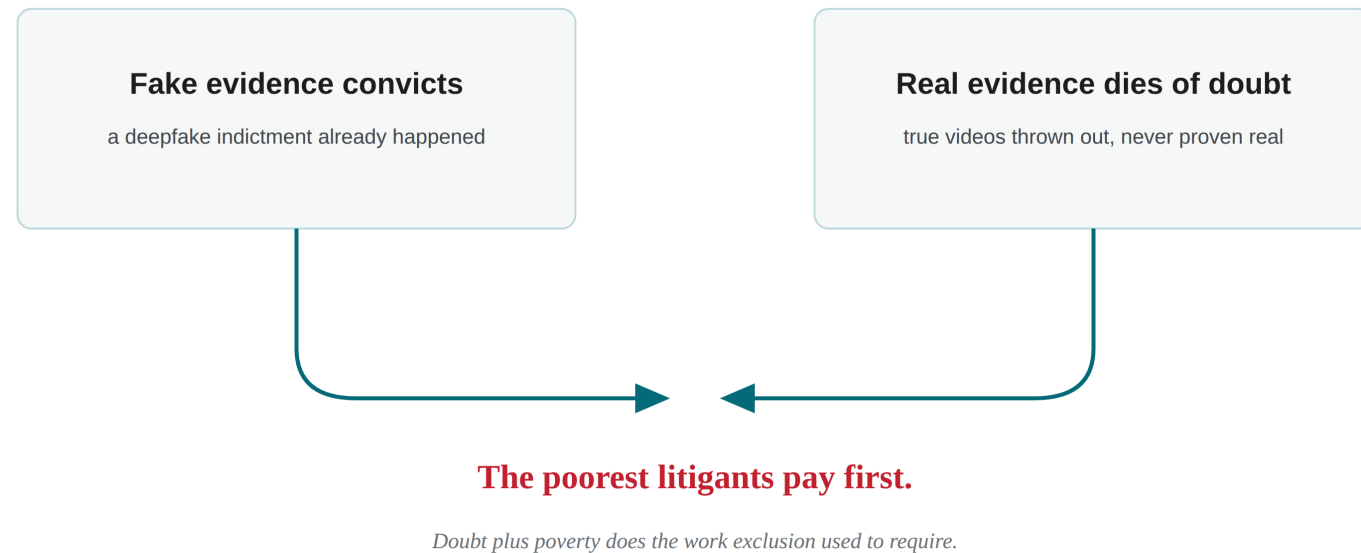
- **Pointed at your clients, it neutralizes true evidence.**

When the challenge lands on the exculpatory phone video or the witness recording, answering costs an examination nobody will fund. The evidence does not get excluded. It quietly dies of doubt plus poverty.

- **And it cuts the other way.**

Federal prosecutors indicted a person on fabricated audiovisual evidence, per the record in that case, and nobody challenged the file. Fakes convict, and real evidence dies of doubt, and both failures land on the poorest litigants first.

The same technology fails in both directions



It keeps happening.



An indictment built on fabricated audiovisual evidence. Nobody challenged the file.

All three at forbes.com/sites/larsdaniel. Dates as shown.

Provenance is the new possession

- Preserve your own evidence the way you preserve the government's, from day one. Native files, source devices, custody notes, and cloud preservation letters before retention windows lapse. Provenance decays on a clock that starts at recording.
- When the government challenges your evidence, make them commit in writing: what, specifically, is the basis? Pure possibility, on the record, is your argument that the challenge fails, because possibility is universal now.
- **When the science sits at the center of the case, my understanding is that Ake supports funding an expert for an indigent defendant. Authentication in the deepfake era is that science.**

DEMAND THE RECORD. *Native files, source devices, and custody notes, for your own evidence too.*

Ake v. Oklahoma, 470 U.S. 68 (1985). Full authentication playbook in the handout, keyed to my published columns.

IF YOU REMEMBER ONE PAGE, MAKE IT THIS ONE

Five systems. Five demands.

FLOCK	The complete audit log export: every search of the plate, who ran it, the typed reason, and the scope.
AI REPORTS	The preservation letter on day one: the machine's draft, the prompts, the audit trail, the usage records.
FORENSIC TOOLS	The tool and version, the AI features enabled, the operator's log, and an image for independent re-examination.
BOUGHT DATA	The tools by name, the origin of the lead, and every license term that limits disclosure.
YOUR OWN EVIDENCE	Native files, source devices, and custody notes, preserved from the day you are appointed.

Every system in this hour keeps a record of what it did. The habit is demanding it.

The warning

The cameras log every plate. The reports write themselves and destroy their drafts. The forensic tools suggest the conclusions. The location trail gets bought, and the receipt is marked confidential.

Every one of these systems keeps a record of what it did.

The abuses were all found the same way: someone demanded the record. That someone is you.

Connect With Me On LinkedIn

I help insurance and legal professionals stay ahead of the technology reshaping their cases and their clients' lives.



Lars.Daniel@Rimkus.com
252-507-5146

TheLarsDaniel.com

