

October 11, 2026

Judge Says Warrantless Flock Search Unconstitutional; Throws Out Evidence Found

I am sure this will be appealed, still interesting. A judge in Oklahoma ruled that a police officer violated the Fourth Amendment after doing a Flock search because her license plate was from out of state. They found 91 pounds of meth, but the evidence was thrown out because the search was illegal.

Please check out our blog at [HTTPS://TCPS-BLOG.COM](https://TCPS-BLOG.COM)

You can also find copies of the weekly newsletter at <https://cybercecurity-mitch-tanenbaum-blog.com/SNU>

We have a YouTube Channel with a lot of videos. Check it out at: [Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube](#)

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCecurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at <https://cybercecurity.us>. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

Security/Privacy Alerts

Judge Says Warrantless Flock Search Unconstitutional; Throws Out Evidence Found

I am sure this will be appealed, still interesting. A judge in Oklahoma ruled that a police officer violated the Fourth Amendment after doing a Flock search because her license plate was from out of state. They found 91 pounds of meth, but the evidence was thrown out because the search was illegal.

The officer's "use of the ALPR Systems was an Unconstitutional Warrantless Search," and "was not supported by probable cause, and it was done without a warrant in violation of [the defendant's] Fourth Amendment rights,"

There are currently more than a hundred thousand warrantless searches of Flock data every month. Flock is laying off people, likely due to the number of cities that are distancing themselves from Flock's radioactivity. Credit: [404 Media](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](https://aigip.ai). If you are a government employee, check out our AI Governance for Govies at the same site.

Want to stay on top of the news about AI - Check out our news feed on the AIGIP web site at <https://aigip.ai/news/latest-ai-news>

President's AI Task Force Faces Expertise and Partnership Challenges

Not a big surprise, given the fact that the feds pay a lot less than the private sector getting the best and the brightest is likely not going to happen. Especially with the short fuse they have. The White House task force is supposed to make recommendations about what the president should do about government engagement with critical infrastructure, AI firms and civil society groups in just 120 days. It has all of the top heavy folks like OMB Director and the Under Secretary of Defense for Research and Engineering, but the experts like CISA and others appear to be absent. Does this mean that this is designed to make it look like the government is doing something while hoping the attention goes away and they don't have to do anything? I don't know. Credit: [Cybersecurity Dive](#)

President's Desire to Rename AI to SI has a Few Hidden Landmines

Being totally honest, I was not clear about this. Turns out it is not as simple as getting out your eraser, removing an "A" and typing an "S". This is separate from actually getting people to change, which is always hard. Learn what the lawyers have to say about this. Credit: [Wiley \(law firm\)](#).

Shocker: Newsom Pokes Trump in the Eye (Figuratively)

Just as soon as the president told federal agencies to use the term SI instead of AI in any place that does not have legal significance (since he cannot do that with his felt tip), Newsom issued his own EO telling state employees that they are prohibited from using the term SI. Who would have guessed that would happen. Credit: [Politico](#)

Art Imitates Life

I happened to turn on a police procedural TV show, **Law and Order**. The storyline in Season 26, Episode 1 is an AI that goes rogue and orders a successful hit on someone. The AI even paid the hitman \$20,000. The DA decides to charge the CEO with second degree murder - depraved indifference, saying the CEO should have known that it could come to this. No AI CEOs have been charged yet, but should they be? Interesting question.

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

**** REMINDER** NEW SPRS/PIEE System Access Requirements**

This is not a change to CMMC, but PIEE is now requiring that you log in at least every 34 days to keep your account active, so make sure you put this on your recurring task list.

Are You Ready for CIRCIA?

CIRCIA is an executive-branch-wide regulation which was mandated by Congress that makes new reporting rules for breaches involving all 16 critical infrastructure categories. This is in addition to the existing rules in DFARS 7012 for breach reporting. The rule has been in the

works for a couple of years now and is now in the final review in OIRA. This is the last step before publication in the federal register. This is different from the FAR CUI Rule, so there is a lot of stuff going on. This rule doesn't allow for "out of scope", so if you are, for example, a defense contractor (or in energy or finance or any other critical sector) and you have a breach anywhere in your organization, you get to report and you don't have a lot of time. Right now, sectors like defense and finance, which already have to report breaches, sometimes to multiple agencies, will have another reporting requirement. We have not seen the final rule - it will be a surprise when it is published - so we don't know what CISA decided about how to deal with overlapping reporting requirements. The best guess is that they will publish it sometime before the end of the year or, at the latest, by the end of first quarter. Once it is published we will see what the effective date is. Could be anywhere from immediately to, maybe, a year later. No one knows. We will watch this and do a video with the details once they make it public. As I said, this affects all critical sectors, all systems, as far as we know. More motivation to avoid getting breached.

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

Bankers Sue Feds Over Crypto Banks

As you are probably aware, the president changed his tune from 2021 when he told Fox that Bitcoin seems like a scam to December 2022 when he launched his own NFT and then 2025 when he launched his meme coin. Between the two he has pocketed around \$650 million. You can probably see why he likes crypto now. Since the beginning of his second term he has been trying to help out the crypto bros who donated millions to his campaign. Recently, the OCC changed the rules of what it takes to get a national trust bank charter, allowing non-depository, non-fiduciary companies to get one. Needless to say, banks are not happy with this and are suing the OCC over it. The issue is based on how the OCC decided to interpret a provision in the National Bank Act added in 1978. The OCC has approved or conditionally approved 21 national trust bank charters during this administration. The Independent Community Bank Association is arguing that the administration is creating a new type of bank not allowed by the National Bank Act. I am sure this will make it to the Supremes. Credit: [Ballard Spahr \(law firm\)](#)

Education

State Financial Regulators Release AI Supervisory Framework

On September 16, 2026, the Conference of State Bank Supervisors (CSBS) announced the release of its Artificial Intelligence (AI) Supervisory Framework (Framework), which provides state examiners (AND ANYONE ELSE) with a detailed roadmap for identifying and assessing AI use at supervised financial institutions—including the questions they may ask and documents

they may request. The guidance includes five documents - core examiner guide, examiner work program, nonbank AI supplement, AI use case risk tiering worksheet and the source support document. Even if you are not in the financial industry, this should be a piece of your AI governance program. Credit: [Step toe \(law firm\)](#) and [Conference of State Bank Supervisors](#)

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. **NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.**

Trump Mobile Hacked - Apparently More Than Once

In the most recent hack the hackers claim to have stolen data from about 3,600 customers. The group published the data. Trump Mobile's response was interesting. They are reported to have said ***"We have no team to handle this' and that anyone who hacks them [is] a terrorist "***. Those may be true statements, but telecommunications is considered critical infrastructure so if that is an admission of fact, the feds could say they have a problem. Credit: [PC Magazine](#)

Bored Teen Hacked Microsoft Database with 17 Trillion Rows

The teen got access to Microsoft's internal Titan analytics services and got access to an estimated 17.3 trillion rows and a metadata table of about 25,000 accounts. Microsoft fixed the bug and gave the kid a whopping \$5,000. With payouts like that kids might choose the dark side instead. Credit: [Tech Radar](#)

Georgia Power and Alabama Power Data Breach - 400,000 Victims

Mississippi Power was also affected but there are no numbers for that company's victims. All of them are part of the Southern Company. Typical stuff stolen - name, address, phone, email, last 4 of the social and other basic account information. Stuff that has been stolen a million times, unfortunately. Credit: [Security Week](#)

Is satellite Internet (Starlink) a military target

While Starlink is the biggest target, it is not the only target and Iran has already knocked Starlink offline once, so what is the plan? Ukraine is building its own version of Starlink. Is this going to be a problem? Only rogue states (like Russia, China and North Korea, among others) are likely to do this. Learn more [here](#).

In the age of cyber, don't forget physical

While we focus a lot of energy on cyber attacks, it is clear that physical attacks are not going away and then you have to deal with the cyber-physical overlap. You need to be prepared for both. Learn more [here](#).

OpenAI says labs should not be liable for AI agent hacking

The software industry has been very successful at avoiding responsibility for its products. Imagine if automakers were able to pull that off. Or airplane manufacturers. Only software. Possibly that is about to change. Learn more [here](#).

Security News for the week ending October 9, 2026

This week's news: Senate passes bipartisan healthcare cybersecurity bill but will it become law, FBI finds scapegoat for breach, AI could crack crypto wallets before quantum computing, AI /

data center IPOs are not doing so well this year and Anthropic offers Free AI security scans to open-source maintainers. Learn more [here](#).

Whether you call it AI or SI, personal agents are still a huge risk

Every AI company out there is releasing personal agent technology. Meta just released theirs (Muse) even though THEY understood the risk. It is about money. For you, it is about an employee's agent taking down the company. Amazon learned about this the hard way. Want to deploy agents, personal or other, you need to make sure that you have a strategy. Contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663