

May 17, 2026

AI Leads to False Arrests and Even Convictions

In Baltimore, on October 20, 2025, a 17 year old student was sitting outside his high school after football practice munching on some chips when AI processing surveillance camera footage decided that his bag of Doritos was a gun. On December 24, 2025, a Tennessee grandmother was released from jail after spending five months there after AI based facial recognition software said she was connected to fraud activities in North Dakota. Police arrested her at gunpoint while she was babysitting her four grandchildren. If you are rich and can afford expensive lawyers, you can likely get the cops to quickly back down. If you are the average person, you are likely much less able to defend yourself and wind up like these folks. As police expand the use of AI without proper oversight, training and policies, this is likely to get much worse before it gets any better. Credit: [Route Fifty](#)

Please check out our blog at <https://www.cybercecurity.com/cyblog>

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

GM Pays Largest Ever California Privacy Settlement

At \$12.75 million it is still couch cushion change for them, but it does make a point that if you break the privacy law you will, at least, be publicly outed. They were selling your driving data to (anyone who had the cash) data brokers. They also agreed to delete your driving data after 180 days (meaning they still track your every trip and keep that data for 6 months) unless you agree to let them keep it. They also agreed to ASK two data brokers that they SOLD your data to - LexisNexis and Verisk - to delete that data. It is unclear if that request is a "voluntary delete" or mandatory. GM says that they stopped selling that data in 2024 - likely right after they were notified by the state that they were under investigation. It is good to understand that the brokers

then sold the data to insurance companies so that they could jack up your rates if they did not like your driving habits. Credit: [The Record](#)

Home Depot Installs Flock Surveillance Cameras

Home Depot is no stranger to political intrigue. This time, it is about surveilling its customers and visitors. As a result of a lawsuit filed last month, it was revealed that Home Depot is working with surveillance giant Flock and has installed cameras in all 233 California store parking lots and that data is being sent to Flock to be shared nationwide. These cameras have been in place for at least a year and it is unclear whether Home Depots in other states also have Flock surveillance cameras. Credit: [My Privacy Blog](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#).

AI Leads to False Arrests and Even Convictions

In Baltimore, on October 20, 2025, a 17 year old student was sitting outside his high school after football practice munching on some chips when AI processing surveillance camera footage decided that his bag of Doritos was a gun. Police swarmed him, cuffed him on the ground and confiscated his empty crumpled bag of chips. On December 24, 2025, a Tennessee grandmother was released from jail after spending five months there after AI based facial recognition software said she was connected to fraud activities in North Dakota. She had never been to North Dakota. Police arrested her at gunpoint while she was babysitting her four grandchildren. If you are rich and can afford expensive lawyers, you can likely get the cops to quickly back down as you both threaten to sue them and actually sue them. If you are the average person, you are likely much less able to defend yourself and wind up like these folks. These are just a few of the stories I have which resulted from law enforcement not properly trained and thinking that computers are always right. Hopefully, the reader is not one of these unfortunate people but as police expand the use of AI without proper oversight, training and policies, this is likely to get much worse before it gets any better. Credit: [Route Fifty](#)

Amazon Workers Are Maximizing Use of AI - But Only in Reports

This is where poor governance shines. Amazon wants its workers to use AI. For example, they want 80% of developers to be using AI every single week. So they do. There is even a term for it - tokenmaxxing. Of course, all they are tracking is how many tokens people are using. Developers create agents that do irrelevant tasks, but use lots of tokens. Mission accomplished. It keeps corporate happy and the developers don't have to change their ways. This is a perfect example of poor AI governance. If you want to know what good governance is, take our FREE AI governance course at [www.aigip.ai](#) . Credit: [Tech Radar](#)

ChatGPT Usage at all-time-low as QuitGPT Dents Popularity

ChatGPT recorded its weakest referral market share since tracking began. This is because there are competitors out there that are viable competitors. This includes Perplexity, Gemini and, of course, Claude. While ChatGPT accounted for 76% of AI chatbot referrals in April and Google only represented 9%, Claude actually brought in more revenue than GhatGPT. Credit: [TechRadar](#)

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.

Nothing to report this week

Reference

Europe Continues to Push Away from American Tech - Munich Ditches Windows

The president would like US tech to be the gold standard. Instead Europe and others are migrating away from US tech, in part because of the attitude of the current administration and in part to stop being locked into license fees and proprietary standards. Munich, Germany has a new strategy called “public money, public code”. The Open Source Program Office is working to build infrastructure free of the constraints of proprietary providers; instead using open interfaces and manufacturer independent standards. As part of this, the German government (not just Munich) said that they will issue all public sector documents ONLY in open formats, which does not include Microsoft Word. Germany’s Schleswig-Holstein state says that they have already moved 80% of state government workplaces away from Microsoft software and France and Switzerland announced plans to move away from Microsoft. Credit: [Cybernews](#)

Software and Hardware to Check Out

Apple Begins to Realize that Their Customers Might Want to Talk to Non-Apple Users

Text messaging between iPhone and Android users has always been a bit of a mess if you are using Apple products. This has not been a problem if you are using third party tools like Signal and Whatsapp. Finally, with iOS 26.5, Apple is beginning to roll out encrypted messaging to non iPhone users. Of course, Apple felt it necessary to say that iMessage (their proprietary iPhone-only messaging app) is still best - as long as you only you want to talk to other iPhone users. Still it is nice to see that Apple is slowly being forced to acknowledge that not everyone on the planet is in a romance with Apple. Credit: [Help Net Security](#)

Important Issues/Patches

The Geniuses at the FTC Realize that Blocking Patches to Millions of Consumer Routers is NOT Good Security

This is a two part problem. The president promised millions of new manufacturing jobs if elected, which have not materialized. He also wants to improve national security. Both of these are good objectives. One piece of the solution is to force Americans (or their Internet provider) to buy American made routers, which do not exist. In order for this to happen these vendors will have to build their routers here. Which takes time and is likely much more expensive. To try and force the issue the FTC issued a policy to stop patches to foreign routers after January 2027. Apparently, someone in the FTC building realized, eventually, that if they did that, the Chinese router makers that have tens of millions of routers installed in the US and their US Internet provider customers would send them Christmas presents because they now have cover for disbanding their software patching efforts and saving a lot of money while making American consumers fair game to every attacker anywhere in the world, because vulnerabilities are not being fixed. The FTC just changed the rule and said existing approved routers could be patched through 2029. I think they are hoping that these routers will be discarded by then, but that is probably not likely and they will change their mind again. Credit: [Toms Hardware](#)

Legislative and Legal Activities

Canadian Bill to Force Tech Companies to Install Surveillance Backdoors Moves Forward

England is not the only country that wants to allow the government to be able to spy at will on its citizens. Canada's C-22 bill does just that and more. Civil liberties groups are not happy, but the government is still pushing. It is also likely that it is unconstitutional, but that may not stop the bill from passing. It allows for a more limited ability to force providers to disclose information without a warrant than previous versions of the bill. It would require providers to retain metadata for up to a year at their cost (or really your cost since prices will likely increase to pay for this massive data collection and retention). There is a requirement in the bill for Parliament to review the effects but not until three years into it. One of the bigger concerns is the requirement for providers to develop backdoors into their systems that allow the government to read your data. This is similar to what happened in England when Apple decided to stop encrypting your data in the cloud rather than inserting a backdoor. This was also a way for Apple to let people know that their data in the cloud was no longer protected. This bill is not law yet, but we will watch it. Of course, depending on whether a particular media outlet is for or against the bill will color the reporting, so it would be wise to read multiple outlet's reports. Credit: [Fasken](#)

Former L3Harris Exec Who Sold Hacking Tools to the Russians to pay \$10 Mil

Peter Williams, a veteran cybersecurity executive who was the head of the hacking and surveillance tech division of U.S. defense contractor L3Harris, has been ordered to pay \$10 million to his former employer. Williams was the central figure in one of the worst leaks of advanced hacking tools in the history of the United States and its closest allies. Credit: [Tech Crunch](#)

Texas sues Netflix Over Data Surveillance Practices

Texas AG Ken Paxton who, no doubt, is running for some office (US Senate), is suing Netflix for collecting and selling (technically sharing) subscriber data with advertisers and data brokers without your permission. Netflix has said multiple times in the past that they do not collect and share user data with advertisers, even though they track every single thing that you do. Before you cancel your Netflix subscription, unless you can find a DVD store that accepts cash, everyone is doing this. What is getting Netflix in trouble is blatantly lying about it. Note that in their response they did not deny doing this, they just spun up a legal defense that what they are doing complies with the law. Not sure that committing fraud (lying) is complying with the law, but they will be up to a jury of 12 very annoyed consumers. They have already been sued over this in Europe. Credit: [The Record](#)

Education

Nothing to report

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.

Canvas LMS Breach Impacts 275 Million Students - FOLLOW UP

The Canvas software is back online; Canvas has admitted that they paid off the hackers not to leak their data. It needs to be understood that paying a group of people who stole 3.6 terabytes of your data and who break the law for a living to give you a promise that they won't leak your

data is probably not worth very much. Given this happened at finals time, it is probably worthwhile for schools to try and figure out what, if anything, they can do to protect themselves in future situations like this. The Canvas CEO also apologized for how (badly) they handled communications. Again, not sure how much this is worth. They did not admit how much they paid the criminals. Credit: [Cybernews](#)

Update: The US House of Representatives has requested a briefing by Instructure's CEO by May 21st. Given there are going to be lawsuits, I suspect that the CEO is going to be limited in what his lawyers tell him he can say. Credit: [The Record](#)

Cushman & Wakefield Hit by ShinyHunters - Leaked 50 GB of Data

This is more ShinyHunters thing than Canvas. This was a Salesforce attack, their bread and butter. What is ugly is that a second group, Qilin, also claimed C&W as a victim. Were there two attacks? The claim is that ShinyHunters stole 500,000 records. To support their claim, they publicly dumped a 50 GB database. They claim to have done this via a voice phishing attack (vishing). Credit: [Breachd Company](#)

TECHNICAL DEBT- It is coming home to roost

You know all that work that your IT team has been telling you that they don't have the resources to fix? That is technical debt and with AI tools, that debt is going to become a much bigger problem. Learn why [here](#).

Does your insurance cover your AI processes?

It might this year and it likely won't next year as insurance companies hate covering events that they have no historical information on. Some renewals and new policies are already explicitly excluding them, so look carefully. If you need assistance with that, please contact us. Learn more [here](#).

Industry trying to fill gap left by CISA meltdown

As the critical infrastructure industries like power, water, gas, etc. realize that after CISA fired more than a thousand people and hundreds more left or got reassigned to other agencies, the likelihood of CISA even doing what it is legally required to do is low. So, some of the large players decided to fund their own private CISA-like agency. While this will help them, it is not likely to help you. You are on your own. Learn more [here](#).

Security News for the week ending May 15, 2026

This week's news: EU continues its purge of US tech companies, WHEN China's AI catches up to Mythos, smart move by the Secret Service, Musk caves. Again. And, Mythos AI destroyed 5 years of Apple security in a week. Learn more [here](#).

You may not realize that you have been getting assistance from CISA, but you have through all of the behind the scenes work they were doing. Now that is all up to you. Are you prepared? If you need assistance, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663