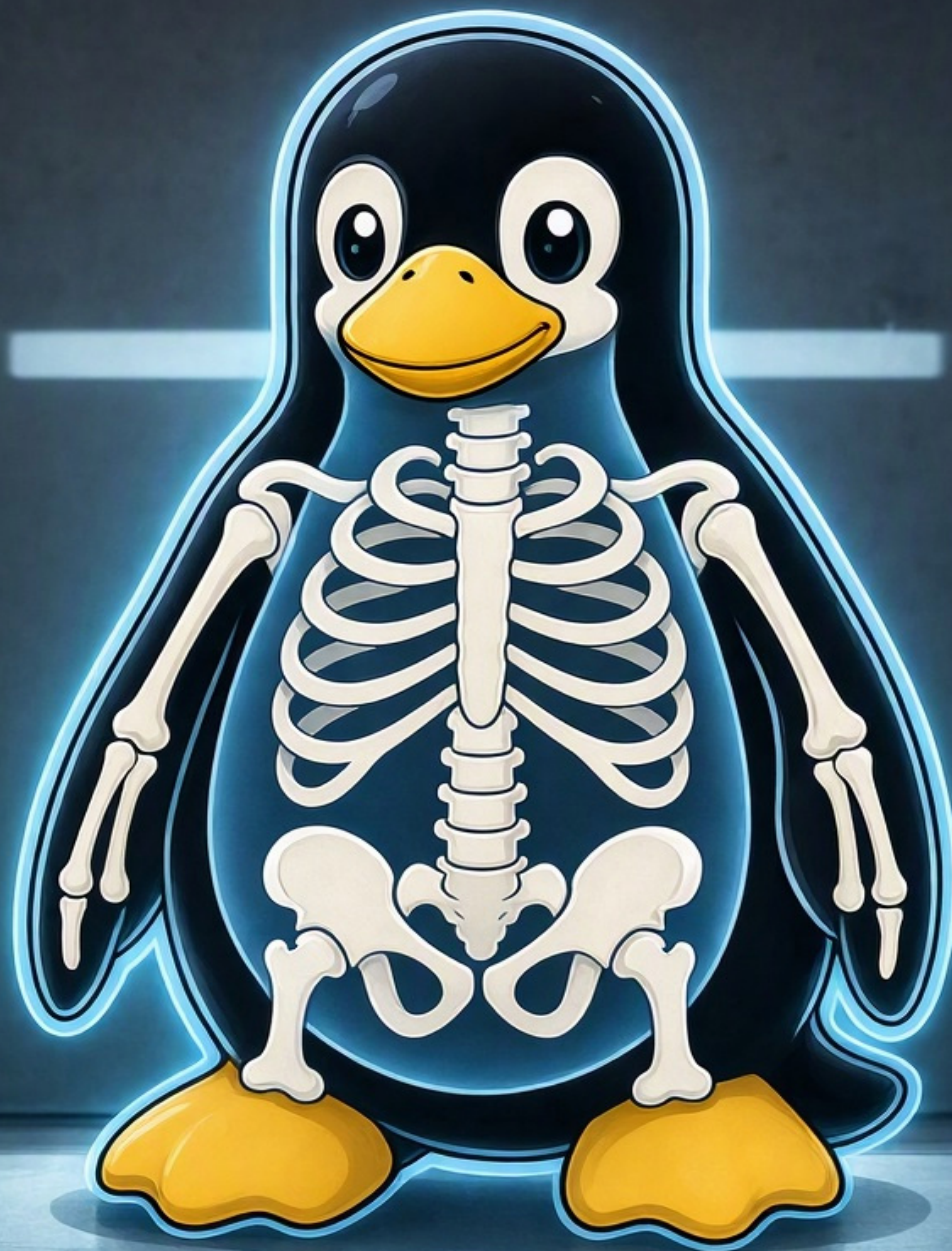


The PCLinuxOS magazine

Volume 238

November, 2026



ICYMI: Free Cloud Storage!

AI Is Finally Helping The People

GIMP Tutorial: Create A Simple Logo

Lessons Learned From 'AdFection' & What To Do Next

Wiki Pick: Automatically Mount A Drive Using /etc/fstab

PCLinuxOS Recipe Corner: Johnny Marzetti Casserole

Social Media When Elections Are Close: Doing The Impossible Better

PCLinuxOS Puzzled Partitions

And more inside...

In This Issue...

- 3** *From The Chief Editor's Desk*
- 4** *Screenshot Showcase*
- 5** *ICYMI: Free Cloud Storage!*
- 11** *Screenshot Showcase*
- 12** *PCLinuxOS Recipe Corner: Johnny Marzetti Casserole*
- 13** *Social Media When Elections Are Close:
Doing The Impossible Better*
- 15** *Screenshot Showcase*
- 16** *GIMP Tutorial: Create A Simple Logo*
- 18** *Screenshot Showcase*
- 19** *Lessons Learned From 'AdFection' & What To Do Next*
- 21** *AI Is Finally Helping The People*
- 29** *Require Police To Get A Warrant To Search ALPR Data*
- 32** *Screenshot Showcase*
- 33** *Wiki Pick: Automatically Mount A Drive Using /etc/fstab*
- 34** *Court Should Curb Abuse
Of Grand Jury Subpoenas Targeting Social Media Users*
- 35** *Screenshot Showcase*
- 36** *PCLinuxOS Recipe Corner Bonus: Mexican Ground Beef & Noodles*
- 37** *PCLinuxOS Puzzled Partitions*
- 41** *Inspiration & Motivation*
- 42** *More Screenshot Showcase*



The PCLinuxOS name, logo and colors are the trademark of Texstar. **The PCLinuxOS Magazine** is a monthly online publication containing PCLinuxOS-related materials. It is published primarily for members of the PCLinuxOS community. The magazine staff is comprised of volunteers from the PCLinuxOS community.

Visit us online at <https://pclosmag.com>.

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)

Assistant Editor: Meemaw

Artwork: Paul Arnote, Meemaw

PDF Layout: Paul Arnote, Meemaw

HTML Layout: tbs

Staff:

YouCanToo David Pardue

Alessandro Ebersol

Contributors:

The PCLinuxOS Magazine is released under the Creative Commons Attribution-NonCommercial-Share-Alike 3.0 Unported license. Some rights are reserved. Copyright © 2026.



From The Chief Editor's Desk

Here in the U.S., as the calendar turns over to November, thoughts about the Thanksgiving holiday move to the forefront of our collective consciousness. It is also customary to express



our gratitude and thanks for the things in our lives that we perceive to be good. As such, I'll attempt to do something similar.

I am thankful, first and foremost, for my wife and kids, and the family my wife and I have created.

I am thankful for my relatively good health.

I am thankful for the home that we have made.

I am thankful for being able to have retired when I did (at the end of 2022), and to be able to be home every day when my kids come home from school.

I am thankful for all of the friends I have made throughout the course of my life. Each friendship delivers unique traits that enhance my own life.

I am thankful for having discovered PCLinuxOS, and for Texstar and all of the others who keep PCLinuxOS running like a well-oiled machine. I am also thankful for the family that I have become a part of, a family of PCLinuxOS users from all corners of the world.

I am thankful for Meemaw and tbs, whom without, this publication would not exist, at least in the manner in which it currently exists. We make a pretty good team (in my honest opinion). Meemaw has been a rock by my side for much

of the time that I've been the magazine's Chief Editor. And, the HTML and eBook versions of the magazine are expertly handled by tbs. You guys are the best!

This month's cover image commemorates the discovery of X-rays on November 8, 1895 by German physicist Wilhelm Roentgen, even though it was done completely by accident. According to an [article](#) from The Conversation, he was doing an experiment and was surprised when a screen on the other side of the lab glowed. Wilhelm worked out that some invisible rays were causing it but had no idea what they were. That is why they're called x-rays, with "x" meaning "I don't know"! The image was created with [Bing Image Creator](#).

Until next month, I bid you peace, happiness, serenity, prosperity, and continued good health!

 **LINUX HANDBOOK**
Level Up Your Linux Skills!

 
Introduction to Linux
FREE Course



Support PCLinuxOS!
Get Your Official
PCLinuxOS Merchandise
Today!

PCLinuxOS



Help PCLinuxOS Thrive & Survive

**DONATE
TODAY**



Screenshot Showcase



Posted by francescoinblack, October 19, 2026, running IceWM.

ICYMI: Free Cloud Storage!

by Paul Arnote (parnote)



Image by [Pete Linforth](#) from [Pixabay](#)

A VPN conceals your IP address by routing your internet traffic through a remote server, preventing anyone surveilling the network from tracking your online activity. **Theoretically, that means no one should be able to identify you when you connect to a network and browse the internet, even your ISP**, according to an [article](#) from Lifehacker. In practice, though, there are plenty of gaps that hackers can exploit. A while back, Lifehacker covered [browser fingerprinting](#), which uses hundreds of data points, like your hardware specs, operating system version, web browser, and GPU signature, to establish a shadow profile that follows you around even when your VPN is enabled. There's another way cyberattackers can intercept your data, and it involves exploiting a communication leak right inside your browser. Major browsers like Chrome, Firefox, and Edge

have a feature called WebRTC that lets them bypass the encrypted Transmission Control Protocol (TCP) tunnel created by your VPN to establish high-speed connections for demanding tasks like video streaming, voice calls, and screen sharing. This leaves your real IP address exposed throughout the transmission, offering plenty of time for attackers to capture the identifying information you are trying to hide. Luckily, VPN providers are getting better at preventing WebRTC leaks through additional security features, but these protections often need to be configured manually in your VPN settings or, if your VPN does not offer WebRTC leak prevention, directly in your web browser. I'll show you how to set it up step by step, so you don't get blindsided by an unintended IP address leak.

Most Americans 50 and older said they would be interested in receiving a vaccine that could reduce their risk of dementia if they were at high risk, survey data showed, according to an [article](#) from MedPage Today. Nearly three in four survey respondents (72.1%) said they would likely or definitely receive such a vaccine, said J. Felipe Montano-Campos, PhD, of the University of Southern California Schaeffer Center for Health Policy and Government Service in Los Angeles, and co-authors. One-fifth of respondents (20.8%) weren't sure, and 7.2% said they likely or definitely would not, Montano-Campos and

co-authors reported in a [JAMA Network Open](#) research letter.

Attackers wasted little time exploiting a recent WordPress vulnerability in the wild, according to an [article](#) from TechRepublic. Threat actors are actively targeting CVE-2026-87902, a critical WordPress Core vulnerability that can lead to remote code execution (RCE) under specific conditions. Researchers observed attempts to identify vulnerable websites less than five hours after WordPress released its fix on Sept. 22, with subsequent attacks progressing to attempts to write files that could execute shell commands. The rapid escalation gives WordPress administrators a narrow window to



act. Sites running vulnerable versions should update immediately and review for post-compromise activity.



Image by [Gerd Altmann](#) from [Pixabay](#)

Cloud storage is likely an essential part of your data management strategy, whether you're just using Google Drive for documents or you back up everything to a remote service. **You can get a significant amount of space for a reasonable monthly fee, but if you prefer not to pay, it's possible to combine free options and cobble together quite a bit of free storage — around 80GB (or more) — at no cost**, according to an [article](#) from Lifehacker. A reminder: You shouldn't rely solely on cloud storage for your backups. Follow the [3-2-1 rule](#), which protects against a single point of failure, such as getting locked out of your account or issues with the service itself.

A single operator used AI agents to attack companies at machine speed, launching 105 attacks and ultimately stealing more than 600,000 credit-card records, according to an

[article](#) from eSecurityPlanet. Researchers at Gambit Security uncovered the campaign, which used three open-source AI systems to automate work normally done by skilled human hackers. The agents scanned for targets and vulnerabilities, ran exploitation attempts, stole information, and deployed malware. At least 27 organizations were compromised during an observed five-day burst. The wider campaign had been running since at least July, and researchers say the operator spent relatively little on AI model usage compared with the scale of the activity. The case therefore offers a concrete example of how AI agents can reduce the human labor needed to run cyberattacks against large numbers of targets, a pattern [Jon Markman](#) from Forbes calls "an early, public demonstration of a new normal."

uBlock Origin is lightweight, effective, and free from shady business practices, says an [article](#) from Lifehacker. Unfortunately, Google's move to Manifest V3 for browser extensions has hobbled ad blockers somewhat. In response, uBlock has split into two products — [uBlock Origin](#) and [uBlock Origin Lite](#). The "Lite" version works with most Chromium-based browsers and Safari for iPhone, iPad, and Mac. The full version of uBlock Origin primarily works in Firefox for desktops, laptops, and Android. With those differences highlighted, this article reveals the 10 uBlock Origin (and uBlock Origin Lite) hacks you should know about.



commandlinefu.com

ICYMI: Free Cloud Storage!



Image by [Nadour Moustafa](#) from [Pixabay](#)

A hacking group claims it breached FBI systems and stole sensitive information tied to thousands of FBI personnel and job applicants, including details about some employees' spouses, according to an [article](#) from eSecurity Planet. ShinyHunters claimed on Sept. 22 that it breached the FBI and obtained sensitive employee and applicant information, according to a [404 Media report](#) that first reported the alleged intrusion. The publication reviewed a sample containing 5,000 purported FBI records, including names, addresses, phone numbers, and information about some employees' spouses. The FBI has not confirmed that its systems were breached or that data was stolen. The bureau said in a statement provided to multiple news organizations that it is aware of claims involving unauthorized activity affecting FBIJobs.gov and is investigating. If ShinyHunters' claims prove accurate, the exposed information could create risks beyond

conventional identity theft, potentially giving threat actors personal details they could use for targeted phishing, impersonation, doxxing, and other attacks against law enforcement personnel and their families.

Over 2 million new cancer cases were attributable to infections globally in 2024, according to an analysis of worldwide cancer incidence, highlighting the importance of effective prevention measures, according to an [article](#) from MedPage Today. Infections led to an estimated 2.3 million new cancer cases in 2024, including gastric cancer, cervical cancer, hepatocellular carcinoma, leukemias and lymphomas, and nasopharyngeal cancer, which accounted for 12% of all cancer cases worldwide. Among 12 carcinogenic infectious agents, the largest numbers of cancer cases were attributable to: *Helicobacter pylori*: 760,000 cases, population-attributable fraction (PAF) 4%, Human papillomavirus (HPV): 750,000 cases, PAF 4%, Hepatitis B virus (HBV): 360,000 cases, PAF 2%, Epstein-Barr virus (EBV): 260,000 cases, PAF 1%, Hepatitis C virus (HCV): 160,000 cases, PAF <1%, and Kaposi's sarcoma-associated herpesvirus (KSHV): 35,000 cases, PAF <1%. (PAF in statistics stands for Population Attributable Fraction, a measure that estimates the proportion of disease cases in a population that could be prevented if a specific risk factor were eliminated. It combines exposure prevalence with relative risk to quantify preventable burden.) Most cancers attributable to *H. pylori* were non-cardia gastric cancers (700,000 cases), while cervical cancer accounted for most HPV-attributable cases (600,000). HBV and HCV

were responsible for 330,000 and 130,000 cases of hepatocellular carcinoma, respectively, while EBV led to 110,000 nasopharyngeal cancers, reported Harriet Rumgay, PhD, of the International Agency for Research on Cancer in Lyon, France, and colleagues in [Lancet Oncology](#).

Google has given Chrome users 247 new reasons to keep their browsers up to date, according to an [article](#) from eSecurity Planet. The company released Chrome 155 with 247 security fixes, including four vulnerabilities rated Critical and another 53 rated High. The update is rolling out to Windows, macOS, and Linux users over the coming days and weeks, according to Google's Chrome [release notes](#). None of the four Critical vulnerabilities are currently identified by Google as being exploited in the wild. But after a year in which attackers have repeatedly targeted Chrome vulnerabilities, the size and severity of this update give security teams another reason to verify that browser patches are actually reaching managed endpoints.



WIKIPEDIA
The Free Encyclopedia

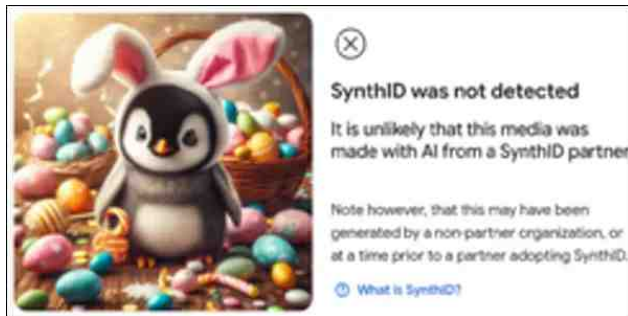
AI agents do not have to break into a website to cause problems. **Wikimedia says OpenAI-linked agents may have helped knock one of**

its data services partially offline, according to an [article](#) from eWeek. In an Oct. 5 disclosure, the Wikimedia Foundation said agents it believes were operated by OpenAI made millions of API requests, crawled millions of pages, and sent hundreds of thousands of queries to its Wikidata Query Service, or WDQS. Wikimedia found no evidence of a breach, but said the traffic may have contributed to a partial outage in May, showing how heavy agent activity can strain public web infrastructure even without a successful attack.

Google is patching seven critical Android vulnerabilities, including flaws that could enable privilege escalation or denial-of-service attacks without requiring user interaction, according to an [article](#) from eSecurity Planet. The company's October Android [Security Bulletin](#), published Oct. 5, details 25 unique Android vulnerabilities, with seven rated critical. A separate Pixel bulletin identifies six additional security flaws affecting supported Pixel devices. For security teams managing Android devices, the updates underscore the importance of checking security patch levels rather than assuming devices are protected simply because they are running Android 17.

"Nature is the world's worst bioterrorist" is a common maxim in the field of biosecurity, a reference to the idea that naturally emerging pathogens cause far more deaths than any biological attack a terrorist could carry out, according to an [article](#) from the Bulletin of the Atomic Scientists. But the trope may soon be outdated. **In an article published Aug. 6 in the**

journal Science, scientists demonstrated that trained AI models can design novel viruses as well as — if not better than — nature itself. Their experiment created viruses that infect bacteria, not humans. Still, much like the multiple [AI models](#) that escaped their test environments to hack other networks this summer, these newly revealed capabilities give biosecurity experts like me pause. How do we keep enabling legitimate scientific progress, while also preventing AI from assisting in the creation of biological weapons?



An abundance of AI imagery is something we all have to live with these days—from school posters to restaurant menus—and while there are still certain tells that indicate something was made with AI, they're not always present. In a lot of cases, it can be almost impossible to distinguish an AI image from a real one. Images produced by Gemini and ChatGPT come with an invisible watermark called [SynthID](#). That way, AI-generated images don't need visible branding in order to identify their origins. Of course, you need access to a detector to know whether this watermark is present. **As it happens, Google just launched a standalone SynthID checker tool on the web, free for anyone to use,** according to an [article](#) from

Lifehacker. This checker supports JPG, JPEG, PNG, BMP, WEBP, AVIF, HEIC, HEIF, TIFF, TIF, and GIF image formats; MP4, MOV, and WEBM for videos, and WAV, MP3, OGG, FLAC, AAC, and M4A for audio. As long as a file was made by a SynthID-supporting AI, it should have a watermark. The SynthID watermark is a standard supported by Nvidia, OpenAI, Kakao, and Google, though OpenAI has its own [detection tool](#). Obviously, Bing Image Creator doesn't participate in the SynthID watermark standard (or it was created before the standard existed), as indicated by me uploading the cover image for the April 2025 issue of The PCLinuxOS Magazine (above) to the SynthID checker tool. The cover was completely created by Bing Image Creator, but SynthID couldn't find an invisible watermark.

Hackers reportedly manipulated supermarket refrigeration systems across France, causing temperatures to rise and food to spoil, while authorities investigate reports of fires and other damage linked to the attack, according to an [article](#) from eSecurity Planet. The Oct. 12 cyberattack targeted refrigeration systems at hundreds of French grocery stores, including locations operated by Intermarché, Netto, Coopérative U, and E. Leclerc. According to [AFP](#), attackers reportedly triggered refrigeration defrost cycles, forcing affected retailers to discard fresh and frozen inventory. "These are the same category of systems that the security industry has been warning about as the next frontier for sabotage attacks," Muhammad Yahya Patel, vCISO and cybersecurity advisor for EMEA at Huntress, told eSecurityPlanet, referring to refrigeration

and other operational technology systems. For cybersecurity teams, the incident highlights how compromised connected equipment can disrupt physical operations, destroy inventory, and pose safety risks without requiring ransomware or data theft.

One of the world's most predictable passwords may have contributed to a data breach involving the personal information of approximately 8.8 million people in Denmark, according to another [article](#) from eSecurity Planet. An individual claiming responsibility for breaching Denmark's Central Register of Persons (CPR) told the Danish newspaper Politiken that they obtained a leaked password belonging to a former employee of a Danish company. Separately, according to The Register's Oct. 13 [report](#), Politiken reported that at least three Pays ApS accounts, including an administrator account, used the password "123456." Danish authorities have confirmed unauthorized access to the registry but have not publicly established that the weak password was the initial entry point. New reporting also suggests the alleged attacker used AI-generated code to automate the retrieval of personal information, raising concerns about third-party security, privileged account protection, and the monitoring of suspicious database activity.





Image by [Gerd Altmann](#) from [Pixabay](#)

Microsoft's October Patch Tuesday addressed 1,413 vulnerabilities, according to CrowdStrike's analysis, including 75 Critical flaws and a Windows zero-day already being exploited by attackers, says an [article](#) from TechRepublic. Released Oct. 13, the updates address security weaknesses across Windows, Office, .NET, and other Microsoft products. The release includes three zero-days: one actively exploited vulnerability and two others that were publicly disclosed before fixes became available. For IT administrators, the immediate priority is the Windows Shell vulnerability that was exploited. But the enormous release also creates a broader challenge: identifying the most dangerous flaws while managing updates across enterprise environments.

Security-wise, most browsers are an open door, happy to reveal your screen size, operating system, language preferences, or GPU model when a website asks. **But telling those websites**

to stop selling your data to third parties is still more confusing than it should be, according to an [article](#) from Lifehacker. Although about a dozen U.S. states—including California, Delaware, New Jersey, and Texas—now require businesses to honor consumers' privacy preferences online, most browsers do not offer a native opt-out option that lets you signal those preferences by default. Now, the [California Opt Me Out Act](#), which goes into effect on Jan 1, 2027, is making it mandatory for browsers to do so. Still, for now, native support for a **global privacy opt-out** remains inconsistent among web browsers. Some privacy-forward browsers like Brave, DuckDuckGo, and Mozilla Firefox enable this feature by default, while others, like Chrome or Edge, require you to install third-party extensions such as the EFF Privacy Badger. Since coverage and setup vary wildly, I'll walk you through the exact steps to enable this feature on every major browser.

Your phone number is the skeleton key to your digital life, and carriers have spent years handing out copies to anyone with a decent script. Resetting a bank password, recovering an email account, approving a crypto withdrawal: All of it can run through a text message sent to a number that a call-center rep can reassign in minutes. **The good news is that all three major U.S. carriers now let you lock your number with a toggle,** according to an [article](#) from Lifehacker. This article describes how the attacks work and where to find each switch.



ICYMI: Free Cloud Storage!



The US government is moving to remove DeepSeek from federal civilian IT systems, citing concerns that the Chinese AI company's technology could expose sensitive information and create security risks, according to an [article](#) from TechRepublic. The Department of Homeland Security (DHS) has ordered federal civilian agencies to remove DeepSeek products from their IT systems and prohibited purchases of the company's technology. According to the DHS notice, the restrictions also extend to certain third-party products and services incorporating DeepSeek technology, potentially affecting federal agencies and vendors that rely on the company's AI models.

On 20 October 2026, the PHP project announced an upcoming security release addressing two critical vulnerabilities in

PHP, according to an [advisory](#) posted by CERT-EU. Public reports indicated that these vulnerabilities could lead to remote code execution. The PHP team released the fixes on 21 October 2026 at 13:30 UTC, in PHP versions 8.5.12, 8.4.27, 8.3.36 and 8.2.35 [4]. Both vulnerabilities can allow **unauthenticated remote code execution**. Technical details are now being discussed publicly, and initial proofs of concept (PoCs) have begun to circulate. This raises the likelihood that attackers are already exploiting the vulnerabilities. CERT-EU advises organisations to patch affected assets immediately. Where that is not feasible, organisations should consider isolating internet-facing applications from public networks until a fix is applied and verified. You can also read more about the newly discovered PHP vulnerabilities here, from this [article](#) from The Guardian. (PCLinuxOS already has the patches).

Google said it's rolling out improved safeguards in its Chrome browser to secure users against ClickFix attacks when Enhanced Protection is enabled, according to an [article](#) from The Hacker News. [ClickFix](#) is a popular social engineering technique in which bad actors trick users into copying and pasting malicious code directly into their computer's operating system, thereby bypassing conventional security controls. As part of these attacks, unsuspecting users who land on legitimate-but-compromised sites or click on malicious ads are redirected to phishing landing pages that display fake Cloudflare or Google reCAPTCHA verification or other non-existent errors and instruct users to copy and paste a

command on the Windows Run dialog (or the Mac Terminal app) to address it. The moment a user presses the Enter key after pasting the command, it triggers a multi-stage infection chain that leads to the deployment of malware, such as information stealers or remote access trojans. In an attempt to blend in with regular activity and evade detection, the commands often make use of living-off-the-land (LotL) tools like PowerShell or cmd.exe to download next-stage payloads.



Turning off tracking on a smart TV may not stop it from communicating with tracking-related servers, according to an [article](#) from eSecurity Planet. Researchers at Northeastern University tested 12 smart TVs from 10 manufacturers and found that some continued sending network traffic associated with automatic content recognition (ACR) even after users opted out. ACR is technology that can identify what people watch on their television screens. The findings raise questions about how reliably smart TV privacy settings work. However, because much of the traffic was encrypted, researchers could not conclusively determine what information was transmitted or whether viewing histories continued to be collected. Opt-out buttons exist to give users

control over whether their smart TVs collect and transmit viewing-related data. However, after running 5,943 experiments, researchers found that some TVs continued sending network traffic consistent with tracking even after users had opted out, raising questions about whether these privacy controls [work as expected](#).

Scientists today say we're just beginning to understand the harm that the tiny bits of plastic we drink, eat and breathe are doing to the human body. **But recently discovered chemical company documents dating back several decades show that industry scientists have long been aware of — and concerned about — the way microplastic particles migrate beyond the gut in animals and humans, depositing in important organs**, according to an [article](#) from the LA Times. And the potential for that knowledge to affect the plastic food packaging industry. Their concern goes back to 1974 and a scientific meeting at a New York City hotel, where a German gastroenterologist presented a scientific paper that showed for the first time that ingested particles like microplastics could infiltrate the rest of the body. His presentation was largely overlooked by the government scientists in attendance but became a point of worried discussion among company scientists. A “horror story” was how one company executive described how that research was received.

Google has been pushing Personal Intelligence to make its AI services useful. Instead of giving you generic answers, Gemini and Google Search can pull information from connected apps, including Gmail and Google Photos, to

better understand what you're asking and provide more relevant responses. **But there's a privacy trade-off.** Google updated its [privacy policy](#) to clarify that it could use information you choose to share with certain Google services to personalize ads, according to an [article](#) from Android Authority. Given how much personal information many of us have in Gmail and Google Photos, it's worth paying attention. Google's privacy policy still says it doesn't use content from Gmail, Drive, or Photos to personalize ads by default. However, an important exception now applies to users who explicitly connect that information to Google services that offer personalized advertising. So, giving Google access to your personal information for smarter recommendations could also lead to more targeted ads, depending on the service and permissions involved.



Screenshot Showcase



Posted by Meemaw, October 5, 2026, running Xfce.

PCLinuxOS Recipe Corner



Johnny Marzetti Casserole

Serves: 6

INGREDIENTS:

cooking spray
8 ounces rotini pasta *or your favorite pasta
1 pound ground beef
½ pound bulk mild Italian sausage
¾ cup chopped onion
¼ cup chopped celery
1 clove garlic, minced
1 tablespoon minced green bell pepper
1 (15 ounce) can tomato sauce
1 (14.4 ounce) can diced tomatoes
2 cups shredded Italian cheese blend
1 ½ cups shredded sharp Cheddar cheese
salt and pepper to taste

DIRECTIONS:

Preheat the oven to 350 degrees F (175 degrees C). Lightly grease a 7x11-inch casserole dish with cooking spray.

Bring a large pot of lightly salted water to a boil. Add rotini and cook until tender yet firm to the bite, 6 to 8 minutes; drain. DO NOT rinse your pasta.

While the pasta is cooking, cook ground beef and sausage in a large skillet over medium-high heat until completely browned and crumbly, 7 to 10 minutes, drain. Add onion, celery, garlic, and bell pepper; cook and stir until vegetables are tender, about 5 minutes. Season with salt and pepper. Remove from the heat and stir in tomato sauce and diced tomatoes. Let cool for 5 minutes.

Spread pasta over the bottom of the prepared baking dish. Sprinkle Italian cheese blend over

rotini, then pour meat sauce over top. Cover the dish with heavy-duty aluminum foil.

Bake in the preheated oven for 45 minutes. Remove the foil and sprinkle Cheddar cheese over the casserole. Continue to bake until Cheddar has melted, about 5 minutes. Rest for 10 minutes before serving.

NUTRITION:

Calories: 790	Carbs: 39	Sodium: 1301mg
Fiber: 3g	Protein: 41g	



Like Us On Facebook!
The PCLinuxOS Magazine
PCLinuxOS Fan Club



Social Media When Elections Are Close: Doing The Impossible Better

by [Corynne McSherry](#)

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons [license](#)

Everyone knows, or should, that perfect (balanced, targeted, transparent, swift and swiftly appealable) content moderation at scale is impossible. That doesn't mean powerful social platforms don't have to try to get at least reasonably close, especially when access to good information can have a profound effect on political participation and speech.

That's why so many people, including the [Meta Oversight Board](#), criticized Meta for suspending a major [political](#) Instagram account for hours during a huge early voting push on October 17; and [for allegedly](#) boosting one candidate in Brazil's recent presidential election. Meta denies deliberate interference in either instance, blaming "[mistakes](#)" in its automated content moderation systems (including AI tools that can't tell the difference between enthusiastic follower engagement and a bot attack).

Mistakes or not, with early voting in the U.S. midterms already underway, these events serve as a stark reminder that all major social media platforms need to have stronger systems in place to ensure that they serve, rather than impede, democratic communication.



This is not inherently an "AI" problem: automated systems can process content at a scale that humans never could, potentially enabling better moderation at scale and alleviating the psychological load on ill-paid moderators whose jobs require them to view incredibly disturbing content. But automated systems also reproduce existing biases, struggle to understand context, and often make mistakes that disproportionately affect journalists, activists, artists, and other vulnerable and marginalized communities. And moderation errors are even more likely when the language is spoken principally by the global majority. In 2020, leaked documents showed that Meta's algorithms incorrectly [deleted](#) nonviolent

Arabic-language content 77 percent of the time, while [failing to detect](#) hate speech under the company's own policies in many instances. Where these systems are faltering in Arabic, they're positively failing in less-resourced languages. As a [2025 report](#) from the Center for Democracy and Technology found, labeled datasets in certain languages and dialects such as Maghrebi Arabic and Kiswahili contain inconsistencies, bias, and inaccuracies due to the limited hiring of annotators who actually speak the languages as well as shifts in the languages themselves. An [investigation](#) into ChatGPT's outputs in several low-resource languages demonstrates the depth of the problem.

But language disparities are just one of several concerns as automated moderation becomes more widespread. From the [systemic suppression](#) of content from Palestine to the repeated [misclassification](#) of LGBTQ+ content as adult or explicit material, these varied examples demonstrate the risks of overreliance on automated moderation—and the need for stronger safeguards.

Fortunately, there is a great deal companies, policymakers, and civil society can do to help ensure that highly automated systems operate in ways that respect human rights, minimize predictable harms, and provide meaningful accountability when they fail. If companies are going to continue relying on automation to moderate users' speech — and there is little reason to believe they won't — then accountability must evolve alongside these technologies.

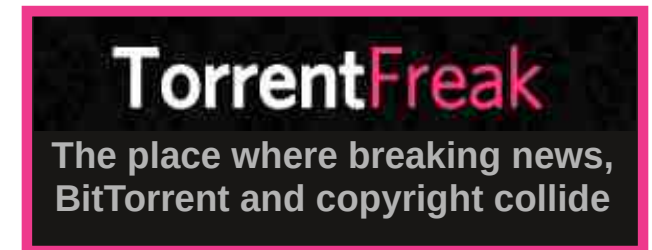
That work should start with publicly committing to the [Santa Clara Principles 2.0](#). Specifically:

1. Automated technologies should help, not replace, human moderators. For example, automated systems can help flag and prioritize content for review, while humans can interpret context, handle sensitive cases, and refine system performance. [This](#) investment is particularly important during the weeks immediately before and after an election.
2. Companies must be transparent about when and how automation is used in content decisions.
3. Companies must regularly audit their automated systems for bias, with particular attention to low-resource languages, vulnerable and marginalized communities, and conflict zones.
4. Companies should [strengthen](#) personal data protection guarantees and policies. Automated content moderation often relies on personal data and profiling, so companies should think carefully about what data these systems use, what's necessary and proportionate and how their systems shape moderation outcomes.
5. Users must have the ability to appeal, and to provide context when they believe human or automated moderation decisions have wrongfully removed their content. Appeals should be promptly evaluated and decided by human moderators.
6. Companies should regularly assess the human rights impact of their moderation decisions, and issue public statements of the results.
7. If they rely on third-party vendors, companies should carefully (and regularly) audit those vendors for compliance with these same principles.
8. Lawmakers should avoid promoting and passing legislation that effectively or explicitly mandates automated moderation systems.
9. Policymakers should also refrain from attempting to dictate platforms technical and design choices to favor or disfavor particular expressions.

10. Policymakers should work to educate the public about how their personal data may be collected and used in electoral contexts.

These recommendations understand that automated content moderation isn't just a technical problem for clever engineers and product teams to solve. Because content moderation shapes public discourse and fundamental rights, its design and oversight must respond to the concerns of policymakers, civil society, independent researchers, and the communities most affected by these systems.

One other distinct and enduring problem makes transparency, checks, and accountability all the more urgent: too few companies have far too much power over our political communication and organizing. Social media gave people the ability to wrest some control over political messaging away from media oligopolies. But we've met the new boss and while it's not the same as the old boss, the song is pretty familiar. The real promise of the web to democratize communication is not likely to be met by social media oligarchs, no matter how sophisticated their content moderation practice.



PCLinuxOS

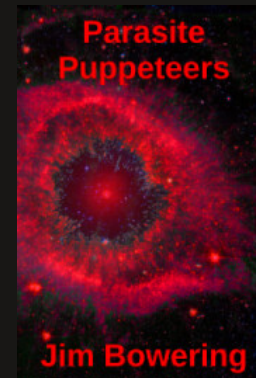
Users Don't
Text
Phone
Web Surf
Facebook
Tweet
Instagram
Video
Take Pictures
Email
Chat
While Driving.

Put Down Your
Phone & Arrive
Alive.

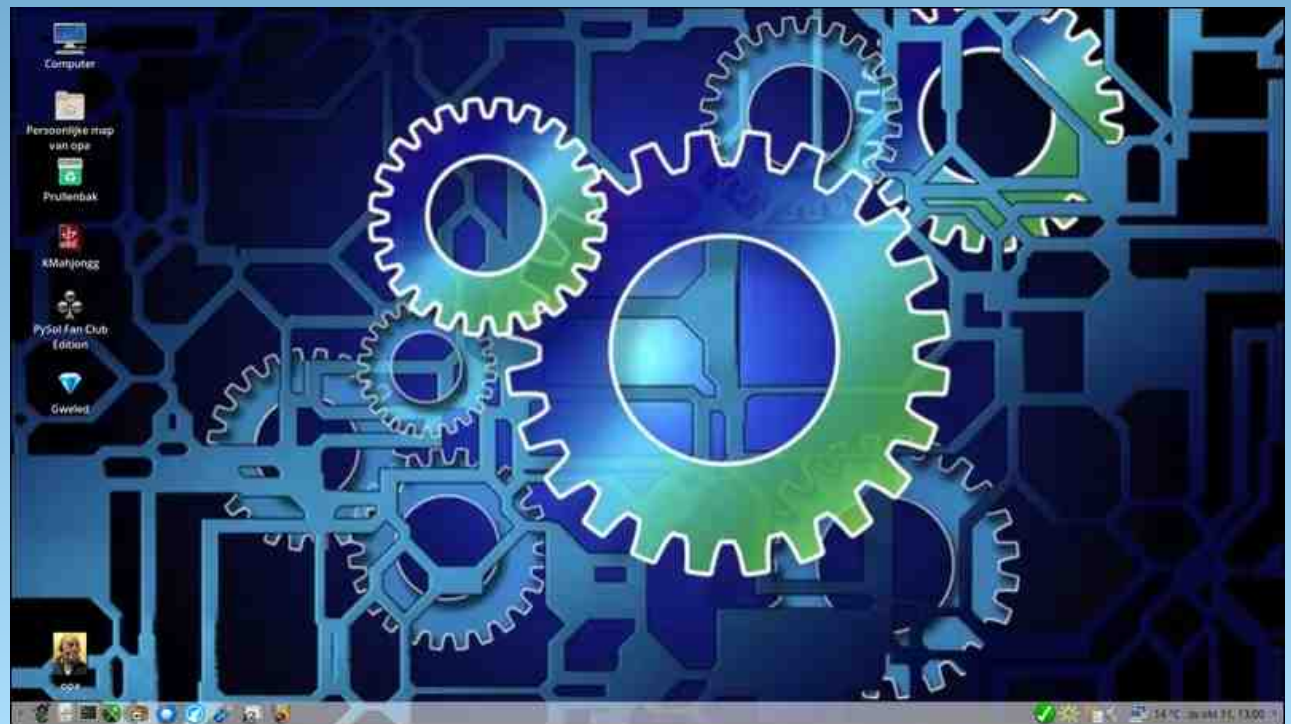
FREE!

*Original SciFi Books
By PCLinuxOS's
Own arjaybe!*

Download Today!



Screenshot Showcase



Posted by mutse, October 11, 2026, running Mate.

GIMP Tutorial: Create A Simple Logo

by Meemaw

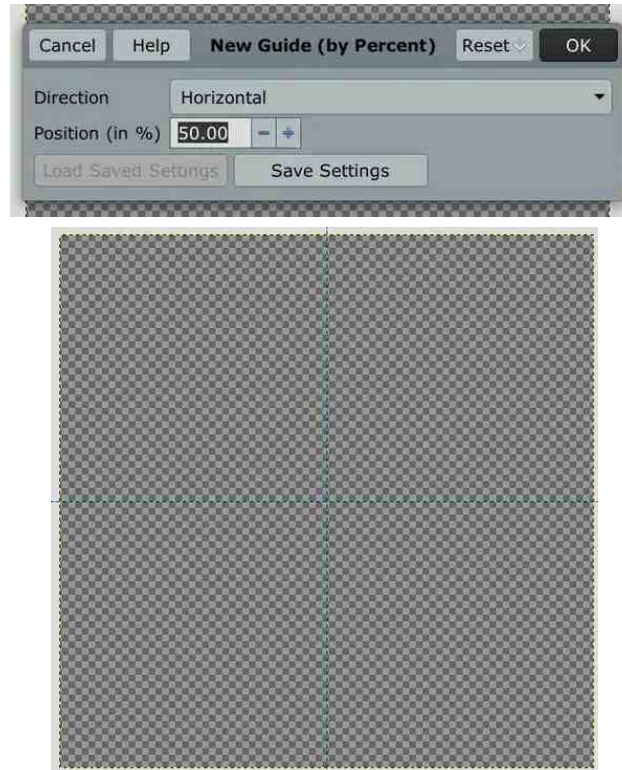


Yes, I know we've done a couple of logo tutorials this year, but they have both used Inkscape ([one](#) of them just last month). If you are more comfortable with GIMP, we can use it, too.

I watched a [tutorial](#) from [Logos by Nick](#) for this one. I simplified it a tiny bit, but it works well anyway.

Open GIMP and create a new project. Mine's going to be square rather than rectangular, so I configured it as a square canvas measuring 1280 x 1280. Make sure it's filled with **Transparency**.

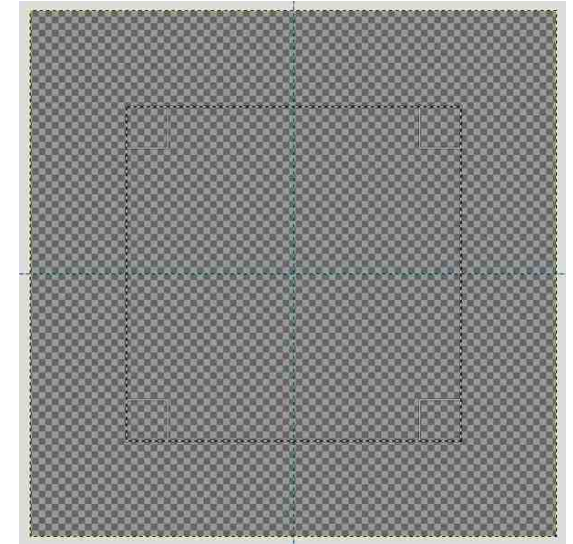
The first thing to do is add some guides to help square things up. Go to **Image > Guides > New guide by percent**. You want two – 50% horizontal and 50% vertical.



You can see them on the canvas. Also check **View > Snap to guides**. This should be checked by default, but make sure.

Now we'll put in our border. Start with the rectangle tool. Starting in the center of the canvas (where the guides cross), drag toward a corner, holding down <CTRL> + Shift to lock the square's sides as all the same (top, right).

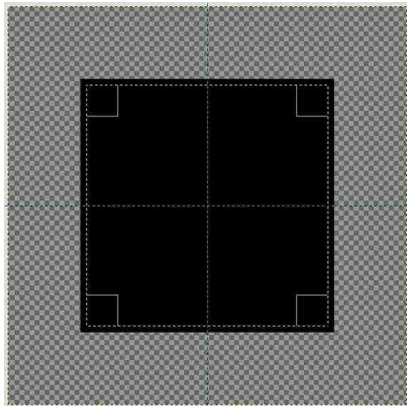
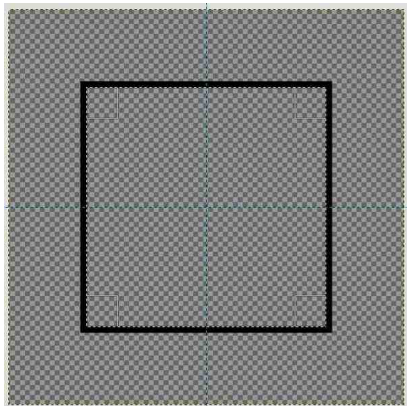
Next, go to **Edit > Fill with FG color**. This will be a black & white logo, so I made sure my



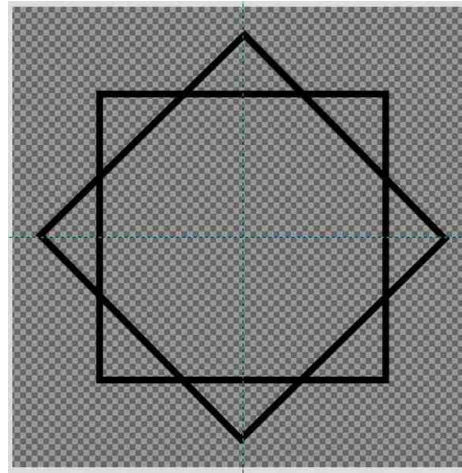
colors were the default black (FG) and white (BG).



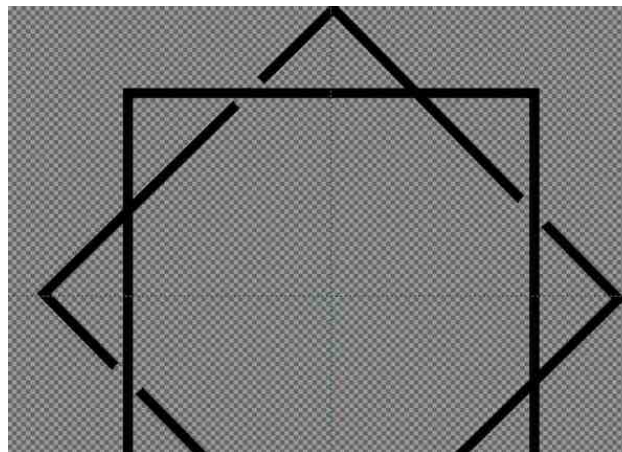
Now you need to go to **Select > None**. We'll make another square on the same layer. This one needs to be a bit smaller than the first. Press the **Delete** key and you'll get an outline. Choose **Select > None** again.



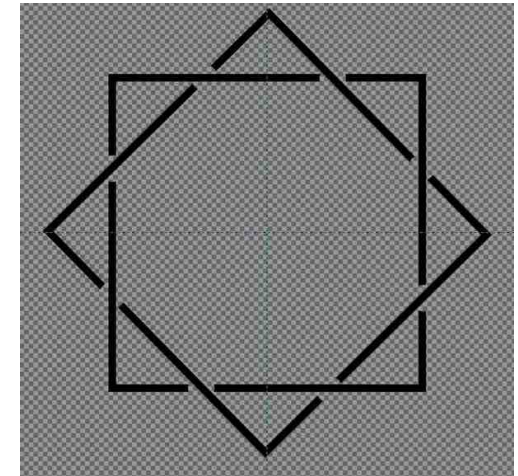
I decided to make another square. You can create another layer and follow the same steps as above, or you can just duplicate the layer in the layers dialog. I chose to duplicate the layer. Now I'm going to rotate the new layer 90° on the canvas. Open the rotate tool and rotate your square (center, top).



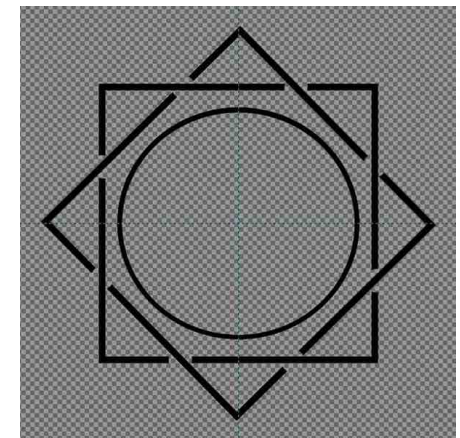
Now I want to make the squares look like they are intertwined. Zoom in, and choose the Eraser tool. We're going to erase selected parts of each square. Some will be on one layer and the others will be on the other layer. Choose a layer and erase four parts of the lines intersecting the other layer's square, then choose the other layer and do the same thing with the other four. Here's my first step:



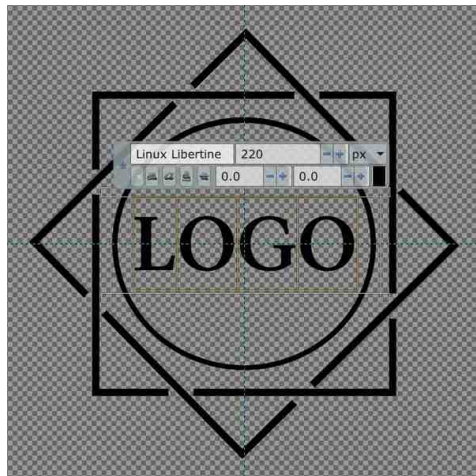
Notice that the ones erased are on corresponding sections of the square. Then I'll choose the other layer and do the same with the other intersections, so it looks like this:



I'm going to add a circle inside this square arrangement. Create another transparent layer and use the ellipse tool, holding down <CTRL> + Shift to make it a perfect circle. Do the same steps as on the squares - fill with FG color - choose **Select > None**, then create another circle and press **Delete**.



Now let's add some text. I'm sure you know how to do this. Choose the text tool and select the font you want to use. I used Linux Libertine Bold, with the size at 220px. I just wrote "LOGO", but you should use the word you need and in the size you want. For a smaller word, above LOGO I used the same font, but with a smaller size. You can use the Alignment tool to center your font where you want it. It should still snap to the guides.



When you have what you want, you can export it to an image. Make sure you use an image format that supports image transparency, like PNG, WEBP, or AVIF. The last two also save images in significantly smaller file sizes. The one at center top is the result I got the second time.



**Looking for an old article?
Can't find what you want?
Try the PCLinuxOS
Magazine's searchable
index!**

The **PCLinuxOS** magazine

Screenshot Showcase



Posted by tbs, October 28, 2026, running KDE.

Lessons Learned From 'AdFection' & What To Do Next

by [Bill Budington](#) and [Thorin Klosowski](#)
Electronic Frontier Foundation
Reprinted under Creative Commons [license](#)

In the last half of October, researchers at Citizen Lab [revealed](#) a horrifying new malware campaign, dubbed “AdFection.” It used an ad network to distribute spyware to journalist’s devices to infect them without the target ever needing to click anything. This sort of attack on journalists is dangerous and incredibly concerning, especially since it’s built on the backbone of a technology we already object to: [behavioral advertising](#). Although this type of attack has only been described targeting journalists, you can take a few steps we outline in the next section to mitigate the risk no matter who you are.

A few factors combined to make this attack a noteworthy first-of-its-kind. First, it utilized the surveillance ad-tech ecosystem to specially target the malicious code. Second, the spyware it delivered was so-called “zero-click,” meaning it required no interaction from the user to be infected: all that is required is for the ad to be delivered and code bundled along with it to be run, which happens automatically. Neither [malvertising](#) nor [zero-click attacks](#) are new on their own. What’s novel about the AdFection attack is combining them, creating a highly targeted, extremely dangerous attack which is



difficult to defend against and even harder to detect.

Let’s take a deeper look from the perspective of one of the Windows devices supplied to the researchers from Al Jazeera. Here’s how the report describes the infection happening:

- Someone browsing the web or using an app on that machine is served an ad created by Discover-Tech, a company exposed in the report

as “purporting to be a legitimate advertising company, [but] appears to be a front for large-scale ad espionage abuse.”

- The ad contains a small snippet of JavaScript code which is automatically executed when rendered in the app or website.
- This code reaches back out to a Discover-Tech server, referred to as their “NOAS server,” with detailed information about the machine



rendering it: its cookie-set advertising ID, IP address, and more.

So far, nothing particularly unusual has happened. Ads that contain JavaScript code and reach back out to their servers with lots of information on your device—and by extension you—are commonplace. It's all part of the data-driven advertising ecosystem. What happens next is more interesting:

- The NOAS server uses this detailed information to determine it is an Al Jazeera machine requesting the ad.
- Instead of returning an empty response (as it does most of the time), it responds with a malicious, zero-click spyware [payload](#). That payload was created by Discover-Tech's partner Candiru/Integrity Labs, a company [previously exposed](#) for involvement in sophisticated malware attacks.
- The payload is then executed and infects the targeted machine.

Companies targeting zero-click malware attacks against journalists might seem like the plot of a blockbuster spy thriller. But this attack was enabled by the everyday practices of ad-tech companies, which unfortunately have extreme latitude in the collection of users' data. By leveraging the tracking identifiers and data collected on devices for the purpose of delivering targeted ads to specific individuals, mercenary spyware companies can repurpose this data in order to fine-tune who they infect —

and hide that they're doing it from everyone else.

Most ads are not delivered directly by the ad creators, but rather by intermediaries that [facilitate Real-Time Bidding auctions](#). Nonetheless, winning bidders are given the ability to execute JavaScript code in the browser of the person who receives the targeted ad. This allows for interactive ads to be displayed, but also (as we've seen) for the compromise of a device just by delivery of malicious code.

While the different components in this [attack chain](#) are not novel on their own, the exposure of this combined attack is significant because it reveals a technique to hyper-target individuals and organizations for infection. Luckily, there are steps you can take to protect yourself from the [myriad of dangers presented by](#) the ad-tracking industry. Here's how.

What You Can Do About It

As we work towards fundamental fixes to the ad ecosystem and banning online behavioral ads altogether, the onus is on all of us to protect ourselves. This is especially important for higher risk individuals or journalists working in states with heavy surveillance. Citizen Lab [outlines](#) several steps, depending on your threat model, to take to help protect yourself:

- Take some simple steps to [lock down](#) your devices right now.

- Establish [strong security fundamentals](#). Sites like our own [Surveillance Self-Defense](#) and [Consumer Reports' Security Planner](#) can help get you started.

- Use a browser extension to reduce tracking. Our [Privacy Badger](#) extension is an excellent start. Network-wide ad blocking services are also worth considering if you're comfortable handling the set-up process.

- On mobile phones, disable or reset your AD ID. Here are directions to do so for [Android](#) and [iPhone](#).

- Consider using more [privacy protective browsers](#).

These steps can be very helpful in protecting yourself, but there is only so much you can do as an individual. [Banning behavioral ads](#) like this would be a good place to start. Behavioral ads aren't just a privacy nightmare as designed. They are the perfect vehicle for malvertising and similar threats, just as we see here.

***Looking for an old article?
Can't find what you want?***

***Try the PCLinuxOS Magazine's
searchable index!***

The **PCLinuxOS** magazine

AI Is Finally Helping The People

by Alessandro Ebersol (Agent Smith)

AI Helping the populace? Who would have thought ...



In early October 2026, the world of proprietary audio, video, graphics, text, and office applications was shaken by the public launch of the Artcraft suite.

What the Artcraft suite is and how it revolutionizes the relationship between consumers and (mega) corporations—which abuse their economic power—is what we will explore next.

Artcraft is a suite of applications created by Brandon Thomas. The project officially began on July 14, 2025, on GitHub, with its first version, 001, released on that date.

Brandon, aided by Anthropic's generative AI Claude Opus 3.5, created clones of several well-known applications, starting with the Adobe suite. As of the time of this writing, the collection already includes 13 applications, namely:

PhotoCraft: The image editor you already know how to use. Photoshop clone.

VectorCraft: Vector illustration. Illustrator clone.

FilmCraft: Movie and video editing. Adobe Premiere clone.

LightCraft: Digital photography non-destructive developer software. Lightroom clone.

PdfCraft: PDF editor, an Acrobat Reader clone.

EffectCraft: Video compositing and effects designer, clone of Adobe After Effects.

DesignCraft: Page layout and publishing, clone of Adobe Indesign.

FigCraft: Interface design editor, clone of Adobe XD.

WordCraft: Text editor, clone of Microsoft Word.

SoundCraft: Audio and track editing, clone of Adobe Audition.

DeckCraft: Slide presentations and editing, clone of Microsoft Power Point.

ARTCRAFT

Capable tools *for artists.*

ArtCraft builds open source tools for artists. We
pride ourselves on freedom of control and
expression.

CADCraft: Computer-aided design and drafting, clone of Autodesk Autocad.

GridCraft: Spreadsheets editor, clone of Microsoft Excel.



Brandon Thomas created these open-source clones out of frustration with **Adobe's** abusive practices. His main reasons were:

- Cancellation “dark patterns”: He has repeatedly been harmed by deceptive design techniques that make it difficult to cancel subscriptions.
- Control over content: The outrage over Adobe’s policies — which force users to accept new terms of service, granting the company the right to access private files and session data for AI training with no opt-out option — was a decisive factor, and take special note of this point: Adobe deliberately trains its AI using content created by its customers, who have paid for the Adobe suite, and yet they end up paying to train Adobe’s AI with their own work.



- Subscription model: The shift from software that users were supposed to “own” to subscription-based models — with constant price increases and exorbitant fees — also motivated the initiative.

After usable versions were posted on GitHub, the project gained more contributors, who are committed to the project, leading to several daily releases of the Artcraft suite.

Dark Patterns: Corporate Trickery



Dark patterns are interface design choices deliberately created to manipulate users and lead them to make decisions they would not make if they had clear information or if the process were simple.

These techniques are often used by companies to create intentional obstacles, such as making it difficult to cancel a subscription or service. A common example cited is when a website or app changes the layout,



colors, or placement of “cancel” and “keep subscription” buttons to confuse the user when they try to leave the platform.

Key features:

- **Intentionality:** Unlike a design flaw, a dark pattern is deliberately designed to benefit the company at the expense of the user's interests.
- **Manipulation:** Uses knowledge of human behavior to lead the user to take a specific action, such as making an unwanted purchase or accepting terms without reading them.
- **Barrier-creators:** In subscription contexts, they are known for making it very easy to sign up but extremely bureaucratic or confusing to cancel—a practice often referred to as a “Roach Motel” (or “easy to get in, impossible to get out”).

But despite Brandon and his team's genius, they might get into trouble.

The Risks for Brandon Thomas



Brandon Thomas's project faces several complex legal risks as it seeks to recreate Adobe software; the main challenges include:

- **DMCA (Section 1201):** The law prohibits the circumvention of “technological measures” that protect access to copyrighted works. Companies often use this section to sue developers who engage in reverse engineering, although there are legal exceptions for interoperability purposes.
- **Terms of Service (EULAs):** End-user license agreements (EULAs) often contain clauses that explicitly prohibit reverse engineering, decompilation, or attempts to recreate the functionality of the original software. In some cases, courts have upheld these contractual restrictions.
- **Copyright and User Interface:** There is a risk of allegations that the clone reproduces elements protected by copyright law, such as the user interface or specific menu hierarchies. Although cases such as Google v. Oracle have established limits on the protection of APIs, Adobe could attempt to seek protection for visual and design elements.
- **Lobbying and Legislative Changes:** According to Louis Rossmann (a consumer rights activist), the greatest risk is not just the current law, but the possibility that large companies will push for reforms (such as compulsory licenses or broader software patents) to raise barriers against open-source alternatives.

To mitigate these risks, developers often use the “clean room” strategy (clean room design), in which the team analyzing the original software is isolated from the team writing the new code, in an effort to ensure that only public features and specifications are used, without copying the original source code.

However, there are legal provisions that cover what Brandon is doing, and they relate to fair use.



Fair Use in Reverse Engineering



Despite the risks Brandon and his team face, U.S. law — specifically Section 1201 of the DMCA — permits reverse engineering under certain specific conditions. The legislation authorizes anyone who has the legal right to use a program to circumvent digital locks for the sole purpose of identifying and analyzing components necessary for interoperability between independently created programs. Now, porting the Adobe suite to Linux has long been a demand from the entire community, and now, thanks to Brandon Thomas's work, it achieves what Adobe never wanted to do—but, as far as we can tell, it would be entirely possible. Adobe simply did not do it due to collusion (with Microsoft/Apple) and market monopolization. And this reason—creating a clone that works on Linux—could legitimize the entire Artcraft suite.

Furthermore, there are several important legal precedents, such as the *Sega v. Accolade* case, where the court ruled that decompiling software can be considered “fair use” when it is the only way to access a program's ideas and functional elements for a legitimate reason.

Although caught off guard, Adobe may fight back and launch a very strong counterattack.

What Adobe Can Do



It is quite plausible that Adobe and other software companies will push for legislative changes to curb the emergence of open-source clones. These clones erode the market “moat” that protects Adobe's business model, so the company may seek to:

- Lobbying for stricter software patent laws: An attempt to eliminate judicial limits on the patentability of abstract ideas, citing the “Patent Eligibility Restoration Act of 2025.”
- Compulsory licensing: The creation of a model in which, even if developers are able to create alternatives, they would be required to pay royalties to the original company, similar to what happens in the music industry.
- DMCA Reforms Through International Treaties: The use of organizations such as WIPO to circumvent the U.S. Congress by creating more restrictive laws that protect their “digital locks.”



Adobe's Blatant Hypocrisy



The company's current situation clearly constitutes a case of double standards, creating a significant imbalance between Adobe's corporate power and user rights.

The conflict of interest:

1. Content Use for AI: Adobe has updated its terms to allow access to users' private files and session data (through both manual and automated means) for the purpose of training its artificial intelligence models. The most critical issue is that the company did not offer an opt-out option, forcing users to accept the new rules or risk losing access to their own work.

2. Protection against competition: At the same time, Adobe uses provisions in its Terms of Service (specifically Section 17b) to expressly prohibit



PCLinuxOS Magazine Graphics Special Edition, Volumes 1 - 4
Unleash your GIMP & Inkscape skills. Over 160 tutorials. Grab your FREE copy now!

users or third parties from reverse engineering or creating alternatives (clones) to its software.

Why it's unfair:

- Permission asymmetry: Adobe claims the right to use others' work to improve its products (via AI), but denies consumers the right to analyze or recreate systems to ensure interoperability or avoid abusive practices.
- Ecosystem lock-in: It can be argued that these practices create an artificial "moat" around the brand, preventing free competition and keeping users locked into expensive subscriptions and hidden cancellation fees.

Brandon Thomas's effort to use AI to create open-source clones is a heroic response to this system, representing an attempt to restore balance in a



market where copyright laws and contractual policies are being distorted in favor of corporate profit rather than consumer freedom.

But wait, there's more ... Not only was Adobe software re-created — and in Rust (of all languages) — but the PlayStation 5 was also jailbroken, using artificial intelligence.

Sony and PS5 Jailbreak



The PlayStation 5 was recently jailbroken, and this development has incredible implications for PlayStation 5 owners.

Thanks to the jailbreak, the PS5's capabilities have increased exponentially:

- Access to game libraries: With the jailbreak, it's now possible to access stores where users can get PSN items for free and play a huge variety of games from different platforms: Nintendo Switch, Xbox, and many other consoles can now be emulated on the PS5.
- Emulation and compatibility: It has been demonstrated that a jailbroken PS5 can run original PS2 discs and even emulators for the PS3 and other

systems, defying Sony's policy of limiting access to older titles through streaming services.

- Moral and technological reflection: This is not just about piracy, but about technology's natural response to the erosion of consumer rights regarding digital products. This trend is a way to rebalance the "pendulum" between companies and users.

But how did AI help jailbreak the PS5?



Artificial Intelligence didn't magically "break" the PlayStation 5, but it acted as a catalyst for manual labor that was already possible before. The process unfolded as follows:

- Reverse Engineering Optimization: The technique of reverse engineering for game consoles has been around for decades. AI helps by automating repetitive and tedious tasks, such as analyzing binaries, trial and error on specific functions, and code mapping, thereby speeding up what would otherwise be a much slower process for humans.
- PC-based: The PlayStation 5 has an architecture very similar to that of a standard computer (PC). Much of the work involved in "unlocking" or

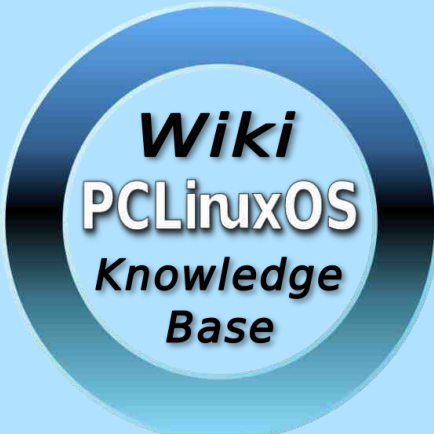
porting games involves remapping calls from Sony's proprietary systems to universal libraries, such as Vulkan.

- **Task Completion:** About 90% of the work (such as shader translation and CPU adaptation) had already been technologically solved by emulation communities years ago. AI helped solve the “last 10%”—or rather, the remaining 5%—of the complexity required to integrate these solutions into the console's specific hardware.

But why did an entire community rally around jailbreaking the PlayStation 5? A simple, straightforward answer: FAFO, Sony.

Sony did not include backward compatibility — which had been a tradition since the PlayStation 2 — and promised to do away with physical discs, leaving users dependent on its online store as the only way to access their games. And, by the way, Sony doesn't have a good track record with its online store, having deleted 550 movies that were legally purchased by its customers. And most of those customers weren't reimbursed — a low move for a corporation like Sony (or maybe not; Sony has always been a scoundrel, ever since 2005, when it infected millions of CDs with rootkits).

Now, the PS5 runs all games from previous generations, plays discs and emulators, and even has a “pirate” online store with free games. Don't even get me started on payback ...



**Visit.
Contribute.
Build.**

**The PCLinuxOS
Wiki**

It Belongs To YOU!

The 2-Ton AI Elephant in the Room



What we're witnessing is the result of the backlash of the consumers, based on years of neglect, and greed of large corporations. The bad deeds of the Big Techs are coming back to haunt them.

From Adobe's well-deserved downfall — it had already been losing ground to Canva, a great online, cross-platform service with integrated AI that generates professional-quality graphic designs — through the successive price hikes for the Adobe suite, its refusal to release its apps for Linux (something its customers had been asking for on the Adobe forum for AGES), its draconian policies regarding terms of service — which now force customers to let Adobe train its AI using users' work, for free, created with the suite they paid for — It's almost as if every one of the company's customers is paying to train Adobe's AI. And let's not forget to mention Sony, which has fallen out of favor with its customers and consumers after a succession of abuses, negligence, and unprecedented greed.

But all these events, which are happening almost simultaneously (and the situation is so fast-paced that if you blink, you'll miss what's going on), have their roots in two things: copyright laws being abused by large corporations, and the disregard and negligence with which these large

companies treat their paying customers, since these companies have gone from being legitimate businesses to extorting their users.

Copyright laws should have been reformed by now, but with corporations like Disney lobbying to extend copyright protection to nearly 100 years, what chance do we have of having laws that are fairer and reflect the current reality? And, even worse, now with AI, no one will be able to claim intellectual property rights anymore, since training AI systems with copyrighted material will allow them to create derivative works with no connection to the originals. But now, ordinary people are fighting back and pushing back—and they're also using artificial intelligence to their advantage. After all, if the big techs can do it, why can't the average Joe?

However, this trend of using AI for the benefit of users could trigger an unprecedented backlash from large corporations, leading them to finally regulate AI.

Well, it will be very interesting to see the mental gymnastics Adobe's lawyers perform as they try to criminalize AI in court, while at the same time the company exploits its users' work, and they have no option but to comply, or risk losing access to their own work.

But since President Trump himself has said he won't regulate AI — that he'll encourage its use and development — only the future will tell what will happen. Still, it's satisfying to see AI helping ordinary people, for a change.

This article was written with the help of AI ... for a change.



The PCLinuxOS Magazine

Created with Scribus

The PCLinuxOS Magazine Special Editions!



Get Your Free Copies Today!

Require Police To Get A Warrant To Search ALPR Data

by [Adam Schwartz](#)

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons [license](#)

This article was co-written by [Andi Cao](#), an EFF legal intern.

Automated license plate readers (ALPRs) are mass surveillance. They photograph every passing car and log where and when it was captured, building a searchable record of where nearly everyone drives. Cities should [not buy them](#), and cities that already have them should shut them down.

Where these systems still operate, courts and state legislatures must reduce their harms by (among other things) requiring police to get a warrant before searching stored ALPR data. A warrant requirement would not make mass surveillance acceptable, but it would require police to justify a search to a judge before accessing records of people's movements. Without this independent judicial check on police power, officers have been searching this data for improper reasons (many exposed by EFF) that violate our fundamental rights.

A warrant requires a judge to find probable cause and specificity—many warrantless police searches of ALPR data lack both. Officers have searched this data to profile Romani people,



monitor protesters, investigate an abortion, find immigrants for deportation, track a man who complained about a deputy, stalk romantic partners, and even for no stated reason beyond “LMAO.” A warrant requirement would force law enforcement to justify these searches before accessing sensitive location records, not leave the people they target to discover and challenge the abuse after the harm is done.

What a Warrant Requires

Warrants are a check on police power. Before officers can search a person or their property,

the [Fourth Amendment](#) requires them to convince a neutral judge, under oath, that probable cause exists, meaning a fair probability the search will turn up evidence of a crime. The warrant must also describe with particularity what will be searched, so police cannot go on a fishing expedition. Critically, the officer who wants to search is not the person who decides whether the search is justified.

That is why warrants are required for so many kinds of police surveillance. For example, police generally need a warrant to [wiretap phone calls](#), to [search the contents](#) of a cell phone, and to obtain historical cell phone [location records](#).

Stored ALPR data reveals sensitive information about the private details of our lives: where we go, when, and with whom. That's why we believe police searches of stored ALPR data should also require a warrant. Earlier this month, a federal judge in Oklahoma [agreed](#).

What Goes Wrong Without a Warrant: San Jose, California

San Jose demonstrates the harmful consequences of letting law enforcement search stored ALPR data without a warrant. EFF and the ACLU of Northern California represent SIREN and CAIR-California in a [lawsuit](#) challenging this practice.

The first problem is the sheer number of times that SJPD officers search stored ALPR data: [261,711 times](#) between June 5, 2024, and June 17, 2025, about 692 searches a day. That scale is the result of having no warrant requirement, which would greatly reduce this kind of casual police surveillance.

Inevitably, officers abuse this unchecked power. In September, San Jose's police chief [disclosed](#) an example from five months earlier: the department had fired an officer who used its ALPR system to track a woman who had accused his cousin of domestic violence, and then shared her location information with his cousin. The abusive search of stored ALPR data [came to light](#) only after the woman told police that her alleged assailant had implied he was tracking her. A warrant requirement would have prevented this.

Of course, similar problems appear nationwide. For each example below, consider how things could have turned out differently if the officer had to put the reason for the search in a sworn warrant application and handed it to a judge.

Racial profiling of Romani people

More than 80 law enforcement agencies [searched the Flock network](#) using terms that unfairly stereotype Romani people, often without mentioning any crime. For example, the Grand Prairie (Texas) Police Department searched for "g*psy" six times using a Flock feature that identifies vehicles traveling together, in effect targeting a whole community without naming a crime.

No judge should sign that warrant. Ethnicity is not evidence of a crime, and a search aimed at an entire ethnic group is the opposite of particular: it targets people for who they are, not evidence that they committed a crime.

Surveillance of protesters

EFF found that more than 50 agencies ran hundreds of [protest-related searches](#) of ALPR data in 2025. For example, the Tempe (Arizona) Police Department ran three searches tied to the No Kings protest across 425 networks, with no identified crime.

This lacks probable cause and targets activity that is protected by the First Amendment.

Investigating an abortion

In 2025, a Texas sheriff's office searched more than [83,000 Flock cameras](#), including cameras in Washington and Illinois, where abortion is legal, listing the reason as "had an abortion, search for female." [Records](#) later obtained by EFF show deputies had opened a "death investigation" after the woman's partner, who was later charged in connection with assaulting her, reported her self-managed abortion.

In a state where abortion is legal, a judge would not grant a warrant for a search like this.

Finding immigrants for deportation

San Francisco police let out-of-state agencies search the city's ALPR data (which itself violates [California law](#)), and [at least 19](#) of those searches were marked as related to ICE (though San Francisco is a [sanctuary city](#)). This problem is widespread. One investigation found more than [4,000 cases](#) in which police departments around the country searched stored ALPR data on behalf of federal law enforcement, including for immigration investigations. Some agencies even connect their ALPR systems to an ["Immigration Violator" hotlist](#) populated by ICE, which includes plates tied to administrative warrants issued by ICE agents without any judge involved.

Here too, a judge in a state where police may not help enforce immigration law would not issue a warrant for these searches.

Retaliation against a critic

In May 2025, Navy veteran Napoleon Jones [lawfully recorded](#) a police traffic stop of another person in Sussex, Wisconsin. Jones alleges that a Waukesha County deputy retaliated by stopping and arresting him. He was released five hours later without citations or charges, and the deputy's supervisor concluded the stop was illegal. Jones filed a complaint against the deputy the next day.

In the weeks that followed, officers reportedly ran more than [100 Flock searches](#) against Jones, including some run by the deputy he had complained about. Deputies testified that a lieutenant ordered the searches in connection with Jones's complaint.

No judge should authorize tracking a man for criticizing the police.

Stalking romantic partners

The Institute for Justice (IJ) has documented [dozens of cases](#) in which officers allegedly used ALPRs to track current, potential, and former romantic partners. For example, a Lufkin, Texas, officer was indicted on 100 felony counts after allegedly searching for his ex-girlfriend and people she knew more than 10,000 times. Likewise, a Milwaukee officer allegedly tracked a woman he was dating and her ex nearly 180 times over two months. IJ found that most of these cases surfaced only after victims reported the officer.

We hope that no officer would write "tracking the location of my ex-girlfriend" on a warrant application, and even if they did so, a judge would not authorize such a search.

Searches for "LMAO"

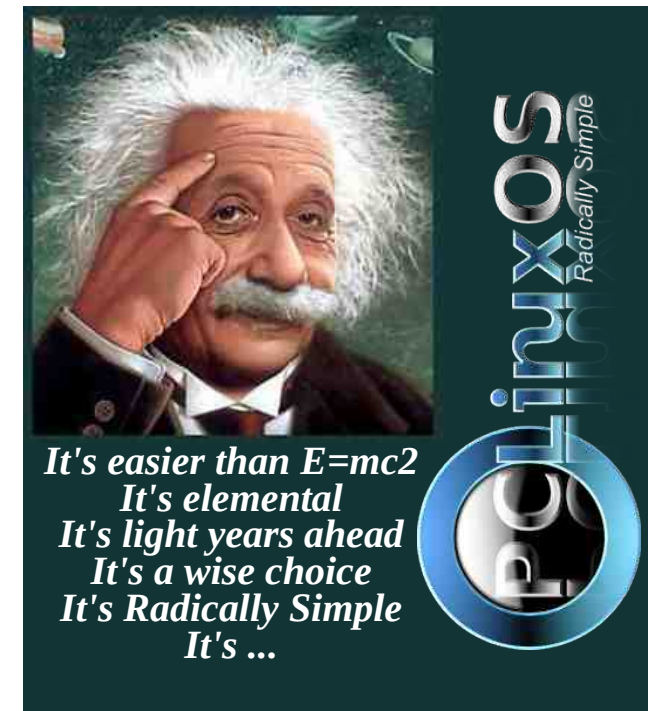
Sometimes officers do not even provide a real reason to search stored ALPR data. EFF found officers [logging](#) search reasons such as "LOL," "LMAO," "idk," and random keyboard mashing. These entries are supposed to document why a search complies with an agency's own use policies. A Goshen (Indiana) Police Department officer searched 6,474 networks, representing data from 82,413 cameras, with "idk" as the reason.

An officer who asked a judge for a warrant to track someone for "LMAO" would be laughed out of the courtroom.

The Solution

The best way to eliminate these abusive searches is to end ALPR mass surveillance. Where these systems remain, however, courts and state legislatures must require police to get a warrant before searching stored ALPR data. Warrants are the time-tested way to put an independent judicial check on police use of a dangerous surveillance technology. Officers must establish probable cause and specifically describe the proposed search before accessing the data, while existing exceptions for genuine emergencies still apply.

These protections must also cover real-time tracking. An ALPR "hotlist" is a list of license plates that trigger an alert when a camera spots a matching plate. Officers can stalk potential romantic partners by putting them on a hotlist, as a Florida deputy [allegedly did](#) with a woman he met on the set of a TV show. Thus, state legislators should require officers to get a warrant before putting a person on an ALPR hotlist (as well as a warrant to search stored ALPR data).



Defending Your Rights



In The Digital World

**PCLinuxOS Magazine
Graphics Special Edition
Volumes 1 - 4**



**Unleash your GIMP & Inkscape Skills.
Over 160 tutorials.
Grab your FREE copy now!**



Like Us On Facebook!
The PCLinuxOS Magazine
PCLinuxOS Fan Club



Screenshot Showcase



Posted by cold sweat, October 7, 2026, running Mate.

Wiki Pick: Automatically Mount A Drive Using /etc/fstab

Relevant to all versions of PCLinuxOS

To automatically mount a drive using `/etc/fstab`, you need to add an entry for it in the `/etc/fstab` file with the correct parameters. Here's how you can do it as the root user.

NOTE: All commands are executed as the **root** user in a **terminal** window.



Image by [MH Rhee](#) from [Pixabay](#)

Step 1: Find the UUID or device path

Run the following command in a terminal window to get the UUID of the drive:

```
blkid
```

Look for the UUID of the partition you want to mount (e.g., `/dev/sda1`).

Step 2: Create a mount point

Decide where you want to mount the drive (e.g., `/mnt/mydrive`) and create that directory if it doesn't already exist:

```
mkdir -p /mnt/mydrive
```

Step 3: Edit `/etc/fstab`

1. Open the `/etc/fstab` file in a text editor with root privileges: `nano /etc/fstab`

2. Add a new line with the following format:

```
UUID=<your-drive-uuid> /mnt/mydrive  
<filesystem-type> <options> 0 0
```

Replace `<your-drive-uuid>` with the UUID you found.

Replace `<filesystem-type>` with the file system type (e.g., `ext4`, `ntfs`, `vfat`).

`<options>` can be something like `defaults` or `noatime`. For NTFS, you might want `ntfs-3g` instead.

Example:

```
UUID=123e4567-e89b-12d3-a456-  
426614174000 /mnt/mydrive ext4 defaults  
0 0
```

Step 4: Test the `/etc/fstab` Entry

You can test if the entry is correct by running:

```
mount -a
```

If there are no errors, the drive should be mounted automatically at the specified mount point on the next reboot.

You can view this tip [here](#), at the PCLinuxOS Knowledgebase Wiki.



Court Should Curb Abuse Of Grand Jury Subpoenas Targeting Social Media Users

by **Mario Trujillo**

Electronic Frontier Foundation

Reprinted under Creative Commons [license](#)

A federal appeals court should curb the government's abuse of grand jury subpoenas to unmask social media users who criticize lawless immigration enforcement.

That is the message from the ACLU, EFF, and other civil liberties and trade groups who filed an [amicus brief](#) in a sealed case in the U.S. Court of Appeals for the District of Columbia.

The [case](#) involves the government's investigation of an anonymous Reddit user who commented on a post about an immigration officer in Minnesota. The Department of Homeland Security (DHS) first issued an administrative subpoena to Reddit to unmask the user. When the user challenged the subpoena in court on free speech and statutory grounds (as [many others](#) have), DHS withdrew it. But then the government obtained a separate grand jury subpoena—a subpoena issued by a prosecutor to gather evidence to present to a grand jury before any criminal charges are filed—for much of the same information. The user then challenged the grand jury subpoena too, and the case is currently being appealed.

The right to speak anonymously is essential. It preserves privacy and shields critics from



government retaliation. In the past year, the Department of Justice (DOJ) has issued grand jury subpoenas to social media companies for their users' personal data. This is frequently done for improper purposes and without really showing that social media users have committed any crime. These subpoenas have the effect of intimidating and chilling critics, as immigration authorities have engaged in [invasive](#), [unconstitutional](#), and sometimes [violent conduct](#).

As the amicus brief makes clear, courts should not defer to the government's claims regarding the legitimacy of using grand jury subpoenas to unmask internet users. Instead, the subpoenas must receive proper First Amendment scrutiny. Like many other types of legal processes, grand jury subpoenas are issued by federal officials without prior court approval. And they too can

be abused to harass or retaliate against people critical of the government.

The amicus brief was filed in early September and recently unsealed. The brief was signed by the American Civil Liberties Union of DC, EFF, the Center for Individual Rights, the Foundation for Individual Rights and Expression, the Cato Institute, and NetChoice.

It is notable that NetChoice signed the amicus brief. It is a trade group that represents many companies who have received similar subpoenas including Reddit, Google, Meta, PayPal, among others. EFF has [called on](#) these companies to do more to defend their users' speech and privacy rights in the face of these subpoenas.



Disclaimer

1. All the contents of the PCLinuxOS Magazine are only for general information and/or use. Such contents do not constitute advice and should not be relied upon in making (or refraining from making) any decision. Any specific advice or replies to queries in any part of the magazine is/are the person opinion of such experts/consultants/persons and are not subscribed to by the PCLinuxOS Magazine.

2. The information in the PCLinuxOS Magazine is provided on an "AS IS" basis, and all warranties, expressed or implied of any kind, regarding any matter pertaining to any information, advice or replies are disclaimed and excluded.

3. The PCLinuxOS Magazine and its associates shall not be liable, at any time, for damages (including, but not limited to, without limitation, damages of any kind) arising in contract, tort or otherwise, from the use of or inability to use the magazine, or any of its contents, or from any action taken (or refrained from being taken) as a result of using the magazine or any such contents or for any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, communications line failure, theft or destruction or unauthorized access to, alteration of, or use of information contained on the magazine.

4. No representations, warranties or guarantees whatsoever are made as to the accuracy, adequacy, reliability, completeness, suitability, or applicability of the information to a particular situation.

5. Certain links on the magazine lead to resources located on servers maintained by third parties over whom the PCLinuxOS Magazine has no control or connection, business or otherwise. These sites are external to the PCLinuxOS Magazine and by visiting these, you are doing so of your own accord and assume all responsibility and liability for such action. Material Submitted by Users A majority of sections in the magazine contain materials submitted by users. The PCLinuxOS Magazine accepts no responsibility for the content, accuracy, conformity to applicable laws of such material.

Entire Agreement: These terms constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.



Help PCLinuxOS Thrive & Survive

**DONATE
TODAY**



Screenshot Showcase



Posted by luikki, October 14, 2026, running KDE.

PCLinuxOS Recipe Corner Bonus



Mexican Ground Beef and Noodles

Servings: 4

INGREDIENTS:

4 ounces dried multigrain or regular rotini or elbow macaroni (1 1/3 cups)
12 ounces extra-lean ground beef
2 cloves garlic, minced
1 can (15 oz) black beans, rinsed and drained
1 can (14.5 oz) no-salt-added diced tomatoes, undrained
3/4 cup salsa
1 teaspoon dried oregano, crushed
1/2 teaspoon ground cumin
1/2 teaspoon chili powder
1/2 cup shredded reduced-fat Colby and Monterey Jack cheese (2 ounces)
1/3 cup light sour cream
3 tablespoons sliced green onions
2 teaspoons coarsely chopped fresh cilantro
1/2 teaspoon finely shredded lime peel

DIRECTIONS:

1 Preheat the oven to 350°F. In a large saucepan, cook pasta according to package directions; drain. Return pasta to a hot saucepan; set aside.

2 Meanwhile, in a large skillet, cook meat and

garlic until meat is browned, stirring to break up meat as it cooks. Drain off fat.

3 Stir the cooked meat into pasta in a saucepan. Stir in beans, undrained tomatoes, salsa, oregano, cumin, and chili powder. Transfer mixture to a 1 1/2- to 2-quart casserole or baking dish.

4 Bake, covered, about 30 minutes or until heated through. Uncover and sprinkle with cheese. Bake, uncovered, about 3 minutes more or until the cheese is melted.

5 In a small bowl, stir together sour cream, 2 tablespoons of the green onions, the cilantro, and lime peel. To serve, top each serving with a spoonful of the sour cream mixture. Sprinkle with the remaining green onions.



NUTRITION:

Calories: 550	Carbs: 55g
Sodium: 800mg	Fiber: 6g
Protein: 46g	



PCLinuxOS Puzzled Partitions

		4	2	8		5		
7							4	
					9		1	
		8			3			
		5					3	9
	3		4	1	2			
			7	3	4			1
	2			5				7
		3						

SUDOKU RULES: There is only one valid solution to each Sudoku puzzle. The only way the puzzle can be considered solved correctly is when all 81 boxes contain numbers and the other Sudoku rules have been followed.

When you start a game of Sudoku, some blocks will be pre-filled for you. You cannot change these numbers in the course of the game.

Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

Each block must contain all of the numbers 1 through 9 and no two numbers in the same block of a Sudoku puzzle can be the same.



SCRAPPLER RULES:

1. Follow the rules of Scrabble®. You can view them [here](#). You have seven (7) letter tiles with which to make as long of a word as you possibly can. Words are based on the English language. Non-English language words are NOT allowed.

2. Red letters are scored double points. Green letters are scored triple points.

3. Add up the score of all the letters that you used. Unused letters are not scored. For red or green letters, apply the multiplier when tallying up your score. Next, apply any additional scoring multipliers, such as double or triple word score.

4. An additional 50 points is added for using all seven (7) of your tiles in a set to make your word. You will not necessarily be able to use all seven (7) of the letters in your set to form a "legal" word.

5. In case you are having difficulty seeing the point value on the letter tiles, here is a list of how they are scored:

0 points: 2 blank tiles

1 point: E, A, I, O, N, R, T, L, S, U

2 points: D, G

3 points: B, C, M, P

4 points: F, H, V, W, Y

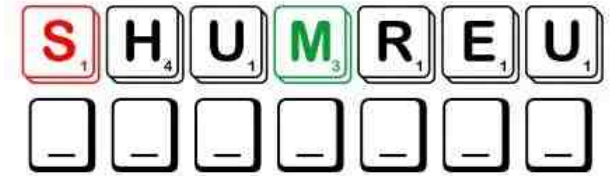
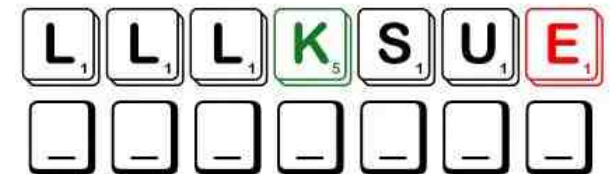
5 points: K

8 points: J, X

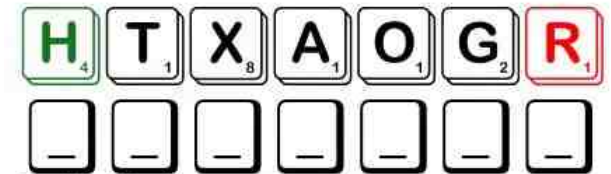
10 points: Q, Z

6. Optionally, a time limit of 60 minutes should apply to the game, averaging to 12 minutes per letter tile set.

7. Have fun! It's only a game!



Triple Word



Double Word



Possible score 251, average score 176.

Download Puzzle Solutions Here

November 2026 Word Find

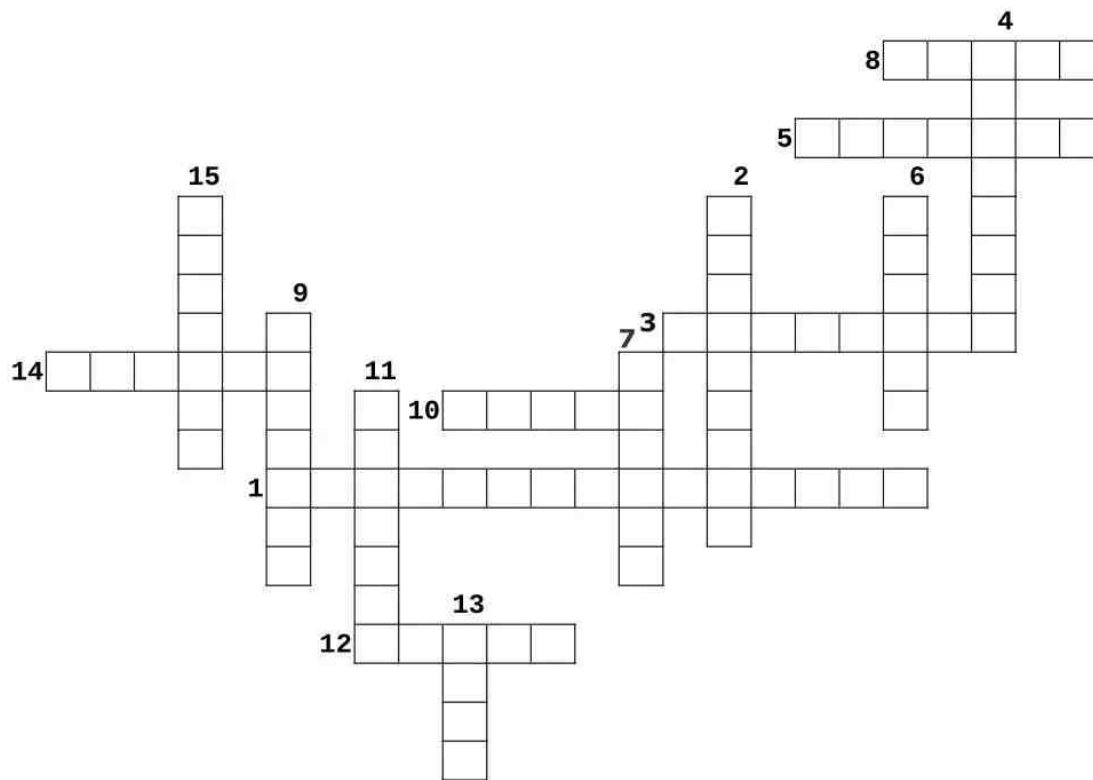
Skeleton

X L R F X U J T B V L X Y J R F I W Z Q W S R B T W X Q R U
 R M E T A C A R P A L G C Y Q I Z P H M O I Y W X S Z L F I
 H X I Y R I V L V G U G T Q Y R J I L U X N H Z G H B D F N
 N L U V O G N P K Z K O Q C F X F S E F O X L C E I U J H B
 X U G O H W T W G X S W J Z D Q E L C K F E A L G L W U E O
 F N J W T S F X C I U V R Y J Q X D X Z N Z C Z G J X D L S
 A J V J O B O K V B H D F S Q M B M A I B I T B D S P A W F
 B M A N D I B L E P P K P X N W H E W F V Y Z V O D Q S A R
 Z B M U N R E T S A I J O F T M I W C A C K Z X E I R P P V
 M F U V O P N C T A E Q S H Z Z U E L D S B S Y R Z I I I H
 D D E V X M B Z O F U W T U V S R C O C C Y X R T U L N A S
 S N G K I I U P J H V U I J A V U M P D P S E S A F I A R V
 V Z Q F N E K A V Y Z A D T I K L R G M E A G T D E Z L R H
 D F A W D R L X P T X G U C B C I K E O T F S L V F Y C L S
 J W I B W U Z V J M G D A M G Z Y A V M Z Y I M T A Y O R U
 C Q L B P A T E L L A L L D S T A I E S U X R M N H O L Z E
 B E U A U T A S O F V O T G U C E T P D C H M D W Q M U B O
 X D C Q I L B Z H E O L Q M I Q A N Z Y H C J D K T L M O Q
 H S D R D I A R R M I P S L D T N T X X V R A C V I A N E A
 X B L Q J U K T L P V U Q W A Z Z I A P I D D T V Z Y K P J
 J I L D S O E B D P U P D R R E F W A T N E I S S A C R U M
 T S T V U B P B N D W T S R M F X C P Z A S H R B G L A I T
 Q A B K R U M E F W R A L K G U S Q I Z N M K G R F I H A C
 T L R A Z M Y A X N L S P F I P G E Z L R D F E M Y F L D C
 L D E S K F D I G S I V Y V K H G J E Z D A M D L D T E J K
 I P P H A L A N G E S Z E W D N I X P H P T E S L E P C J S
 B M M V F L U X O J A T Y Z F Z E K W B S B Z P X L T W U S
 J M T V L U M B A R V E R T E B R A E X E O O N G X Z O I Z
 X G Z R B J Z G N F D Y V F Z E W B T N P Y P B D M U U N H
 H L W B I A O S E D A R F Q Z H A N R O S W S Y G V Q F J F

CERVICAL VERTEBRAE	CLAVICLE
COCCYX	FEMUR
FIBULA	HUMERUS
LUMBAR VERTEBRAE	MANDIBLE
METACARPAL	METATARSAL
PATELLA	PELVIS
PHALANGES	RADIUS
RIBS	SACRUM
SCAPULA	SKELETON
SKULL	SPINAL COLUMN
STERNUM	TARSAL
THORAX	TIBIA
ULNA	

[Download Puzzle Solutions Here](#)

November 2026 Crossword Skeleton



1. The five largest vertebrae in the lower back.
2. The small bones that form the fingers and toes.
3. The collar bone, which is joined at one end to the scapula, or shoulder blade, and at the other to the sternum, or breastbone.
4. The lower jaw of a vertebrate animal.
5. The flat bone in the middle of the chest that protects the organs of the torso from injury.
6. The final fused vertebrae at the base of the spine.
7. A triangular bone made up of five fused vertebrae and forming the posterior section of the pelvis.
8. A bone of the leg situated between the pelvis and knee.
9. A flat triangular bone located at the front of the knee joint.
10. The inner and larger of the two bones of the lower human leg, extending from the knee to the ankle.
11. The long bone of the arm or forelimb, extending from the shoulder to the elbow.
12. The bony framework of the head, enclosing the brain and supporting the face.
13. The bone of the forearm on the side opposite to the thumb.
14. The outer and narrower of two bones of the human lower leg, extending from the knee to the ankle.
15. Either of two large, flat, triangular bones forming the back part of the shoulder.

[Download Puzzle Solutions Here](#)

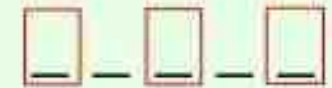
Mixed-Up-Meme Scrambler



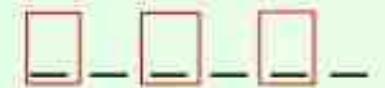
ALCAN



INLOG



BAMGEL



SAUCCU



How the food critic described his job ...

— — — " — — — — — — — — — — "

[Download Puzzle Solutions Here](#)

Inspiration & Motivation

***Good Things Don't Come To Those Who Wait.
They Come To Those Who Work
Their Asses Off And Never Give Up.***



Image by Gerd Altman from Pixabay

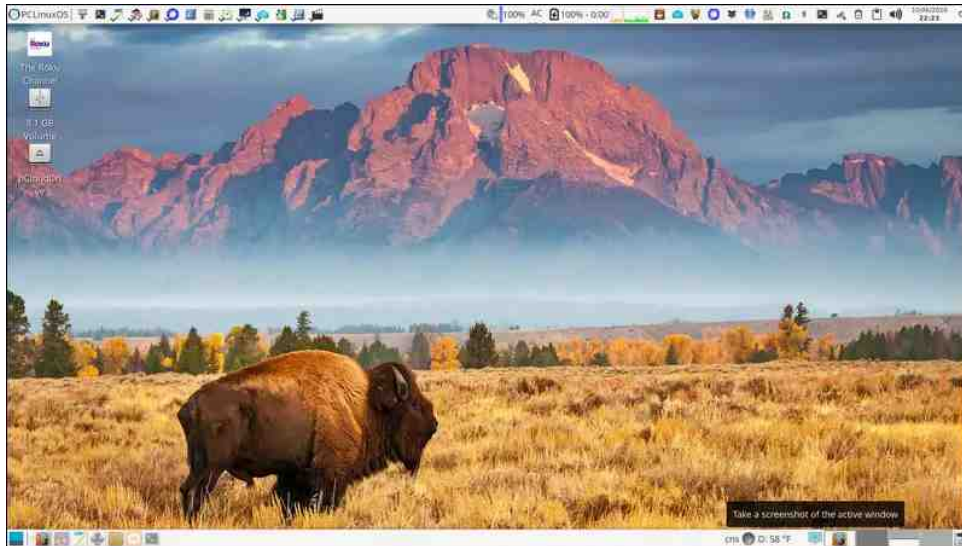
More Screenshot Showcase



Posted by francescoinblack, October 6, 2026, running IceWM.



Posted by MBL2, October 29, 2026, running KDE.



Posted by parnote, October 6, 2026, running Xfce.



Posted by mutse, October 6, 2026, running Mate.