THURSDAY, APRIL 16, 2026 · ISSUE #73

The Rizz News

Yesterday's Top Tech Stories — Curated by RizzBot

Google broke its promise to me – now ICE has my data

▲ 1621 · 706 comments · eff.org

TL;DR: Google violated its longtime promise to notify users before sharing data with law enforcement by handing a PhD student's information to ICE without warning after he briefly attended a pro-Palestinian protest.

Google handed over the personal data of Amandla Thomas-Johnson, a British-Trinidadian Ph.D. student who briefly attended a pro-Palestinian protest at Cornell University in September 2024, to Immigration and Customs Enforcement after receiving an administrative subpoena in April 2025. The company broke a nearly decade-long policy of notifying users before complying with law enforcement data requests, even though ICE's request that Google not alert Thomas-Johnson carried no legal enforcement mechanism or court order. The Electronic Frontier Foundation filed complaints with both the California and New York Attorneys General on Tuesday, asking them to investigate Google for deceptive trade practices over the broken promise.

WHAT THE COMMUNITY SAYS

Commenters are wrestling with a genuine legal ambiguity about whether First Amendment protections extend to non-citizens who are outside the United States when enforcement action is taken against them for speech that occurred while they were legally inside it. Underneath that doctrinal debate runs a sharper cultural tension, with some participants arguing that framing this as a question of legal technicalities at all misses the more troubling point that the government is maintaining surveillance lists of people who attend political protests.

Stop Flock

▲ 965 · 293 comments · stopflock.com

TL;DR: Flock Safety's AI-powered license plate readers, now deployed across thousands of communities nationwide, track every driver's movements, associations, and routines without warrants, creating an unprecedented mass surveillance network already proven vulnerable to serious abuse.

Flock Safety's AI-powered license plate reader network has grown to over 100,000 cameras nationwide, with a crowdsourced tracking map at DeFlock.me documenting roughly half of them across thousands of law enforcement agencies. The system goes far beyond basic plate recognition, building what the company calls a "Vehicle Fingerprint" that logs color, damage, wheel type, and even bumper sticker placement, while a feature called "Convoy Analysis" can identify associations between drivers based on vehicles frequently appearing near each other. Concerns about misuse are already materializing, including a case where a Kansas police chief used Flock cameras 228 times to surveil an ex-girlfriend without cause, and a 2025 investigation in which a journalist driving 300 miles across rural Virginia was captured by nearly 50 cameras operated by 15 different agencies, all without a warrant or any suspicion of wrongdoing.

WHAT THE COMMUNITY SAYS

293 comments discussing the topic.

Live Nation illegally monopolized ticketing market, jury finds

▲ 575 · 179 comments · bloomberg.com

TL;DR: A jury has found that Live Nation illegally monopolized the ticketing market, marking a landmark legal victory against the entertainment giant's dominant industry control.

A federal jury found Live Nation illegally monopolized the ticketing market, delivering a significant antitrust verdict against the entertainment giant. The ruling could have major implications for the company's control over concert venues, ticketing, and artist management through its Ticketmaster subsidiary. Specific financial penalties and remedies, including a potential breakup of the company, may follow as the case proceeds to sentencing.

WHAT THE COMMUNITY SAYS

Practitioners and fans are converging on a shared diagnosis that Ticketmaster's real problem is vertical integration, where the company profits from resale churn and therefore has no incentive to stop scalpers from cornering primary markets. The debate then fractures sharply over solutions, with some pushing structural fixes like Dutch auctions or ticket release timing to manipulate scalper risk, while others argue the cleanest answer is simply ID-tied non-transferable tickets, a proposal that draws pushback from those who see it as an unnecessary restriction on consumer freedom.

Cybersecurity looks like proof of work now

▲ 506 · 182 comments · dbreunig.com

TL;DR: Anthropic's powerful new AI model Mythos can autonomously complete complex corporate network attacks, transforming cybersecurity into a costly token-spending arms race between defenders and attackers.

Anthropic's unreleased security-focused LLM Mythos completed a simulated 32-step corporate network attack in 3 out of 10 attempts, the only model to do so, according to a new third-party analysis from the AI Security Institute. Each attempt consumed 100 million tokens at a cost of roughly $12,500, totaling $125,000 for the full test run, with no signs of diminishing returns as token budgets increased. The findings suggest cybersecurity may be evolving into a raw computational arms race, where defenders must out-spend attackers token-for-token to discover vulnerabilities before adversaries can exploit them.

WHAT THE COMMUNITY SAYS

Practitioners in the security field appear largely convinced that AI represents a genuine leap forward in vulnerability research, comparing it favorably to the paradigm shift brought by fuzzing, while skeptics are less disputing the capability itself than questioning

whether an institute staffed by AI industry alumni can produce unbiased benchmarks to measure it. Underlying the whole exchange is a tension between the credibility of the source and the validity of the conclusion, with cynics noting that "spend more tokens to improve security" conveniently doubles as a GPU sales pitch.

Cal.com is going closed source

▲ 362 · 282 comments · cal.com

TL;DR: Cal.com is abandoning its open source roots due to AI-powered security threats that can systematically scan codebases for vulnerabilities, while releasing a community version called Cal.diy under the MIT license.

Cal.com, the open-source scheduling platform, announced it is closing its source code, citing AI-powered security threats that allow attackers to systematically scan public codebases for vulnerabilities. The company pointed to a specific example where AI uncovered a 27-year-old vulnerability in the BSD kernel and generated working exploits within hours, arguing that open source code now effectively hands attackers a blueprint to exploit weaknesses. Cal.com will release a snapshot of its existing codebase to the public under the MIT license as a project called Cal.diy, though the company notes its production code has already significantly diverged through major rewrites of core systems including authentication and data handling.

WHAT THE COMMUNITY SAYS

282 comments discussing the topic.

God sleeps in the minerals

▲ 537 · 105 comments · wchambliss.wordpress.com

TL;DR: A viral blog post titled "God Sleeps in the Minerals" sparked widespread online discussion, drawing hundreds of Hacker News points alongside debate over its poetic, spiritually-charged title.

A photo essay titled "God Sleeps in the Minerals," published on WordPress and shared to Hacker News on April 15, 2026, quickly accumulated 426 points and sparked debate in its comment section. The piece, which draws its title from a quote attributed to Paramahansa Yogananda, features high-resolution mineral photography that some users praised as beautiful while others criticized the slow image load times on the page. The post was widely syndicated, appearing in at least three tech and indie developer digests including Datasphere Labs and a Chinese-language Hacker News roundup.

WHAT THE COMMUNITY SAYS

Rockhounding enthusiasts are wrestling with the gap between the accessible joy of amateur collecting and the reality that museum-quality specimens are largely locked behind private mining operations and serious money. A quietly interesting thread runs through the comments about whether scarcity is what makes specimens worth displaying at all, with one commenter pushing back to argue that some institutions, like the Computer History Museum, prove that context and explanation can make even ordinary objects compelling.

Want to write a compiler? Just read these two papers (2008)

▲ 492 · 150 comments · dadgum.com

TL;DR: Two accessible papers and Jack Crenshaw's tutorial series debunk the myth that writing compilers is difficult, offering beginners a straightforward path to building working compilers without overwhelming complexity.

A 2008 blog post argues that compiler writing is far less daunting than textbooks suggest, pointing to Jack Crenshaw's 1988 series "Let's Build a Compiler!" as proof the topic is accessible enough for first-year programming students. The post recommends pairing Crenshaw's work with the academic paper "A Nanopass Framework for Compiler Education" by Sarkar, Waddell, and Dybvig, which proposes breaking compiler construction into dozens or even hundreds of small, simple transformation passes rather than tackling large complex stages at once. Together, the two resources offer a practical path to building a working

compiler without wading through the dense theory that dominates most textbooks on the subject.

WHAT THE COMMUNITY SAYS

Practitioners in this thread are sharply divided on the Dragon Book, with many arguing its theoretical density actively discourages beginners while others defend it as excellent once you know where to start, specifically pointing to Chapter 2 as a standalone entry point. What emerges beneath the debate is a deeper nostalgia for the hands-on magic of compiler writing, with commenters crediting everything from Niklaus Wirth's 99-page gem to building a Forth interpreter in assembly as the experiences that actually made the subject feel alive.