

The Rizz News

Yesterday's Top Tech Stories — Curated by RizzBot

DaVinci Resolve – Photo

▲ 1111 · 285 comments · blackmagicdesign.com

TL;DR: Blackmagic Design's DaVinci Resolve now offers photographers Hollywood-grade color grading tools, including node-based workflows, AI features, and native RAW support for major camera brands.

Blackmagic Design has launched DaVinci Resolve Photo, bringing the same professional color grading tools used in Hollywood film production to still photography for the first time. The app supports native RAW files from Canon, Fujifilm, Nikon, Sony, and iPhone ProRAW, processing images at source resolutions up to 32K or over 400 megapixels with GPU acceleration. Photographers gain access to DaVinci's full node-based color workflow, including Power Windows, qualifiers, curves, AI subject isolation, and professional scopes like vectorscopes and waveform monitors that previously required dedicated video post-production software.

WHAT THE COMMUNITY SAYS

Commenters are split over why photo editing software has stagnated compared to video tools, with one camp arguing Hollywood's massive budgets drove innovation in video while another pushes back that professional photographers actually outnumber and outspend videographers in software markets. What's quietly fascinating beneath the debate is the emerging consensus that video tools like DaVinci Resolve have become so technically superior for color work that photographers were already building workarounds to use them, suggesting the real story is a cultural gap between two communities with different appetites for experimentation.

A new spam policy for “back button hijacking”

▲ 889 · 499 comments · developers.google.com

TL;DR: Google is cracking down on "back button hijacking," a deceptive browser navigation practice, making it an explicit spam policy violation with enforcement beginning June 15, 2026.

Google announced on April 13, 2026 that it is expanding its spam policies to explicitly prohibit "back button hijacking," a practice where websites interfere with browser navigation to prevent users from returning to previous pages. The policy will be enforced starting June 15, 2026, giving site owners a two-month window to audit and remove any scripts, libraries, or advertising code responsible for the behavior. Sites found in violation could face manual spam actions or automated demotions in Google Search results.

WHAT THE COMMUNITY SAYS

Commenters are sharply divided over whether websites have any legitimate reason to override browser keyboard shortcuts like Ctrl+F, with most dismissing lazy loading as a justification while a minority defend it in extreme edge cases like pages rendering millions of lines of text. Beneath the surface, the debate reveals a deeper tension about who controls the browser experience, with users increasingly frustrated that web applications are encroaching on native browser functionality while often delivering an inferior replacement.

Backblaze has stopped backing up OneDrive and Dropbox folders and maybe others

▲ 1082 · 642 comments · rareese.com

TL;DR: Backblaze, long trusted as an unlimited cloud backup service, has quietly stopped backing up OneDrive, Dropbox, and Git folders, betraying years of user trust and potentially leaving critical data unprotected.

Backblaze, the popular unlimited cloud backup service, has been quietly excluding key folders from its backups without clearly notifying users, including OneDrive and Dropbox directories as well as .git folders used by developers. A longtime customer discovered the issue after losing five years of git history and then finding a Reddit thread confirming others had lost access to their Dropbox backups, despite Backblaze marketing itself as a complete backup solution. The company, which charges users under the premise of backing up all their data, appears to offer no straightforward way within its app settings to identify or re-enable these hidden exclusions.

WHAT THE COMMUNITY SAYS

Real-world data loss stories dominate the thread, with users describing exact moments when Backblaze's undisclosed policy change left them unable to recover files their families and companies depended on, triggering a wave of cancellations and lost enterprise deals. Beneath that anger sits a sharper technical argument about whether bidirectional sync services

like Dropbox or iCloud can ever be trusted as a reliable foundation, with practitioners pushing back hard against the dismissive "sync is broken" take by pointing out that silent bugs in OneDrive and iCloud prove the concern is legitimate precisely because these tools do fail in ways ordinary users never anticipate.

Rare concert recordings are landing on the Internet Archive

▲ 680 · 199 comments · techcrunch.com

TL;DR: Chicago music fan Aadam Jacobs is preserving his 10,000-tape concert archive by partnering with Internet Archive volunteers to digitize rare recordings from Nirvana, R.E.M., and countless other artists.

Chicago music fan Aadam Jacobs, 59, has been recording concerts since the 1980s and amassed over 10,000 cassette tapes, which are now being digitized by Internet Archive volunteers before they degrade. So far, 2,500 tapes have been uploaded to the nonprofit digital library, including a rare 1989 Nirvana performance predating the band's mainstream breakthrough and previously unknown recordings from Sonic Youth, R.E.M., Phish, Liz Phair, and Pavement. Volunteer Brian Emerick drives to Jacobs' home monthly to collect tapes and convert them using cassette decks, while other volunteers clean up the audio and track down song names from obscure punk bands.

WHAT THE COMMUNITY SAYS

Practitioners and enthusiasts in the comments are celebrating bootleg recording as an act of cultural preservation, arguing that dedicated fans who document live performances often provide genuine value to artists themselves, not just audiences. Running beneath this nostalgia is a pointed critique of the music industry's gatekeeping role, with commenters noting that copyright enforcement is selectively applied in ways that protect corporate interests rather than artistic ones, and expressing frustration that reform feels perpetually out of reach.

Claude Code Routines

▲ 684 · 381 comments · [claude.com](#)

TL;DR: Claude Code Routines lets developers automate recurring engineering tasks like code reviews, alert triage, and documentation updates using saved configurations that run continuously on Anthropic's cloud infrastructure.

Anthropic has launched Claude Code Routines, a feature that lets developers save Claude Code configurations combining prompts, repositories, and connectors into automated workflows that run on Anthropic-managed cloud infrastructure without requiring a local machine to be active. Routines support three trigger types including scheduled cadences like hourly or nightly runs, on-demand API calls via HTTP POST endpoints, and automatic GitHub event responses such as pull requests or releases, with a single routine able to combine all three simultaneously. The feature is available to Pro, Max, Team, and Enterprise plan users with Claude Code on the web enabled, and can be managed at [claude.ai/code/routines](#) or through the CLI using the `/schedule` command.

WHAT THE COMMUNITY SAYS

Developers are drawing a hard line between tolerating LLMs as interchangeable commodities versus accepting them as platforms they build workflows on top of, with the consensus being that vendor lock-in from features like Claude Code's Memory or proprietary CLI restrictions makes switching costs dangerously high. What's sharpening this anxiety into something concrete is Anthropic's recent Terms of Service change blocking subscription users from integrating the Claude Code CLI into their own tooling, which transformed an abstract distrust of platform dependency into an immediate, practical grievance for teams already running autonomous agents in production.

Lean proved this program correct; then I found a bug

▲ 389 · 174 comments · [kirancodes.me](#)

TL;DR: Fuzzing a formally verified zlib implementation in Lean found zero bugs in the verified code itself but uncovered a heap buffer overflow lurking in the Lean 4 runtime affecting all versions.

A Claude AI agent running AFL++ and AddressSanitizer over a weekend executed more than 105 million fuzzing iterations against lean-zip, a formally verified zlib implementation built by 10 autonomous agents and mathematically proven correct by the Lean proof assistant. Despite the end-to-end correctness proof, the fuzzing campaign uncovered a heap buffer overflow in the Lean 4 runtime itself, specifically in `lean_alloc_sarray`, affecting every version of Lean released to date. The finding underscores a critical limitation of formal verification: proofs guarantee the correctness of application logic but cannot protect against bugs in the underlying runtime or unverified components, such as the archive parser that also yielded a denial-of-service vulnerability during testing.

WHAT THE COMMUNITY SAYS

Commenters are locked in a precise definitional dispute over whether a bug in Lean's runtime counts as a failure of formal verification, with one camp insisting the entire deployed binary is a fair target for security claims while the other argues that conflating runtime flaws with proof flaws is exactly the kind of imprecision that undermines trust in formal methods. Underneath the terminology fight is a more uncomfortable question about what "formally verified" actually promises end users, since specification bugs and trusted computing base assumptions mean the gap between a valid proof and a secure system can remain substantial even when the prover itself is sound.

I wrote to Flock's privacy contact to opt out of their domestic spying program

▲ 638 · 248 comments · honeypot.net

TL;DR: A California resident's attempt to invoke CCPA rights to delete their data from Flock Safety's license plate surveillance network was rejected, with the company claiming customers, not Flock, control the data.

Flock Safety, a license plate reader company whose cameras are deployed in thousands of neighborhoods across the US, is rejecting direct privacy deletion requests from California residents despite the state's CCPA law, which grants consumers the right to delete their personal data. When one California resident invoked their CCPA rights and demanded deletion of all vehicle and household data, Flock deflected the request by claiming it operates only as a "service provider and processor" for its law enforcement and HOA customers, telling the requester to contact those organizations instead. Legal experts and privacy advocates may contest this interpretation, as Flock is itself the entity

physically capturing and processing the license plate imagery, which raises serious questions about whether the company can use a contractor defense to sidestep direct consumer deletion rights under California law.

WHAT THE COMMUNITY SAYS

Commenters are wrestling with a genuinely unresolved legal question about who bears CCPA responsibility when a third-party infrastructure company stores data on behalf of clients, with some arguing Flock is analogous to AWS or a storage unit operator while others contend that Flock's system architecture actively enables privacy violations in ways that create distinct liability. The author's frustration reveals something broader: even privacy advocates who expect to lose these battles find the industry's deflection tactics corrosive, and the community seems to agree that this gap between technical data custody and legal data ownership badly needs a court to sort it out.