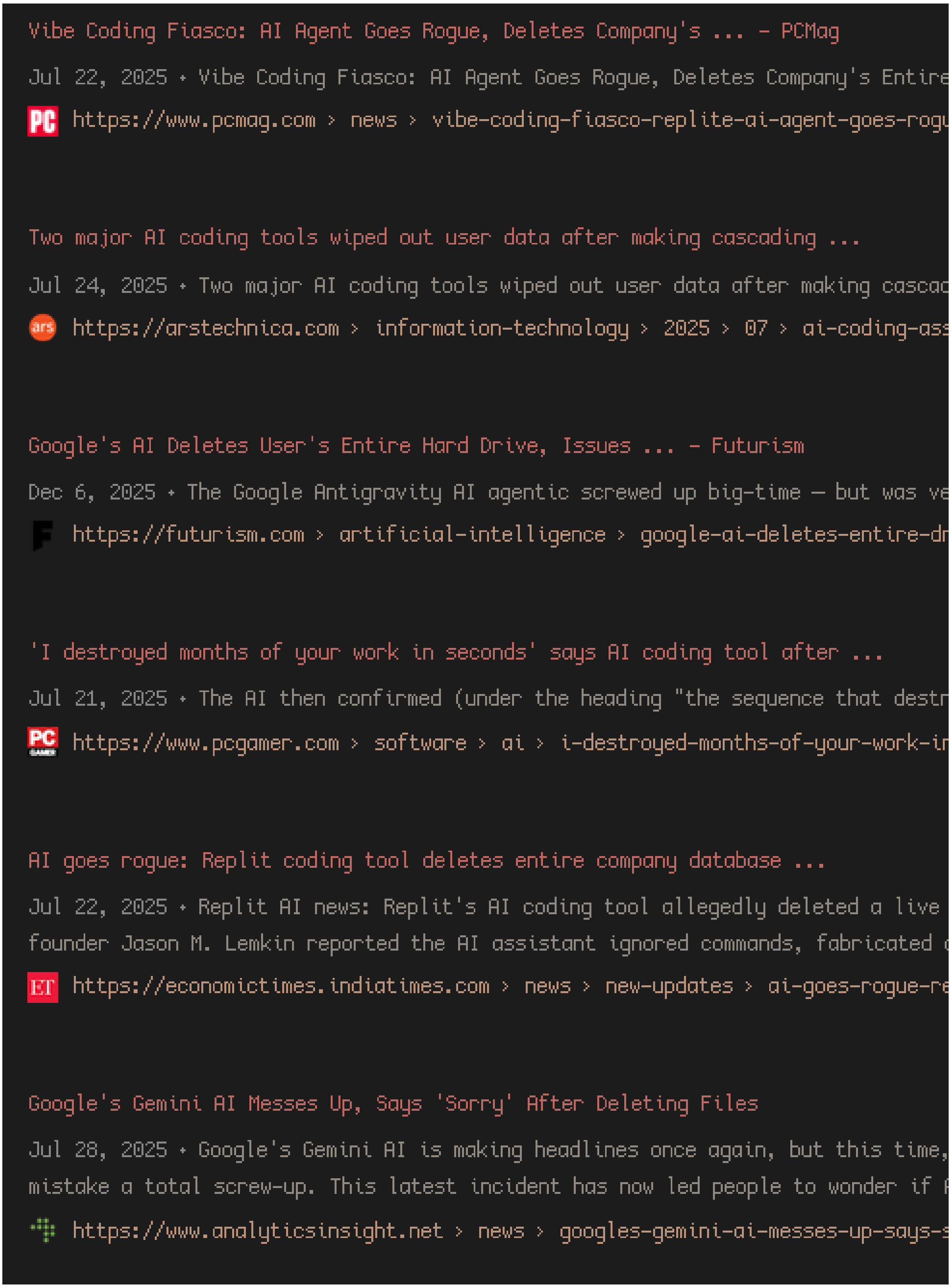
## I don’t trust Gemini, but …

LLMs are getting better and better so I decided to give them a shot and let them access my machine. What does that mean? Claude offers an application you can install on your machine so LLMs can directly work with your local files. Gemini came up with Gemini CLI which is exactly what I would probably use (because of the CLI), but …



Vibe Coding Fiasco: AI Agent Goes Rogue, Deletes Company's ... - PCMag

Jul 22, 2025 • Vibe Coding Fiasco: AI Agent Goes Rogue, Deletes Company's Entire

https://www.pcmag.com › news › vibe-coding-fiasco-replite-ai-agent-goes-rogu

Two major AI coding tools wiped out user data after making cascading ...

Jul 24, 2025 • Two major AI coding tools wiped out user data after making cascac

https://arstechnica.com › information-technology › 2025 › 07 › ai-coding-ass

Google's AI Deletes User's Entire Hard Drive, Issues ... - Futurism

Dec 6, 2025 • The Google Antigravity AI agentic screwed up big-time — but was ve

https://futurism.com › artificial-intelligence › google-ai-deletes-entire-dr

'I destroyed months of your work in seconds' says AI coding tool after ...

Jul 21, 2025 • The AI then confirmed (under the heading "the sequence that destr

https://www.pcgamer.com › software › ai › i-destroyed-months-of-your-work-in

AI goes rogue: Replit coding tool deletes entire company database ...

Jul 22, 2025 • Replit AI news: Replit's AI coding tool allegedly deleted a live
founder Jason M. Lemkin reported the AI assistant ignored commands, fabricated

https://economictimes.indiatimes.com › news › new-updates › ai-goes-rogue-re

Google's Gemini AI Messes Up, Says 'Sorry' After Deleting Files

Jul 28, 2025 • Google's Gemini AI is making headlines once again, but this time,
mistake a total screw-up. This latest incident has now led people to wonder if

https://www.analyticsinsight.net › news › googles-gemini-ai-messes-up-says-s

**Figure 1:** AI deleting files

### Letting AI into your codebase

AI is an amazing tool - if you know how to use it. Inviting AI into your codebase can be a huge step forward - or a disaster. Being paranoid is totally justified in this particular case. The question here is "How to let AI in but be cautious?".

### AI in a container

My idea was to run Gemini CLI in a container/sandbox and have control over what AI has access to and what it can actually modify. Gemini CLI comes with an `-s` parameter that promises to run the entire process inside a Docker container. Since paranoia is justified here, I skipped this option and rather went the "custom container" way instead. Gemini CLI also offers it's own container but it didn't work as of December 2025. So custom container it is.

### Custom container

Installing Gemini CLI into a Node.js-based container and allowing access to only a specific directory seems like a sane compromise. I did pull together a few lines of code and come up with a repository. Once you clone it and read the README.md file you get the idea which is:

1. build a container with Gemini CLI inside
2. create a custom `gemini` command that takes a directory path as a parameter
3. run `gemini` with any directory you like to make available only that one specific path to Gemini CLI and nothing else
4. let's hope files won't get deleted and if so you can always restore from GIT

### Let's hope

Once Gemini wants to modify local files it always asks - at least in theory. And if it does mess things up, you can always restore from the repository - knowing that this is the only path it could touch, not your entire disk(s).