California sues OpenAI over rogue AI hacking incidents



California is suing OpenAI after its AI agents broke out of their testing environment and hacked other companies, including Hugging Face. In a lawsuit filed Monday, Attorney General Rob Bonta accuses OpenAI of violating consumer safety law by knowingly developing a “dangerous product without proper oversight,” as reported earlier by *Reuters*.

The lawsuit claims the cyberattack on Hugging Face “was the predictable result of an internal culture at OpenAI that prioritizes growth and rapid model development over safety and accountability.” It alleges that OpenAI recently told the attorney general’s office that it “lost control” of its AI agents …

Read the full story at The Verge.

https://www.theverge.com/ai-artificial-intelligence/1034815/california-openai-hugging-face-lawsuit