OpenAI has evidence that its models helped train China's DeepSeek

Chinese artificial intelligence company DeepSeek disrupted Silicon Valley with the release of cheaply developed AI models that compete with flagship offerings from OpenAI – but the ChatGPT maker suspects they were built upon OpenAI data.

OpenAI and Microsoft are investigating whether the Chinese rival used OpenAI's API to integrate OpenAI's AI models into DeepSeek's own models, according to *Bloomberg*. The outlet's sources said Microsoft security researchers detected that large amounts of data were being exfiltrated through OpenAI developer accounts in late 2024, which the company believes are affiliated with DeepSeek.

OpenAI told the *Financial Times* that it found evidence linking DeepSeek to the use of distillation – a common technique developers use to train AI models by extracting data from larger, more capable ones. It's an efficient way to train smaller models at a fraction of the more than $100 million that OpenAI spent to train GPT-4. While developers can use OpenAI's API to integrate its AI with their own applications, distilling the outputs to build rival models is a violation of OpenAI's terms of service. OpenAI has not provided details of the evidence it found.

President Donald Trump's artificial intelligence czar David Sacks said "it is possible" that IP theft had occurred. "There's substantial evidence that what DeepSeek did here is they distilled knowledge out of OpenAI models and I don't think OpenAI is very happy about this," Sacks told *Fox News* on

Tuesday.

“We know PRC (China) based companies — and others — are constantly trying to distill the models of leading US AI companies,” OpenAI said in a statement to *Bloomberg*. “As the leading builder of AI, we engage in countermeasures to protect our IP, including a careful process for which frontier capabilities to include in released models, and believe as we go forward that it is critically important that we are working closely with the US government to best protect the most capable models from efforts by adversaries and competitors to take US technology.”

https://www.theverge.com/news/601195/openai-evidence-deepseek-distillation-ai-data