

Fearing leaks, Apple restricts ChatGPT use among employees

Enlarge / An AI-generated cartoon depiction of a chatbot being crossed out.

Benj Edwards / Stable Diffusion

reader comments

27 with

According to internal sources and company documents reviewed by The Wall Street Journal, Apple has restricted its employees' use of ChatGPT and AI coding tools such as GitHub Copilot for fear of leaking confidential data to outside sources. Meanwhile, Apple is also reportedly developing similar AI technology.

ChatGPT is a conversational large language model (LLM) developed by Microsoft-backed OpenAI that is capable of tasks ranging from answering questions and writing essays to assisting with programming chores. Currently, the ChatGPT AI model only runs on OpenAI or Microsoft servers and is accessible through the Internet.

Apple's decision to limit the use of external AI tools stems from a concern that confidential data could be exposed due to the nature of these AI models, which send user data back to developers for cloud processing and assistance in future AI model improvements.

OpenAI previously faced privacy issues with ChatGPT when a bug

permitted some users to access information from other users' chat history. In response to criticism from Italy, OpenAI implemented an option for users to turn off their chat history, which also prevents OpenAI from training future AI models using their chat history data.

An ongoing trend

Apple is well-known for its rigorous security measures, and its decision to ban external AI tool use reflects a growing trend among companies such as Samsung and JPMorgan Chase. The Wall Street Journal reports that Amazon encouraged its engineers to utilize its proprietary AI tools (like CodeWhisperer) for coding assistance instead of external tools.

Advertisement

To address privacy concerns among businesses, Microsoft recently announced plans to launch a privacy-focused version of ChatGPT that would target banks, health care providers, and other large organizations with heightened concerns about data leaks and regulatory compliance.

This more expensive business version of ChatGPT is set to run on dedicated servers, separate from those used by other companies or individual users, which is expected to help prevent inadvertent data leaks and prevent sensitive data from being used to train the AI language model. Even so, it's doubtful a high-profile competitor like Apple would trust Microsoft with its confidential data under these circumstances.

Apple's internal AI developments

The Wall Street Journal also says that Apple is working on its own LLMs under the leadership of John Giannandrea, a former Google employee who is now Apple's senior vice president of

Machine Learning and AI Strategy.

Recently, we covered an internal report from The Information that questioned the conservatism of Apple's AI strategy amid criticism of drawbacks in its now seemingly outdated Siri voice assistant. Siri, which launched in 2011, briefly inspired a miniature version of the AI hype we're seeing now.

It's important to note that while Apple has restricted ChatGPT use for its employees, that ban does not extend to Apple users. Just yesterday, OpenAI released an official ChatGPT client for iPhone users in the US, who can now easily access the tool on the go with an OpenAI account.

<https://arstechnica.com/?p=1940472>