Experts urge caution over use of Chinese AI DeepSeek

UK officials say they are monitoring any national security threat to data from the new AI

4 min. read · View original

Experts have urged caution over rapidly embracing the Chinese artificial intelligence platform DeepSeek, citing concerns about it spreading misinformation and how the Chinese state might exploit users' data.

The government said its use was a personal choice for citizens, but officials were monitoring any national security threat to data from the new AI and said they would not hesitate to take action if threats emerged.The new low-cost AI wiped $1tn off the leading US tech stock index this week and it rapidly became the most downloaded free app in the UK and the US. Donald Trump called it a “wake-up call” for tech firms.

Its emergence has shocked the tech world by apparently showing it can achieve a similar performance to widely used platforms such as ChatGPT at a fraction of the cost.

Michael Wooldridge, a professor of the foundations of AI at the University of Oxford, said it was not unreasonable to assume data inputted into the chatbot could be shared with the Chinese state.

He said: “I think it’s fine to download it and ask it about the performance of Liverpool football club or chat about the history of the Roman empire, but would I recommend putting anything sensitive or personal or private on them? “Absolutely not … Because you don’t know where the data goes.”

Dame Wendy Hall, a member of the United Nations high-level advisory body on AI, told the Guardian: “You can’t get away from the fact that if you are a Chinese tech company dealing with information you are subject to the

Chinese government's rules on what you can and cannot say."

"We should be alarmed," said Ross Burley, a co-founder of the Centre for Information Resilience, which is part-funded by the US and UK governments. "We've seen time and again how Beijing weaponises its tech dominance for surveillance, control and coercion, both domestically and abroad."

He said, if unchecked, it could "feed disinformation campaigns, erode public trust and entrench authoritarian narratives within our democracies".

Peter Kyle, the UK technology secretary, on Tuesday told the News Agents podcast: "I think people need to make their own choices about this right now, because we haven't had time to fully understand it … this is a Chinese model that … has censorship built into it.

"So, it doesn't have the kind of freedoms you would expect from other models at the moment. But of course, people are going to be curious about this."

skip past newsletter promotion

after newsletter promotion

DeepSeek is an open-source platform, which means software developers can adapt it to their own ends. It has sparked hopes of a new wave of innovation in AI, which had appeared to be dominated by US tech companies reliant on huge investments in microchips, datacentres and new power sources.

Wooldridge said: “It does rather forcefully signal, in case anybody hadn’t got the message, that China is not behind in this space.”

Some people testing DeepSeek have found that it will not answer questions on sensitive topics such as the Tiananmen Square massacre. When asked about the status of Taiwan, it repeats the Chinese Communist party line that the island is an “inalienable” part of China.

“The biggest problem with generative AI is misinformation,” Hall said. “It depends on the data in a model, the bias in that data and how it is used. You can see that problem with the DeepSeek chatbot.”

One user, Azeem Azhar, an AI expert, asked about the events in Tiananmen Square and was told that DeepSeek could not provide detailed information and that "this topic is highly sensitive and often censored in many countries, including China".

However, the AI then did explain that the events were "widely recognised as the suppression of pro-democracy protests" and said: "The Chinese government responded with a violent crackdown, resulting in the deaths of hundreds (or possibly thousands) of people, including both protesters and soldiers."

People use AI models such as DeepSeek and ChatGPT to help them process personal papers or documents for work, such as meeting minutes, but anything uploaded can be taken by the owner of the company and used for training the AI or for other purposes.

DeepSeek is based in Hangzhou and makes clear in its privacy policy that the personal information it collects from users is held "on secure servers located in the People's Republic of China".

It says it uses data to “comply with our legal obligations, or as necessary to perform tasks in the public interest, or to protect the vital interests of our users and other people”.

China’s national intelligence law states that all enterprises, organisations and citizens “shall support, assist and cooperate with national intelligence efforts”.