Risks to Kansans from DeepSeek

Jacqueline Deal, PhD

2/13/25

Overview:

DeepSeek is a Chinese AI company founded in 2023 by Liang Wenfeng. DeepSeek gained international attention with the release of its generative AI large language model DeepSeek-R1 in January 2025. R1 rivals leading offerings from U.S. firms but was allegedly developed at a fraction of the cost and in spite of U.S. export controls designed to slow Chinese AI development.[1] The CCP may derive strategic value from Kansans' usage of the DeepSeek app by providing CCP-aligned answers to their queries while harvesting their data in real time.

Risks to Kansan DeepSeek App Users:

- **Censorship** – R1 has built-in censorship mechanisms, particularly on topics sensitive to the CCP.[2] This could enable the CCP to use DeepSeek to shape Kansans' views in directions favorable to the party.
- **Disinformation** – The platform could also be used to spread disinformation or propaganda aligned with CCP interests.[3]
- **Public (un)safety** – Experts have identified that DeepSeek's model can be easily manipulated into providing dangerous information, such as instructions for creating bioweapons or promoting self-harm.[4] Relative to OpenAI's ChatGPT, Google's Gemini and Anthropic's Claude, R1 is "more susceptible to jailbreaking"[5] – i.e., allowing users to bypass health and safety protocols – and thus poses a greater danger to public safety.
- **Privacy infringement and surveillance** – DeepSeek's data collection policies explicitly state that user inputs, including text and audio, are stored on servers located in China.[6]

---

[1] The United States has sought to slow Chinese AI development because AI is inherently dual-use, i.e., it has not only civilian or commercial applications but also military applications. DeepSeek has been accused of understating how much it spent to develop R1, using Western models to train R1, and evading export controls on processors – see https://stratechery.com/2025/deepseek-faq/;
https://www.axios.com/2025/01/29/openai-deepseek-ai-models-data-training;
https://nypost.com/2025/01/29/business/palmer-luckey-doubts-deepseek-claims-says-us-media-fell-for-ccp-propaganda/;
https://www.bloomberg.com/news/newsletters/2025-01-31/us-probes-whether-deepseek-bypassed-chip-restrictions

[2] https://www.theguardian.com/technology/2025/jan/28/we-tried-out-deepseek-it-works-well-until-we-asked-it-about-tiananmen-square-and-taiwan

[3] https://www.pbs.org/newshour/politics/house-lawmakers-propose-deepseek-ban-on-u-s-government-devices

[4] https://www.wsj.com/tech/ai/china-deepseek-ai-dangerous-information-e8eb31a8

[5] Ibid

[6] https://apnews.com/article/deepseek-china-generative-ai-internet-security-concerns-c52562f8c4760a81c4f76bc5fbdebad0

Given the CCP's data, intelligence, and national security laws, this means that the party will have access to American account information whenever it wants.[7] Further, Western researchers have recently discovered that user data is transmitted directly from the app to China Mobile, a sanctioned company, and Bytedance, the owner of TikTok, the subject of a Congressional divestment law.[8] The CCP's access to TikTok user data via Bytedance and use of it for surveillance of political dissidents has already been reported.[9] This suggests that the CCP could exploit DeepSeek user data for similar ends.

Next Steps:

DeepSeek's compliance with CCP policies and data practices has already provoked bans in several U.S. states,[10] as well as other countries.[11]

On February 6th, Reps. Josh Gottheimer, D-N.J., and Darin LaHood, R-Ill., introduced the "No DeepSeek on Government Devices Act," a bill that would ban federal employees from using the Chinese AI app on government-owned electronics.[12] More broadly, independent legal analysis indicates that DeepSeek could be banned from app stores in the United States under the existing "Protecting Americans from Foreign Adversary Controlled Applications Act" or via presidential authorities exercised in recent Executive Orders.[13]

Kansas has an opportunity to take decisive action and join Florida, Texas, and New York in moving to protect its citizens ahead of the slower federal process.

---

[7] https://www.hawley.senate.gov/fbi-director-china-can-compel-tech-companies-doing-business-country-turn-over-any-information-china/

[8] Ibid and https://arstechnica.com/security/2025/02/deepseek-ios-app-sends-data-unencrypted-to-bytedance-controlled-servers/

[9] https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html

[10] https://gov.texas.gov/news/post/governor-abbott-announces-ban-on-chinese-ai-social-media-apps; https://dms-media.ccplatform.net/content/download/163205/file/Prohibited%20Applications%20List_Final_v3.pdf ; https://abcnews.go.com/US/deepseek-banned-government-devices-new-york-state/story?id=118653885

[11] For instance, DeepSeek is banned on governmental devices in Australia, South Korea, and Taiwan – https://www.aljazeera.com/news/2025/2/6/which-countries-have-banned-deepseek-and-why

[12] https://www.pbs.org/newshour/politics/house-lawmakers-propose-deepseek-ban-on-u-s-government-devices

[13] https://www.alstonprivacy.com/deekseek-grabs-headlines-but-could-it-be-unlawful-by-april-considerations-for-companies-from-recent-us-data-regulations/