# Australia’s home affairs department kept no real-time records of ChatGPT use, raising ‘serious security concerns’

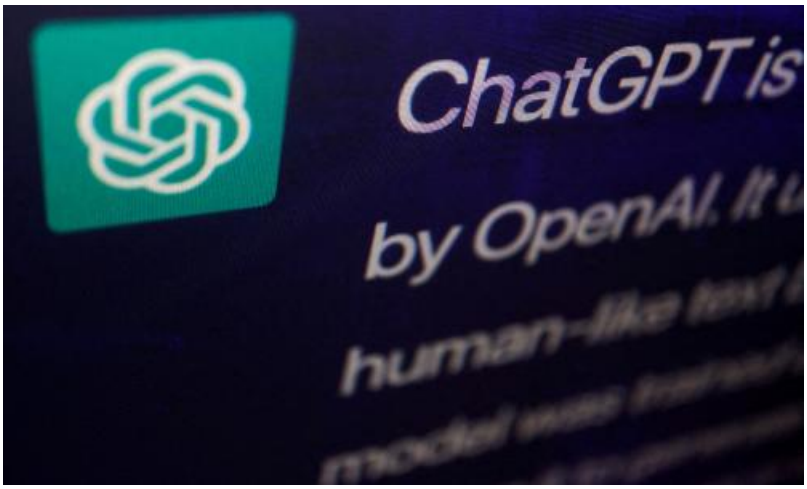
Publication Date: 2023-08-09

Author: Ariel Bogle

Section: Technology

Tags: ChatGPT, Australian politics, Artificial intelligence (AI), Computing, news

Article URL: https://www.theguardian.com/technology/2023/aug/09/home-affairs-department-chatgpt-ai-chatbot




Staff in the home affairs department have said they could not recall what prompts they had entered into ChatGPT during experiments with the AI chatbot, and documents suggest no real-time records were kept. In May, the department told the Greens senator David Shoebridge it was using the tool in four divisions for “experimentation and learning purposes”. It said at the time that use was “coordinated and monitored”. Records obtained by Guardian Australia under freedom of information law suggest no contemporaneous records were kept of all questions or “prompts” entered into ChatGPT or other tools as part of the tests. Shoebridge said this raised potential “serious security concerns”, given staff appeared to be using ChatGPT to tweak code as part of their work. In response to a request for all prompts used between November 2022 and May 2023, the department provided a questionnaire about which queries staff remembered using and for what purpose. Staff members remarked in the survey they “don’t recall exactly” what prompts they entered, or that they “don’t remember exactly as it was a long time ago”. “I can’t recall details but it was very generic and no details of departmental infrastructure or data were used,” one wrote. Sign up for Guardian Australia’s free morning and afternoon email newsletters for your daily news roundup Shoebridge said the documents called into question the claim that use of ChatGPT was being monitored, and raised serious questions about the reliability of the responses provided. “In fact, no system exists to even record the information Home Affairs officers are pumping into the ChatGPT prompt,” he said. “Given that Home Affairs’ use of ChatGPT was for experimentation and learning purposes, the lack of record-keeping measures further fuels our concerns that clear guardrails and protections are not put in place by the department.” A Home Affairs spokesperson said the department did not restrict staff from accessing ChatGPT for experimentation until mid-May 2023, but prohibited the unauthorised disclosure of official information. “Access to ChatGPT from departmental systems remains suspended, unless an exception is approved,” they said. “No exceptions have been granted to date.” No instances of ChatGPT being used for department decision making have been identified. Many of the prompts staff said they used related to computer programming, such as “debugging generic code errors” or “asking chat gpt [sic] to write scripts for work”. Others used ChatGPT to “find errors and correct scripts”, noting that “answers are not always 100% accurate”. In the information computer technology division, one of the four areas where the experiments were undertaken, one person used the tool for “business related topics like trobleshooting [sic] client-side and servver-side [sic] scripts like javascripts and escripts, questions on how-to perform certain functions in certain language etc”. Security concerns about chatbots based on large language models include the risk that sensitive information entered as part of

prompts could be incorporated into the model's underlying dataset, meaning it could be exposed later by questions from other users. In cyber risk services, a Home Affairs staff member used ChatGPT for "technical research" with possible questions relating to "the UK government's supply chain security policies". Another in the refugee humanitarian and settlement division trialled ChatGPT to "generate discussion questions to inform a briefing" about a non-profit from another country. The fourth division where experiments took place was the data and economic analysis centre. In May the home affairs secretary, Michael Pezzullo, told Senate estimates the use of ChatGPT or Bard was "barred and suspended", and called for a whole-of-government approach to the technology. "I don't think individual officers, who won't necessarily be attuned to those risks or have the capacity to engage with those applications, should be in a position where they say: 'Gosh! This'll help me do my work quicker. I'm going to download ChatGPT,'" he said at the time.