October 18, 2023

Considerations for Using ChatGPT or other Large Language Models (LLMs)

Below includes consideration of risks and privacy concerns associated with using ChatGPT (created by OpenAI) and other GPT based large language models (LLM).

Considerations on Data Accuracy, Privacy, and Security:

The following points address the key areas of concern with a goal to support library staff in both use recommendations and communication with patrons.

1. Trustworthiness of ChatGPT Statements:
    a. ChatGPT is an AI tool that uses a machine learning model based on pattern-matching, not an actual thinking entity. It generates responses by identifying and matching patterns from its training data. Our brains tend to perceive intentional thought behind most things we see, but ChatGPT and other LLMs do not have thought behind their text and should never be viewed as a definitive source of knowledge.
2. Bias in AI-generated Responses:
    a. ChatGPT may inadvertently produce biased responses due to biases present in its training data or in the way it was prompted. Users should be vigilant when using ChatGPT, recognizing that its responses may unintentionally reflect these biases.
    b. Never take AI-generated content at face value and cross-check it with unbiased sources whenever possible.
3. Privacy Statement:
    a. ChatGPT has a privacy policy that details how they collect, use, and share user data, ensuring the protection of user data and compliance with applicable privacy laws.
    b. News articles in the spring of 2023 noted some concerns around practices of data collection and privacy.
4. Account Information and Sharing:
    a. ChatGPT does not sell email lists or user information to third parties, and their privacy policy explicitly states their commitment to safeguarding the privacy and security of the information they collect.
5. Data Storage and Tracking:
    a. ChatGPT retains user data, including inputs and outputs, for a limited period and uses this data to train and improve their models. Using the OpenAI website allows them to gather usage data and analytics.

    ChatGPT can be a helpful tool and it is important to be aware of its limitations and potential risks, particularly concerning the trustworthiness of the information provided. It is essential to verify any information from ChatGPT using reliable sources and to treat the AI-generated responses with caution.

Recommendations for Library Staff Use:

With consideration of existing City and MPL policies on staff use of IT equipment and software, staff should adhere to the following recommendations when using ChatGPT or other LLMs:

1. When creating an account for ChatGPT or other LLMs for work purposes, staff should use their @milwaukee.gov email account.
2. Any work product developed in ChatGPT or other LLMs must be stored using existing and approved systems (e.g. Network Drive)
3. Staff will not disclose any confidential or proprietary library information in the course of using ChatGPT or other LLMs. This includes internal staff communication, staff information, patron information, and any library information that is protected under Wisconsin State Statutes.

Resources:
- "[ChatGPT is Temporarily Banned in Italy Amid an Investigation Into Data Collection](#)" NPR; March 31, 2023
- ChatGPT:
  - [ChatGPT (OpenAI) Privacy Policy](#)
  - [ChatGPT (Open AI): What is GPT?](#)
- [Eight Things to Know about Large Language Models](#) by Samuel R. Bowman outlines information on the field of modern LLMs.
- "[OpenAI CEO Admits a Bug Allowed Some ChatGPT Users to See Others' Conversation Titles](#)" CNBC; March 23, 2023
- Videos on Future with AI:
  - [Tom Scott - Everything is About to Change](#) (15:49)
  - [Hank Green - The Coming AI Invasion](#) (3:54)
  - [Adam Conover - AI is BS](#) (25:15)