WeirFoulds LLP

To Use or Not to Use: Navigating Privacy Risks Associated with Generative AI Tools

October 4, 2023

By James G. Kosa, Vipal Jain

By now, you may either have heard of generative artificial intelligence (AI) tools or put them to the test yourselves. Generative AI tools like ChatGPT, Cohere, and DALL-E2 are popular tools that allow organizations to generate images, text, sounds and creative content based on a prompt. While these tools can provide practical benefits such as improved efficiency and productivity, they raise privacy risks which are important to mitigate.

In a simplistic sense, generative AI tools work by creating new content from a large language model, which is trained on a very large set of data. The content is created in response to the user's input prompt in a manner akin to autocomplete text prediction tools which predict the next word in your sentence based on the words that precede it. While most of the dataset for tools such as ChatGPT comes from the internet, many generative AI tools explicitly state that user input could be used to train the model as well, forming part of that training dataset.

Privacy Provisions Raise Concern

Privacy concerns arise if the data inputted in generative AI tools contains confidential information or personal information, such as names, addresses, contact information, financial information, medical records, or other identifiers. For example, if an employee inputs a confidential agreement containing personal information into the tool requesting that it simply be summarized, that sensitive information is made available to "train" the tool. The sensitive information could be incorporated into the large language model, and when used in the future, some of that data could reemerge in some form as output in response to another query. The organization would be found offside of privacy laws if it does not have proper consents in place that allow for such additional uses. Something else to be cautious of is the 'mosaic effect.' While one innocuous piece of input data may not reveal any personal and/or sensitive information in itself, it could reveal this when combined with other information collected by the generative AI tool.

When using these technologies, whether they are free and publicly available or require a license to use, users typically agree to terms of use, which can raise concerns for organizations regarding the use of their input data. For example, OpenAI, the AI research company behind ChatGPT states explicitly in their Privacy Policy[1] that it may use personal information, including such information found in input data, for various purposes such as:

- to provide, administer, maintain and/or analyze the services;
- to improve its services and conduct research; and
- to develop new programs and services.

Additionally, OpenAI's Privacy Policy states that in certain circumstances, it may provide personal information to third parties without further notice, unless required by the law. These third parties may include vendors, service providers, successors, or affiliates of OpenAI. The Privacy Policy provides some general examples of vendors and service providers (e.g., cloud services, information

technology service providers, web analytics services) but beyond that, the Privacy Policy does not specify who the particular vendors and service providers are or what specific services are being provided by them.

How to Protect Against Privacy Risks

Here is a list of ways to help protect against privacy risks arising from generative AI tools:

- **Exercise Opt-out Clause**: Consider exercising an 'opt-out' clause, if available, when using a generative AI tool to keep your input data from being used as training data. Unfortunately, even if an 'opt-out' option exists, certain risks may still remain. Input data is still at risk of being disclosed to third parties if the terms of use or privacy policy governing generative AI tool allows for this.
- **Avoid Inputting Personal and Confidential Information**: By not inputting personal and confidential information in a generative AI tool, you avoid the risk of such data being used as training data and being disclosed to third parties. You also reduce the risk of being offside privacy laws, particularly where proper consents have not been collected to permit such additional uses.
- **Develop a Generative AI Policy**: Organizations can proactively help address the risks associated with generative AI tools by developing a generative AI policy. This can help establish clear requirements for responsible use of generative AI tools, ensure compliance with legal requirements and best practices and reduce the potential for misuse. Additionally, a generative AI policy can help provide a framework for continuous monitoring and set out the consequences for failing to comply with requirements.
- **Training Staff**: In addition to developing a generative AI policy, consider training staff on the responsible use of generative AI technologies. Not only would this empower staff with the knowledge and skills needed to handle generative AI tools, the training would also help reduce the risk of data breaches. Additionally, the training would promote a culture of transparency and accountability by helping staff understand their role with respect to the use of generative AI tools.

If you have questions or need further support to protect against the use of generative AI tools, please contact us.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

[1] At the time of publication, Open AI's Privacy Policy was last updated on June 23, 2023.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

Vipal Jain

Toronto
416.619.6294

Email:
vjain@weirfoulds.com

Vipal's practice focuses on privacy and technology matters. She advises organizations across various sectors on matters relating to privacy law compliance, technology contracting, cybersecurity incidents and artificial intelligence.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035

© 2025 WeirFoulds LLP