MILLER CANFIELD

Artificial Intelligence in the Workplace: Spotlight on Confidentiality Concerns

February 22, 2024

Generative artificial intelligence ("GAI") has the potential to revolutionize efficiency and productivity in our day-to-day working lives. But while this technology is becoming more sophisticated by the day, companies should still proceed with caution when using GAI in a workplace setting due to its potential impact on confidential and proprietary information. Almost every workplace houses some type of sensitive or confidential information, such as personnel files, financial data, proprietary and/or trade secret information.

Corporations and employers should understand the risks of inadvertent disclosure of confidential information that workplace use of GAI may pose, so that they are best prepared to assess and manage those risks.

Confidentiality Concerns When Using GAI Tools in the Workplace

- Many GAI systems, including ChatGPT, are "public facing" tools, meaning any member of the public can use them without restrictions. Further, anything typed into a GAI system by a user will be utilized by the GAI to respond to future queries by members of the public. If you or your employees are using this type of GAI in the workplace, there is potential for your confidential information to get out into the public. Once your confidential information is entered into a public GAI tool, there is likely no "un-ringing that bell," and no telling where the information may go or who may be able to use it.

- Workplace use of GAI may also raise concerns for third-party confidential information in your company's possession. Suppose, for example, your company received confidential information from a potential business partner subject to a non-disclosure agreement (NDA). Inputting that third-party confidential information, or any part of it, into a GAI-tool query risks violating the NDA.

- Almost every workplace relies to some extent on third-party vendors (data-storage centers, engineering subcontractors, healthcare systems, etc.) who may themselves be using GAI tools. If you have provided a third-party vendor with confidential information to perform work for your company, the vendor knowingly or unknowingly might risk disclosing the information depending on the type of GAI tools it employs.

- Inputting confidential information into a public GAI tool may have implications for attorney-client privilege as well. If your company's users draw on otherwise attorney-client privileged communications with the company's counsel to formulate GAI queries, there may be an argument that your company has waived the attorney-client privilege by disclosing the information to a third party.

Tips for Preserving Confidential Information When Using GAI in the Workplace

While each company's confidentiality concerns regarding GAI will be unique and context-dependent, you may want to consider the following general best practices when using GAI in the workplace:

- Develop, implement, and regularly update company policies regarding workplace use of GAI. Train GAI users throughout your company on the risks GAI use poses for disclosure of confidential information, and develop specific GAI use protocols designed to minimize risk.

Continued

- Rather than using a public-facing GAI tool, consider implementing a "closed" system that is trained solely on your company's data and does not feed your company's data or company user queries back into the public domain.
- Do your due diligence with respect to your third-party vendors' use of GAI. Understand how, or if, your vendors are using your company's confidential information in tandem with GAI tools and develop clear agreements with your vendors to place restrictions on such use as necessary.
- Consider executing NDAs or related contractual provisions addressing employee use of your company's GAI.

Please contact your Miller Canfield attorney or one of the authors of this alert if you would like to discuss your specific GAI-related legal service needs.