Your Trade Secrets and Confidential Information Could Be Inadvertently Disclosed Using AI Tools

Client Alert
5.8.2023

It was bound to happen. The recent news that Samsung engineers inadvertently disclosed trade secrets by submitting them to ChatGPT serves as yet another reminder of the evolving risks associated with using AI tools[1].

At the time, Samsung did not prohibit its engineers from using ChatGPT. In one instance, an engineer used ChatGPT to optimize test sequences for identifying faults in Samsung's chips. These test sequences were confidential because they save chip manufacturers time when testing and verifying chips, leading to cost reductions and a competitive advantage over prior sequences. In the second instance, an employee asked ChatGPT to convert a confidential meeting into a presentation. In accordance with its policies, ChatGPT retains inputted user data to further train itself. So the confidential test sequences and meeting notes are now on ChatGPT's servers, making them impossible to retrieve.

Tools based on large language models, like ChatGPT, also typically use provided input and subsequent responses to further hone the performance of the system itself. For example, ChatGPT's Help page acknowledges that "conversations [between users and ChatGPT] may be reviewed by our AI trainers to improve our systems." Users can request deletion of their conversations in the event of an inadvertent disclosure. There also is a "User Content Opt Out Request" which appears to allow a user to opt out from use of the user's provided input to improve the ChatGPT models. *Id*.

Even if ChatGPT kept all users' data private and didn't use user input to improve its own system, like any complex computer system, ChatGPT itself may still be vulnerable to attacks that can expose internal data that ChatGPT intended to keep private. Such a breach recently happened, in which some ChatGPT users

Related People

Aaron Kamlay
Shareholder

Daniel G. Vivarelli, Jr.
Shareholder

Related Services

Artificial Intelligence

Intellectual Property

Trade Secrets Theft

were able to see titles from other users' chat histories. Since ChatGPT can auto-generate those titles based on user input, even this seemingly minor breach could lead to exposure of confidential information that was provided by those users.

Furthermore, countless other services provide intermediary interfaces to ChatGPT and new ChatGPT-like services are becoming available every day, not all of which may have even the same options for protecting user-submitted data that ChatGPT provides. Those same services also may have privacy policies that allow data to be shared with affiliates, partners, or even for advertising purposes, further muddying the issue of how broadly confidential information may be disseminated.

Once trade secret or confidential information is provided to a tool like ChatGPT, it can be difficult – if not impossible – for the end user to determine whether the information is no longer truly confidential or has lost some degree of trade secret protection due to the disclosure. This problem can be compounded if separate third-party interfaces or connectors to the underlying AI tool are used, which also would have access to the confidential information and may disseminate the information further than expected by the end user.

Stories like this, in combination with the recent explosion of AI tools, should prompt companies to develop clear policies for use of AI tools. In the meantime, it would be wise to assume nothing submitted into any AI tool can remain confidential, and to consult your Butzel attorneys to understand the relevant risks and develop clear guidelines for use of these and similar tools in the future. And bear in mind that, as AI tools evolve and improve, companies may need to implement policies that permit use of AI tools to stay competitive.

Daniel Vivarelli
202.454.2841
vivarelli@butzel.com

Aaron Kamlay
202.454.2877
kamlay@butzel.com

[1] ChatGPT is technically a chat interface to a large language model (LLM), a type of neural network specifically used to process and generate text. For simplicity and following common shorthand, we'll refer to ChatGPT and similar tools as "AI tools".