# Corporate Insights: How to Protect Your Company in the New World of AI

BY MMAICHLE • OCTOBER 31, 2023

The new technology advancement using artificial intelligence ("AI"), ChatGPT (Chat Generative Pre-Trained Transformer) is a computer model that uses machine learning to generate relevant responses that mimic human-like conversations. According to a February 2023 analysis by Swiss Bank UBS, ChatGPT is the fastest-growing app of all time. The analysis estimates that ChatGPT had 100 million active users in January 2022, only two months after its launch. For comparison, it took nine months for TikTok to reach 100 million users. With its widespread use, corporate counsel should be aware of the risks of using of AI and ensure that those risks are mitigated as much as possible for the company.

One concern is that ChatGPT (and similar machine learning platforms) is still in its infancy. Although there are millions of users, ChatGPT launched less than a year ago and through its own admission, is still in the testing phase. There is simply not enough data to ensure its accuracy. Indeed, the data in the base model does not consider data prior to 2021 (paying subscribers have the ability to use real-time data via a Bing plug-in) and also does not have access to real-time information or knowledge beyond its training data. This leads to inaccurate results.

Privacy and confidentiality in using ChatGPT are also concerns. ChatGPT records every conversation and shares that information with other companies and its AI trainers. When an employee types confidential information into the dialog box, it's recorded and saved on ChatGPT's servers. If that data contained a trade secret of the company or personal information of another employee, the information is now used in new ChatGPT searches, exposing the company to data privacy breaches. For this reason, companies such as Amazon and Apple have largely restricted employee use of ChatGPT.

ChatGPT also creates ethical issues, such as bias. Language models like ChatGPT are trained on vast amounts of data, which can inadvertently introduce prejudice in the training data. OpenAI, the owner of ChatGPT, states on its website, "[w]hile we have safeguards in place, the system may occasionally generate incorrect or misleading information and produce offensive or biased content" (emphasis added). Such biases, if relied upon, could lead to discrimination claims within an organization.

The last major concern is data security. ChatGPT can be exploited by malicious actors to develop programs and platforms that mimic others. These actors can also use the chatbot to create applications meant to install malware on users' devices. Additionally, phishing emails become harder to notice because ChatGPT can mimic a person. This puts companies at greater risk for cyberattacks. While corporate counsel cannot eliminate these risks within a company, the risks can be mitigated by putting in place some processes and procedures.

 

- Corporate counsel should draft polices about acceptable use of ChatGPT. These policies should include internal use and external use. Think of this similar to corporate policies around internet usage. Among other things, the policy should include language about validating the ChatGPT data and using confidential information.
- Companies should invest in comprehensive training and awareness programs to educate employees about the responsible and secure use of AI tools like ChatGPT. This training should cover topics such as data protection, confidentiality, privacy best practices, and the potential risks associated with AI-powered technologies.
- Make sure IT has additional safeguards in place and routinely audits such safeguards. For example, some companies have created a custom pop-up notice about security each time an employee uses an AI platform. By doing so, security teams can mitigate these risks and help safeguard against potential security breaches.

These three steps can help corporate counsel protect its company from misuse of ChatGPT.

This article was originally published in the *ACC-Northeast FOCUS Newsletter* and it is reprinted with permission.

 