

ChatGPT in the Workplace—A Legal Minefield! What You Need to Know to Protect Your Business



Devin Bates
dbates@mwlaw.com
(501) 688.8864

05/08/2023

As artificial intelligence (“AI”) technology continues to advance, more and more people are logging on and experimenting with the technology. ChatGPT, one free and popular AI, is reportedly the fastest-growing consumer application in history.^[1] But it is also ripe for abuse in the workplace. For example, there have been reports of employees farming their job out to ChatGPT and then using their free time to take on a second job.^[2] While these tools can increase efficiency and productivity, they also come with risks and legal implications, particularly when used in the workplace and especially when used without guidance from employers.

What You Need to Know About How ChatGPT Works

While the technology is quickly evolving and there are many models out there, the one seemingly most prone for overuse at present is ChatGPT. A person can access the free service online, and feed it prompts, information, documents, data, etc. The computer takes all of the input, runs it through a black box (that virtually no one knows anything about), and then produces output. What happens to your information, documents, data, etc., and what exactly it relies upon to produce output, is largely unknown. But it is safe to say that the input fed into the machine educates the machine to enable it to assist you and other users in the future.

How Generative AI Models Such as ChatGPT can be Used in the Workplace

There are myriad ways that generative AI could be used in the workplace, especially if employees are left to their own devices to make decisions about applying the new technology. We are not necessarily endorsing these uses, but we are merely identifying them as a few that employees may attempt. Those uses could include:

1. **Customer support:** ChatGPT can be trained on frequently asked questions and customer inquiries to provide quick and accurate responses to customers. This can reduce the time required by customer support staff, speed up responses, and in theory improve the customer experience.
2. **Document analysis:** ChatGPT can be used to analyze and summarize large volumes of documents, such as legal contracts or financial reports. This can reduce the employee time required to identify key information and make informed decisions.

3. **Writing assistance:** ChatGPT can be used to assist employees with writing tasks, such as drafting emails or memos. ChatGPT can provide suggestions for sentence structure, grammar, and word choice to help employees write more clearly, effectively, and rapidly.
4. **Knowledge management:** ChatGPT can be used to create a knowledge base for employees, where they can ask questions and receive answers on a variety of topics. This can help new employees quickly get up to speed on company policies and procedures, and allow existing employees to access information more quickly and easily.

Steps that Employers Can Take To Mitigate Risks

As an employer, it is important to understand the potential risks associated with the use of generative AI, ChatGPT, and other Large Language Models (“LLMs”) in the workplace. Here are some steps you can take to limit liability:

1. **Develop a policy:** Create a policy that outlines how generative AI including ChatGPT and other LLMs can be used in the workplace. Clearly define what types of information can and cannot be shared through these tools, and specify who is authorized to use them.
2. **Provide training:** Make sure your employees are trained on the proper use of generative AI. This includes understanding the risks associated with these tools and how to avoid potential legal pitfalls. Depending on your industry and the types of confidential information in your possession, special retraining should be provided with regard to confidentiality and privacy. Especially if your business is in possession of HIPAA, FERPA, GLBA, FCRA, COPPA, ECPA, VPPA, and/or DPPA protected information, or any other sensitive information, retraining employees on their obligations in light of this new technology will be important. Also retrain employees about the policies and procedures for handling sensitive business information and corporate intellectual property.
3. **Review regulations and ethics rules:** If your profession is governed by regulations, and/or if you operate under a code of ethics, it is wise to review these controlling rules in light of this new technology. Articles online can only take you so far, and you need to ensure that your response to generative AI is tailored to the unique needs of your business, and the unique laws of each state.
4. **Monitor usage:** Regularly monitor employee use of generative AI platforms to ensure compliance with company policies and legal requirements. This can be done through monitoring software or regular audits.
5. **Limit access:** Restrict access to certain platforms to only those employees who have a legitimate business need for them. This can help minimize the risk of sensitive information being shared inappropriately. If you end up being one of the employers that has banned ChatGPT all together,^[3] back up that ban with a program that limits access.
6. **Make appropriate disclosures, and obtain consent:** To the extent that your business elects to allow employees to use generative AI models, consider whether that requires disclosure to your customers, and specifically consider whether that requires their informed written consent. If confidential information is proposed to be shared through online AI models, obtaining this consent is likely prudent.
7. **Protect against the rogue employee:** Have appropriate non-compete, non-solicitation, confidentiality, and/or other agreements in place to protect against any rogue employee who decides to share confidential information through generative AI,^[4] or who decides to use their new found free time to act disloyally.^[5] Some of these protections may require a special

agreement, and other parts of this can be handled through a comprehensive review of your employee handbook. Just don't let ChatGPT write those for you!

8. **Consult with legal counsel:** Finally, consider consulting with legal counsel to ensure that your policies and procedures are in compliance with all applicable laws and regulations.

In conclusion, generative AI including ChatGPT and other LLMs can be valuable tools for businesses looking to increase efficiency and productivity. However, they also come with legal risks and implications that must be carefully considered. By developing clear policies, providing training, monitoring usage, limiting access, and consulting with legal counsel, employers can help limit their liability and ensure that these tools are used appropriately in the workplace.

[1] <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>

[2] <https://www.businessinsider.com/chatgpt-second-job-overworking-overemployment-2023-4>

[3] <https://www.nbcnews.com/tech/tch-news/samsung-bans-use-chatgpt-employees-misuse-chatbot-rcna82407>

[4] <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/#:~:text=On%20April%206.,to%20ChatGPT%20to%201024%20bytes.>

[5] <https://www.businessinsider.com/chatgpt-second-job-overworking-overemployment-2023-4>