# Does Your Company Need a ChatGPT Policy? Probably.

**February 8, 2023**

ChatGPT is an AI-language model developed by OpenAI that was released to the public in November 2022 and already has millions of users. While most people were initially using the publicly available version of ChatGPT for personal tasks (*e.g.*, generating recipes, poems, workout routines, etc.), many have started to use it for work-related projects. In this Debevoise Data Blog post, we discuss how people are using ChatGPT at their jobs, what are the associated risks and what policies companies should consider implementing to reduce those risks.

## How Employees Are Using ChatGPT at Work

Dozens of articles have been written about how ChatGPT will replace certain jobs. But, at least for now, it appears that ChatGPT is not replacing workers, but rather, increasing their productivity. Here are some examples:

- **Fact-Checking**: Employees are using ChatGPT in the same way that they might use Google or Wikipedia to check facts in documents that they are either producing or reviewing.

- **First Drafts**: ChatGPT can generate drafts of speeches, memos, cover letters and routine emails. When asked to write this blog post, ChatGPT came up with several helpful suggestions, including "Employees using ChatGPT must undergo training to understand the tool's capabilities and limitations, as well as the best practices for using it in the workplace."

- **Editing Documents**: Because it is a language model that was trained on millions of documents, ChatGPT is very good at editing text. Employees are taking poorly worded paragraphs and having ChatGPT fix grammatical errors, provide more clarity and generally increase readability.

- **Generating Ideas**: ChatGPT is surprisingly good at generating lists. For our upcoming webcast on the role of ChatGPT in the legal profession, ChatGPT came up

with questions about maintaining privilege, checking for accuracy and disclosing the role of ChatGPT to clients and courts.

- **Coding**: Two of the most common uses for ChatGPT at work are generating new code and checking existing code, with many programmers saying that ChatGPT has made them much more efficient and productive.

## Risks of Using ChatGPT at Work

- **Quality Control Risks**: As impressive as it is, ChatGPT can produce inaccurate results. When drafting sections of a legal brief, it sometimes cites to cases that are irrelevant or do not exist. Because it is a language model, it often struggles with computational tasks and can give incorrect results when asked to solve basic algebra problems. OpenAI is well aware of these limitations. Indeed, ChatGPT itself often issues warnings that it might generate incorrect information. It also has gaps in its knowledge about world events that occurred after 2021. These risks may be lower when the person reviewing ChatGPT's outputs can easily spot and correct these kinds of errors. But if the reviewer is not able to easily identify what is wrong with (or missing from) ChatGPT's response, or there is no person reviewing it at all, then the quality control risks increase. How significant these risks are depends on the use case. For example, the risk is lower when it is summarizing news stories on a particular topic for internal awareness than it would be for generating essential code for the core operations of the company's information systems.

- **Contractual Risks**: There are two primary sources of contractual risks associated with the use of ChatGPT for work. *First*, there may be restrictions on the company's ability to share customers' or clients' confidential information with third parties including with OpenAI through ChatGPT. *Second*, the sharing of certain client data with ChatGPT may also violate contractual provisions with those clients regarding the purposes for which their data can be used. In conducting this analysis, companies should keep in mind that the usage rights for ChatGPT are set out in multiple documents including the Terms of Use, Sharing & Publication Policy, Content Policy, and Usage Policies, which provide that OpenAI may use content provided to ChatGPT to develop and improve its functionality. It is also important to note that many employees sign up for ChatGPT in their personal capacity, and therefore it is not entirely clear to whom these terms apply.

- **Privacy Risks**: Similar to some of the contractual risks, sharing personal information about customers, clients or employees with OpenAI through ChatGPT can create privacy risks. According to the ChatGPT FAQ, OpenAI may use ChatGPT

conversations for training purposes and to improve its systems. Depending on the nature of the personal information being shared with ChatGPT, companies may have obligations to update privacy policies, provide notices to customers, obtain their consent and/or provide them with opt-out rights, etc. These obligations may stem from U.S. state or federal privacy law, and companies should consider the evolving interpretation of automated decision-making, profiling and other related concepts under the 2023 state privacy laws. Uses of ChatGPT that involve personal data also raise questions about how companies—and in turn OpenAI—might approach deletion rights or requests to remove data from their ChatGPT-generated workstreams or the model itself.

- **Consumer Protection Risks**: If consumers are not aware that they are interacting with ChatGPT (as opposed to a human customer service representative), or they receive a document from a company that was generated by ChatGPT without that being clearly disclosed, there is a risk of claims of unfair or deceptive practices under state or federal law (aside from the obvious reputational risks). Depending on the circumstances, clients may be upset if they paid for content that they later learn was generated by ChatGPT but was not identified as such.

- **Intellectual Property Risks**: The use of ChatGPT raises several complex IP issues. *First*, to the extent that employees use ChatGPT to generate software code or other content, that content may not be protectable by copyright in many jurisdictions since it was not authored by a human being. That is currently the position of the United States Copyright Office, although the requirement for human authorship is under challenge in recently filed litigation. *Second*, there is risk that ChatGPT and any content it produces may be deemed a derivative work of copyrighted materials used to train the model. If that view prevails, software code, marketing materials and other content generated by ChatGPT may be found infringing, particularly if such content looks substantially similar to the copyrighted training data. In addition, to the extent that employees submit confidential code, financial data, or other trade secrets and confidential information into ChatGPT for analysis, there is a risk that other users of ChatGPT may be able to pull that same data out, thereby compromising its confidentiality and potentially supporting an argument that such data was not the subject of reasonable steps to preserve its confidential status. *Finally*, if software submitted to ChatGPT includes open source, it is worth considering whether such submission could be deemed to constitute a distribution that may trigger possible open source license obligations.

- **Vendor Risks**: Many of the risks described above also apply to company data that is provided to or received from vendors. For example, should contracts with vendors specify that information provided by the vendor to the company cannot be

generated by ChatGPT without prior consent? Should contracts also specify that confidential company data cannot be entered into ChatGPT?

## Ways to Reduce ChatGPT Risks

Given these legal, commercial and reputational risks, some companies have started to train their employees on the proper use of ChatGPT and draft policies on the use of ChatGPT for work. Training should alert employees to the reality that ChatGPT is not perfect and results from a query to ChatGPT should still be verified using traditional means. The policies surrounding ChatGPT tend to divide ChatGPT uses into three categories: (1) uses that are prohibited (*e.g.*, using ChatGPT to check for mistakes in confidential company or client documents, or sensitive company code); (2) uses that are permitted with authorization from some designated authority (*e.g.*, generating code, so long as it is carefully reviewed by an expert before being implemented); and (3) uses that are generally permitted without any prior authorization (*e.g.*, creating purely administrative internal information such as generating ideas for icebreakers for new hires). In addition, companies are taking steps to reduce the risks associated with the use of ChatGPT, including the following:

- **Risk Rating**: Creating a set of criteria for assessing whether a particular ChatGPT use is low, medium or high risk (*e.g.*, will confidential company or client information be shared with ChatGPT, will the output be shared with clients, etc.?).

- **Inventory**: Requiring that all uses of ChatGPT for work be reported to a team that keeps track of these uses and evaluates them as either low, medium, or high risk based on established criteria (updating the criteria as appropriate).

- **Internal Labelling**: For certain uses, requiring users to mark content generated by ChatGPT with an easily identifiable label, so that reviewers know to pay extra attention to these materials.

- **External Transparency**: Clearly identifying content that was created by ChatGPT when sharing it with clients or publicly.

- **Record keeping**: For high-risk uses, maintaining a record of when the content was generated and the prompt that was used to generate it.

- **Training**: Providing periodic training for employees on both acceptable and prohibited uses of ChatGPT, based on experience at the company and other organizations.

- **Monitoring**: For certain higher-risk use cases, deploying tools (including those created by OpenAI or other providers of generative AI models) to determine whether information was generated by ChatGPT or other AI tools in violation of company policy.

* * *

Please do not hesitate to contact us with any questions.

**NEW YORK**

Megan K. Bannigan
mkbannigan@debevoise.com

Avi Gesser
agesser@debevoise.com

Henry Lebowitz
hlebowitz@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Benjamin Leb
bjleb@debevoise.com

Jarrett Lewis
jxlewis@debevoise.com

Melissa Muse
mmuse@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

Lex Gaillard (Law Clerk)
adgaillard@debevoise.com

ChatGPT