Clark Hill

Your Employees Are Using ChatGPT and Other LLMs: Risks and Legal Implications of ChatGPT in the Workplace

April 14, 2023

Authors

Myriah V. Jaworski , Chirag H. Patel

ChatGPT's recent public debut caused a public stir with commentators imagining the tool's ability to both streamline individual workflows and reduce workforces. ChatGPT is one type of a large language model (LLM) that understands and can respond to natural language prompts.

Some individuals have moved quickly to leverage ChatGPT for work-related tasks, even where the use is not expressly sanctioned by their organizations. More commonly, organizations are realizing after the fact that organizational information, sometimes proprietary, confidential, or regulated information, has been input into ChatGPT or other publicly available AI large language models by its employees.

On April 11, 2023, the President announced the initiation of a study regarding potential accountability measures for artificial intelligence (AI) systems, particularly the impact of those systems on national security and education.

In this post, we discuss how individuals and organizations are using ChatGPT to assist with work-related tasks, and how to address the associated risks and legal implications of ChatGPT or LLM use in the workforce.

How ChatGPT is Being Utilized

Uses of ChatGPT to automate or streamline work-related tasks include:

- Creating and drafting content. ChatGPT is frequently used to generate content for anything from informational blog posts to research reports, including citations to (sometimes fake) underlying resources.
- Generating documents and drafts. ChatGPT is able to quickly generate letters and simple documents with minimal inputs, or convert large text into digestible responses and answers to questions. Additionally, ChatGPT is able to review, improve, and rephrase existing text.
- Fact-checking and research. ChatGPT is able to quickly scrape the internet or specific websites to find answers to questions (again, sometimes wrong). Some users rely on this functionality to automate manual research tasks.
- Generating lists. ChatGPT is able to quickly consolidate large amounts of data and generate concise lists.
- Coding. ChatGPT is able to generate simple code snippets as well as automate iterative but redundant coding tasks.

The Risks of ChatGPT

- Quality control and reliable use: While ChatGPT can research the internet for information quickly, the quality of its output directly relies on the dataset it relies on to generate its response. ChatGPT has documented issues with relying on unreliable or made-up sources and producing incorrect results. Moreover, ChatGPT's responses are influenced by user feedback. In some instances, users have convinced ChatGPT that an inaccurate answer is correct. Thus employers should consider the relative risk of allowing employees to rely on ChatGPT or LLM research and analysis (*g*., when asked to summarize a document the reliance on ChatGPT's research and analysis is low). The higher the reliance, the more the employee should be required to manually audit ChatGPT's responses for accuracy.
- Contract obligations, including confidentiality: If the user's inputs into ChatGPT include data obtained from a customer or other third party, the use of this information with ChatGPT may violate contractual obligations. Any user inputting confidential information or personal information into ChatGPT should carefully consider the source of that information and whether any contract prohibits the use or sharing of that information that is inconsistent with the data's use in ChatGPT.
- Privacy obligations: Users inputting personal or customer data into ChatGPT should also consider how that use impacts their obligations under any privacy law that the organization is subject**.** More specifically, organizations may need to update privacy policies to identify ChatGPT as a source to which information is disclosed (and how that information is used) and provide the user deletion and opt-out rights.
- Consumer protection claims: Customers receiving work product created with the assistance of ChatGPT may claim the failure to disclose that fact was false and deceptive. To avoid such claims, the organization should consider affirmative disclosure and consent, or appropriate waivers.

- Intellectual property risks: There are complex and unresolved questions around whether documents or code generated entirely or with the assistance of ChatGPT are entitled to legal protection. Indeed, the United States Copyright Office's current position is that non-human authored works are not entitled to copyright protection. On the other side of the coin, writings that are produced by ChatGPT that are derived from protected publications may be deemed to be infringing on the original author's works. Also, as discussed above with contractual provisions, inputting proprietary or trade secret information into ChatGPT could be deemed a disclosure or failure to protect that information.
- Insurance: Insurance underwriters are beginning to consider how the use of AI within an organization creates additional risk. Thus, using AI, particularly when not surrounded by adequate guardrails, may increase the costs of insurance premiums.

Risk Mitigation

Given these significant risks, organizations should affirmatively form policies around the use of ChatGPT by employees within the organization. To mitigate risk, the organization should employ the following strategies:

- Create a policy around acceptable AI internal use: Conduct a risk analysis as to the various ways ChatGPT could be employed within the organization and form an acceptable use policy based on the organization's risk tolerance.
- Track internal use: Require employees to disclose the ChatGPT in any work product, and then maintain an inventory of any work product that utilized ChatGPT for easy identification
- Disclosure, consent, and contract compliance: Determine where it is necessary to disclose the employment of ChatGPT with consumers and contract parties to avoid claims of authorized disclosure or breach of contract. Where necessary, obtain appropriate consent. The type and level of consent will depend on the context; changes in law may impose specific consent requirements.
- Audits, training, and monitoring: Continue to monitor the use of ChatGPT with conformity to the acceptable use policy, unanticipated and new uses, and changes in legal requirements. The organization should also conduct regular training to keep employees informed of the acceptable uses of ChatGPT, and the risks to the organization of authorized uses.

As mentioned above, the President announced a new study surrounding AI technologies like ChatGPT, that may lead to the regulation of the use of those technologies. Contact counsel to determine if your organization is subject to legal or regulatory requirements for the use of any AI, ML, LLM tools.

Related Practice Areas

Cybersecurity, Data Protection & Privacy

Related

Legal Updates

New Jersey Appellate Court Enforces "Pay-if-Paid" Clause Shifting Risk in a Construction Contract

Legal Updates

Right To Know - April 2023, Vol. 5

Cyber, Privacy, and Technology Report

Legal Updates

Department of Education's Proposed Change to Its Title IX Regulations on Transgender Students' Eligibility for Athletic Teams

Also of Interest:

Cybersecurity, Data Protection & Privacy

Tax & Estate Planning

To Contact Or Arrange A Consultation With The...

The Clark Hill approach is equally pragmatic and growth-minded, which is why we understand our clients’ toughest business challenges. Our multidisciplinary, global team of advisors focuses on smart legal solutions, delivered simply.

Contact Us

Policies & Disclaimers

Client Log-in

Payments

Employee Resources