

Top 4 Employer AI Risks And How To Mitigate Them

By **Randi May and John Walpole** (September 1, 2023, 4:04 PM EDT)

The explosive growth of generative artificial intelligence continues to captivate our curiosity.

Generative AI is a type of artificial intelligence system capable of generating human-like text, images or other media in response to prompts.

AI platforms, such as OpenAI, Github Copilot, Claude, and many more, are among the fastest-growing consumer applications in history, with ChatGPT alone reaching over 100 million users in the first two months of 2023.[1]

Employers cannot ignore the fact that their workforce is almost certainly using generative AI to perform or assist with their tasks.

A recent survey conducted by the Boston Consulting Group revealed that nearly half of respondents, 46%, have experimented with generative AI, and 27% stated that they use it regularly to perform their tasks at work.[2]

By late January, 43% of professionals were using AI tools for work-related tasks[3] and 57% of employees reported that it boosts their productivity.[4]

Generative AI offers certain benefits to companies.

For example, it can enhance efficiency and efficacy through automation of repetitive and mundane tasks, which, in turn allows employees to focus on more complex and creative aspects of their jobs. Likewise, AI may accelerate research and development processes by quickly analyzing vast amounts of data.

Overall customer service experiences can also be enhanced through AI-powered chatbots and other tools that provide prompt, personalized services to customers at any time.

However, the use of generative AI by employees to perform their job duties presents significant challenges to their employers.

Generative AI is here to stay, so companies are now left to adapt their businesses, processes and procedures to address this useful, but also potentially disruptive technology.



Randi May



John Walpole

This article highlights the top four risks to consider when making decisions regarding the use of generative AI, and how to mitigate them.

1. The Input Is Not Confidential

The "input," or data or information entered into a generative AI program to be processed and used to generate a response or perform a task, is not confidential.

Once information is entered, the AI platforms retain the right to reuse that input. Consequently, any confidential or proprietary information included in the input becomes publicly accessible within the generative AI platform.

Thus, if a worker inputs any confidential or propriety information, even unknowingly, that information is likely to be included in another user's AI generated content — perhaps even a competitor's.

Moreover, information used as inputs may also violate industry-specific rules or guidance, or applicable contractual or other obligations regarding disclosure.

2. Intellectual Property Issues

The result, response or data produced by a generative AI program after processing the input is referred to as the "output," and it raises issues regarding intellectual property infringement and ownership.

AI systems are trained on enormous amounts of data, including third-party intellectual property, for which advance use authorization has not been obtained. In fact, AI outputs have already caused a flurry of litigation. For example:

- In *Doe v. GitHub Inc.*, filed in the U.S. District Court for the Northern District of California in November 2022, software engineers filed a class action lawsuit against GitHub, Microsoft and OpenAI entities alleging that the defendants trained GitHub Copilot and OpenAI Codex on copyrighted material and licensed code, violating open-source licenses and infringing on intellectual property rights.[5]
- In the Northern District of California, artists filed a class action lawsuit in January — *Anderson v. Stability AI Inc.* — against Stability AI, Midjourney and DeviantArt for copyright infringement over the unauthorized use of copyrighted images to train AI tools, alleging that their artworks were used without consent or compensation.[6]
- In *Getty Images (US) Inc. v. Stability AI Inc.*, filed in the U.S. District Court for the District of Delaware in February, Getty Images alleges that Stability AI infringed upon its copyrights by using Getty Photos to train its AI art-generation platform.[7]

Moreover, the ownership of AI generated intellectual property is unclear, particularly if multiple parties contributed to its development.

Whether existing intellectual property laws apply to outputs has yet to be determined by the courts.

For example, in *Thaler v. Perlmutter*[8], filed in the U.S. District Court for the District of Columbia in June

2022, the plaintiff petitioned the court to overturn the U.S. Copyright Office's decision to deny a copyright for artwork created by "Creativity Machine," an AI platform. The U.S. Copyright Office denied copyright protection to AI generated output, limiting its protection to human work.[9]

Employees' use of generative AI may therefore create exposure to liability for infringement. Additionally, it may cause the loss of copyright or other legal protections in work product that would have been protected if created by a human.

3. Misinformation, Bias and Ethics

Significant media attention has been dedicated to misinformation, bias and ethics in generative AI.

Regarding bias and discrimination, several government agencies and the White House have issued statements and guidance.

For example, the White House's Blueprint for an AI Bill of Rights provides that users "should not face discrimination by algorithms and systems should be used and designed in an equitable way." [10] The Consumer Financial Protection Bureau has proposed a rule to make home appraisal computed by algorithms fairer and more accurate.[11]

Outputs generated by AI platforms may result in false, although authoritative-sounding statements, referred to as "hallucinations." OpenAI even acknowledges that ChatGPT may produce harmful instructions or biased content.[12]

To address this, certain platforms maintain that they have implemented measures to minimize bias and provide respectful, neutral and unbiased outputs.

However, AI systems face challenges freeing their programs entirely from biases as the data the systems were trained on may reflect certain biases. Thus, employees' work product that relied on generative AI which may contain false, misleading or biased content presents significant risks of exposure.

AI use in the workplace also presents ethical concerns:

- Illusorily, in the case of *Mata v. Avianca Inc.*, filed in the U.S. District Court for the Southern District of New York in February 2022, ChatGPT infamously generated fabricated legal citations in a court submission.[13] Another example is that generative AI may disclose or access personally identifiable information.

Additionally, transparency and disclosure are important concerns. Employers should consider whether it wants to, or may even be obligated to, disclose to clients, customers and others that generative AI was used to perform certain tasks.

4. Input and Output Preservation

Absent specific direction to the workforce and information technology personnel, neither input nor output may be preserved. In the litigation context, information associated with generative AI functions may be discoverable.

If not properly preserved, companies could be subject to liability for spoliation. Likewise, generative AI

input and output may be requested by investors and/or in connection with due diligence associated with potential transactions.

What Are Employers To Do?

Companies should address their employees' use of generative AI and make prompt decisions about whether to permit or prohibit their workforce from using generative AI platforms to perform their tasks, in whole or in part.

Companies should then communicate this decision right away and implement training, as may be necessary.

Legal Landscape

While the legal landscape surrounding the use of generative AI is quickly evolving, it remains mostly unspecific, meaning that lawyers are left to figure out how to apply the current legal framework to these issues.

The U.S. Equal Employment Opportunity Commission chair, Consumer Financial Protection Bureau, and Federal Trade Commission released a joint statement, outlining a commitment to enforce their respective laws and regulations to promote responsible innovation in automated systems.[14]

The FTC guidance on companies' use of AI advocates for AI tools to be transparent, explainable, fair and empirically sound.[15]

Specifically, the FTC advises companies to be mindful not to mislead consumers about their use of AI, refrain from secretly collecting sensitive data, consider what data is used in their models and how it is used in decision making. Its guidelines also state that companies should disclose to consumers if the use of an algorithm will change the terms of a deal with consumers.

To address potential discrimination, the FTC advises that companies should self-test algorithms, including both inputs and outputs, to ensure it does not create a disparate impact on a protected characteristic.

The FTC also provides guidance for companies subject to the Fair Credit Reporting Act, such as providing consumers access and an opportunity to correct information used to make decisions about them and providing an adverse action notice when automated decisions are based on information from a third-party vendor.

The Need for an AI Policy

Companies would be well-served by developing and disseminating a policy regarding the use of generative AI in the workplace.

It is vital for employers to carefully review the applicable generative AI platforms' terms of use in order to determine the risks that any particular platform may impose.

Businesses should also consult company stakeholders, such as legal, human resources, compliance, management and IT departments, to identify areas of the business that may potentially benefit from the

use of generative AI.

Once the risks and potential benefits of generative AI in a particular workplace have been evaluated, companies can decide whether, and to what extent, generative AI will be permitted or prohibited. Like all policies, they can always be amended if business concerns or risk tolerances change. In fact, given its rapid evolution and the currently ill-defined legal landscape, AI policies ought to be updated somewhat regularly.

Whatever policy businesses adopt, it is critical that it is clearly communicated to their workforce, and not simply added to an employee handbook residing on an intranet or similar platform.

Likewise, if any use of generative AI will be permitted, companies would be well-advised to train their workers and to update the training as needed.

If permitted, employers may wish to identify which areas of the business may use generative AI, which tasks it may be used for, and/or which platforms are permitted. Alternatively, AI policies can require that workers obtain prior authorization and appropriate review before using generative AI to perform a task.

Policies may also mandate that workers affirmatively disclose that generative AI has been used in connection with a particular assignment. Expectations regarding how to preserve protection of third-party, sensitive, proprietary, and/or confidential information and about intellectual property ownership and infringement need to be clearly set forth in an AI policy.

To address discovery issues in potential litigation and requests for information from potential investors or buyers, companies may want to determine appropriate retention of inputs and outputs.

Regardless of whether uses of generative AI are specifically permitted or prohibited, employers should be prepared for the fact that their workforce may use it in whatever way they determine makes them more efficient.

To this end, companies may wish to conduct periodic audits to ensure compliance with their policy, particularly given the perils that generative AI in the workplace present.

Conclusion

The use of generative AI has exploded, and this includes workers' use to perform their duties.

Although AI offers benefits, its use also presents significant risks. Clear policies regarding its use can significantly mitigate these risks.

Randi B. May is a partner and John F. Walpole is an associate at Tannenbaum Helpert Syracuse & Hirschtritt LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Krystal Hu, ChatGPT Sets Record for Fastest-Growing User Base - Analyst Note, Reuters, (Feb. 2, 2023, 10:33 AM), <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/#:~:text=It%20took%20TikTok%20about%20nine,to%20data%20from%20Sensor%20Tower.>

[2] Vinciane Beauchene, et al., AI at Work: What People Are Saying, Bcg, (June 7, 2023), <https://www.bcg.com/publications/2023/what-people-are-saying-about-ai-at-work>.

[3] 70% of Workers Using ChatGPT at Work are Not Telling Their Boss; Overall Usage Among Professionals Jumps to 43%, Fishbowl, (Feb. 1, 2023), <https://www.fishbowlapp.com/insights/70-percent-of-workers-using-chatgpt-at-work-are-not-telling-their-boss/>.

[4] Eri Panselina, Survey: AI is the Future, but Only 14% of Employees are Being Trained on the Tools, TalentLMS, (Mar. 15, 2023), <https://www.talentlms.com/blog/ai-at-work-chatgpt-survey/>.

[5] Doe et al. v. GitHub, Inc. et al., 22-cv-6823 (Nov. 3, 2022, N.D. Cal).

[6] Anderson et al. v. Stability AI, Ltd. et al., 23-cv-00201 (Jan. 13, 2023, N.D. Cal.).

[7] Getty Images (US), Inc. v. Stability AI, Inc., 23-cv-00135 (Feb. 3, 2023, D. Del.).

[8] Thaler v. Perlmutter et al., 22-cv-01564 (June 2, 2022, D.D.C.).

[9] Re: Zarya of the Dawn, United States Copyright Office, (Feb. 21, 2023), <https://www.copyright.gov/docs/zarya-of-the-dawn.pdf>.

[10] The White House, Blueprint for an AI Bill of Rights, <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.

[11] Rohit Chopra, Algorithms, Artificial Intelligence, and Fairness in Home Appraisals, Consumer Financial Protection Bureau, (June 1, 2023), <https://www.consumerfinance.gov/about-us/blog/algorithms-artificial-intelligence-fairness-in-home-appraisals/>.

[12] Natalie, What is ChatGPT?, OpenAI, <https://help.openai.com/en/articles/6783457-what-is-chatgpt>.

[13] Mata v. Avianca, Inc., 22-cv-01461 (S.D.N.Y. 2023).

[14] Press Release, U.S. Equal Employment Opportunity Commission, EEOC Chair Burrows Joins DOJ, CFPB, And FTC Officials to Release Joint Statement on Artificial Intelligence (AI) and Automated Systems (Apr. 25, 2023), <https://www.eeoc.gov/newsroom/eeoc-chair-burrows-joins-doj-cfpb-and-ftc-officials-release-joint-statement-artificial>.

[15] Andrew Smith, Using Artificial Intelligence and Algorithms, Federal Trade Commission, (Apr. 8, 2020), <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms>.