



Feb 16, 2024

Categories:

[Publications](#)

[Technology Blog](#)

Authors:

[Jean Paul Yugo](#)

[Nagashima](#)

[Ashley J. Earle](#)

[Katelyn E. Moody](#)

Using Generative AI in Manufacturing: Three Key Considerations

This is the second in a series of articles outlining successful approaches to integrating AI into businesses in ways that allow the promise of AI to be realized while minimizing its risks. This article examines the potential of generative artificial intelligence (AI) tools like ChatGPT to enable companies engaged in manufacturing to improve their efficiency and quality of work, as well as the risks for successful AI integrations. When implementing new AI tools, intellectual property rights management, confidentiality protection, and accountability are key issues for manufacturers to consider.

1.) Consider the Effect of AI on Intellectual Property Rights

Generative AI has many implications for intellectual property (IP) ownership and clearance. For example, businesses cannot necessarily “own” outputs created using generative AI tools, in large part because AI-generated content is ineligible for copyright protection unless its creation involved substantive human control. Another essential concern is ensuring an AI output does not infringe on third parties’ IP rights. This section focuses on the ownership considerations for the main “buckets” of IP protection.

Copyright. Manufacturing businesses may be concerned about using generative AI in their daily work routine because of copyright infringement risks. There may be fears that businesses are unknowingly using AI tools that incorporate copyrighted material in generated outputs, leading to copyright disputes over the company’s design of a product or schematics. AI output is driven by a combination of the prompts or the query the businesses enter (AI input) and the specific AI models they use. Businesses can control the AI input by implementing policies prohibiting the organization from entering inputs that copy or are substantially similar to existing artwork, authorship, music, or design (Works). They can also exert some contractual control over the AI model. For instance, businesses can contractually require AI vendors to ensure that AI

outputs do not generate Works that are copies or substantially similar to copyrighted materials.

Businesses trying to protect their AI-generated output must keep in mind that AI-generated Works may not be copyrightable unless the AI output had a substantive amount of human control over the AI-generated content.

Trademark. While an AI output cannot be copyrighted without substantial human contributions, it may be protected under trademark laws. For instance, AI tools may be leveraged to workshop name ideas, create logos, suggest product packaging, or create unique designs. Because trademarks are source identifiers, an AI output may be registered so long as the business continues to use the AI output as a mark for its brand. AI tools can also help monitor and police the brand by identifying products with the same or similar trademarks that may infringe on a company's registered trademark. Establishing solid governance and proper procedures for AI tools can optimize a business's trademark monitoring practices.

Trade Secrets. When using AI tools, manufacturers should be vigilantly attuned to the risks of losing their trade secrets protection. Businesses must implement reasonable measures to keep any trade secret information confidential. For instance, inputting [sensitive corporate information](#) into a publicly available AI system can result in losing trade secret status. This occurs because current generative AI tools do not delineate between sensitive, confidential, and non-confidential information, not to mention that the terms of use for many generative AI tools state that inputted data may be used for AI training purposes. Once sensitive data is ingested, it becomes very difficult to unlearn the trade secret information making such information publicly available. To avoid compromising trade secret protection, businesses should implement company-wide AI usage policies and procedures to prohibit employees from entering confidential and proprietary information in AI tools that are not approved by the company.

2.) Be Aware of Your Confidentiality Obligations

Businesses should review existing agreements, including vendor contracts, for provisions related to how each counterparty's information may be used. For example, information subject to non-disclosure agreements (NDAs) is confidential information that may not be appropriate for use with AI tools. Employees may not appreciate it, but inputting such confidential information in an AI tool could be interpreted as a disclosure under the terms of their NDA. Once NDA-protected information is entered, the AI tool may use the data to train its algorithms. Due to the nature of AI algorithms, it may be difficult to delete such information or for the AI tool to unlearn it. Being aware of contractual confidentiality obligations is key to navigating the age of AI.

3.) Be Transparent and Responsible

Manufacturers should promote transparency and accountability internally when using AI tools. Businesses can promote transparency by labeling AI output or notifying the stakeholders about the use of AI in making certain decisions. They can also make responsible use of AI by implementing procedures that ensure an AI input does not draw from the business's confidential or proprietary information. Similarly, businesses should take care that appropriate licenses and consents are obtained before inputting third-party or personal information into the AI system. Establishing processes to vet AI outputs for inaccuracies or misleading results (hallucinations) is important so that incorrect calculations or assumptions are not mistakenly used by the business.

The best practice for a business is to establish [a robust AI governance program](#) covering all forms of AI throughout the organization and its operations. For manufacturing and other regulated industries, an AI governance program will include an acceptable AI use policy for employees and other protections that address both common and industry-specific risks and that ultimately lead to AI success.

Frost Brown Todd has a dedicated team that advises clients on their own AI integrations, helping them institute governance programs, proactively address data security and privacy concerns, and navigate a host of other AI opportunities and risks unique to

their industry. We would love to help optimize your business by advising on the responsible and safe adoption of AI solutions. For more information, contact the authors or any attorney with the firm's [Artificial Intelligence](#) team.

AI Legally Speaking

Explore the collection of articles below for more AI-related coverage and legal analysis.

- [***Managing Data Security and Privacy Risks in Enterprise AI***](#)
- [***New Expectations for AI: Governance is Key for AI Success in Health Care***](#)
- [***USPTO Guidance Suggests Two Strategies for AI Inventions***](#)
- [***FTC's New Rule on Consumer Reviews: Ensuring Compliance with Human- and AI-Generated Content***](#)
- [***Decoding Colorado's Artificial Intelligence Act***](#)
- [***Investment Management + AI = New Opportunities, Unique Risks***](#)
- [***AI Chatbots, Hallucinations, and Legal Risks***](#)
- [***AI and Energy: Network Innovation and Growth***](#)
- [***AI and Health Care Providers: Managing the Risks with Data***](#)
- [***Will AI Destroy the DMCA Copyright Compromise?***](#)
- [***Three Steps to AI Success for CEOs***](#)

[Learn More](#)

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.