HUSCH BLACKWELL

THOUGHT LEADERSHIP

ARTICLES

PUBLISHED: NOVEMBER 5, 2024

Legal Insights for Manufacturing: Artificial Intelligence

Service

Artificial Intelligence

Industry

Manufacturing

Professionals

ERIK DULLEA
DENVER:
303.749.7270
ERIK.DULLEA@
HUSCHBLACKWELL.COM

OWEN DAVIS
DENVER:
303.749.7268
OWEN.DAVIS@
HUSCHBLACKWELL.COM

This article is excerpted from our third-annual *Legal Insights for Manufacturing* report, published in October 2024.

Manufacturers have been using artificial intelligence (AI) in their operations for years, but recent advances in generative AI—that is, AI that creates new content by learning patterns from existing data—have expanded the scope of what is possible. As use cases proliferate, so, too, do the risks associated with AI, especially as federal, state, and local governments begin crafting regulations to manage its use.

UNDERSTANDING THE VARIETIES OF AI

ARTIFICIAL INTELLIGENCE
A broad term encompassing the development a
computer systems capable of performing tasks
ly require human intelligence.

MACHINE LEARNING
A subset of AI that trains systems to learn from
make decisions or predictions based on pattern

NEURAL NETWORKS
A type of machine learning algorithm that mimi
ture and function of the human brain—allowing
learn and process complex data.

DEEP LEARNING
A subfield of machine learning that uses neural
multiple layers to learn and extract features fro

GENERATIVE AI
A subset of AI that focuses on generating new
as text or images, based on patterns learned fr

Source: Gabriela Jhean, "AI vs Generative AI: What's the Difference?" May 21, 2024

Because AI is a broad umbrella term and different forms of AI use data in different ways, it is important to precisely define AI when performing legal or regulatory risk assessments. At their core, traditional forms of AI and generative AI are similar. In implementation and scope, however, they are very different. For example, traditional AI may be trained on millions of users' video-watching history to suggest what a specific user may like to watch next. Generative AI is trained on hundreds of millions (or even billions) of wide-ranging media to suggest (or generate) new content. Whereas traditional AI may be used to make suggestions among thousands or even millions of possibilities, generative AI is being used to create new content. In the manufacturing setting, that could be new design options that calculate a complexity of factors, such as weight, strength, or specific materials, or production-related tasks.

Intellectual Property and AI

The earliest and most compelling applications of generative AI to manufacturing have involved core operations related to design and production, including rapid prototyping, autonomous operations, and predictive maintenance. As such, cutting-edge legal considerations for manufacturers often touch upon intellectual property (IP), especially given that IP law generally does not protect ideas themselves, but rather the way in which ideas are implemented or take shape. Furthermore, if something is well-known and deemed to belong to the public at large, IP law will not protect it, so as more companies and individuals begin using generative AI, their use creates numerous risks—both to IP that already exists and to the ability to claim new IP.

Manufacturers concerned about the risks presented by generative AI can take several steps to reduce those risks. First, adopt an AI policy that sets out clear guidelines on how AI can (and cannot) be used at your company. The policy should focus not only on what tasks can use generative AI (the output), but what information can be used to accomplish those tasks (the input). Second, perform an audit to determine to what extent your company is potentially disclosing proprietary information to open-source resources, such as GitHub. Third, keep up to date on changing laws that may affect your IP rights. AI's legal and regulatory setting is evolving on an almost daily basis. Finally, create a framework to help you make educated decisions about when it is okay to use new forms of AI (and when it makes sense to consult an outside expert for more information). AI is a rapidly changing area of technology and manufacturers need a framework in place that balances their company's priorities and risk management while allowing the company to use new forms of AI.

AI vendor contracts should also address IP considerations. Every contract should address IP ownership between the parties, including ownership of not only what the manufacturer inputs into the AI solution, but what the solution outputs as well. Because the output may be based on vast amounts of data on which the AI solution trained, the answer to this latter question may be more difficult. If a company provides inputs or prompts to the AI product/service, then the company will

likely want to maintain its ownership rights over that input or prompt. Additionally, if a company's inputs or prompts are used by the AI product/service to create any output, then the company will likely want ownership rights over any output, including any work product or deliverable created from that output. The company should consider at least prohibiting the use of that output from being used for other purposes, including additional training of the AI.

Another ownership consideration is whether the AI vendor's product or service relies on a third party's technology. Many vendors are relying on third-party technology for their own AI models. Companies should require vendors to represent and warrant that the vendor has the right to use the third party's technology through a license and shall comply with all use restrictions under that license. Any representation and warranty should also make it clear that the vendor has full power and authority to grant the rights under the contract to the company.

Finally, for all AI products/services, vendors should also represent and warrant that the products/services will not misappropriate, violate, or infringe any third-party IP rights. Companies should consider indemnification protection for any claims that result from the misappropriation, violation, or infringement of any third-party IP rights and corresponding liability for any indemnification obligation.

HUSCH BLACKWELL

ASSESSING AI RISK BY INTELLECTUAL PROPERTY TYPE: A PRIMER

COPYRIGHTS

- Website copy/image can be protected by copyright if human-created, but not if Gen-AI creates the content.
- Use of Gen-AI can expose a company or individual to claims of copyright infringement.
  - Cases filed to date mostly allege infringement by copyright owners naming the companies who design and program the Gen-AI tools, rather than the end users.
  - Companies that have custom-trained Gen-AI tools could find themselves named as defendants in lawsuits if they use copyrighted material to train those tools.

TRADE SECRETS

- Trade secret definition includes "all forms and types of…business…information" so long as "the owner thereof has taken reasonable measure to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means…"
- Information is significantly less likely to be considered a trade secret when created in whole or in part by Gen-AI.
- If trade secret information is publicly disclosed when used to train Gen-AI, the information will likely be deemed to no longer meet the trade secret definition.

PATENTS

- Assume something generated by Gen -AI technology cannot be protected by patent.
- Although the USPTO has not completely foreclosed the ability to obtain a patent if the inventor use Gen-AI during the invention process, it did reiterate the restrictions that only a natural person can be deemed an inventor.
- Unlike copyright, AI IP lawsuits have not (yet) alleged patent infringement.

TRADEMARKS

- Trademark law has to date been the least affected by Gen-AI.
- Trademark law does not require the word- or design-mark to have been created by a human to receive protection.
- Because Gen-AI tools are trained on existing material, there is a significant risk that any logo or design is confusingly similar to an existing trademark. Use of Gen-AI to create marks which are then used to offer goods and services can present risk of trademark litigation.

Striking Deals Involving AI

When manufacturers opt to utilize third-party AI tools and services rather than attempt to develop those tools internally, it is important to develop a standard process for onboarding the vendor and perform a risk assessment for the technology.[1] As a starting point, companies need to identify key information such as the specific use case and business reason for using the product, the product/service's inputs and outputs, whether the product is being used for a high-risk processing activity, and the vendor's access to company data. If the vendor insists on using its contractual terms, the analysis also should identify whether those terms are negotiable and, if not, whether the company is willing to assume the risk of whatever terms are presented. If the vendor is a start-up, will the company be left holding the bag if the vendor closes shop in the face of thirdparty litigation, regulatory investigations, or business failure?

Although specific terms will depend on the exact use case, terms that typically require definitions are artificial intelligence (or a similar term like AI technology), generative AI, inputs, and outputs. Defining artificial intelligence is particularly important given that it establishes the scope of all obligations.

"Third-party offerings" is another common and significant term if the vendor's product/service will be used in combination with a different vendor's product/service. As touched on above, this is a common occurrence as many AI products/services are built on another vendor's product/ service such as OpenAI. The underlying vendor's terms may alter or nullify any warranties or indemnification provisions and, therefore, require close review.

In addition to defining the key terms, contracts should address obligations and rights regarding inputs (i.e., what information goes into the AI) and outputs (i.e., what information comes out of the AI). With respect to inputs, companies need to consider what data will be provided, whether it will be secured by the vendor, and whether privacy or business proprietary considerations come into play. For example, if the company will input customer data, the contract should address privacy considerations and a data processing agreement may be appropriate. If the company will input business proprietary information, the contract should require the vendor to keep that information confidential and use it only for the company's business purposes. The contract also should address how the vendor can use and share the data, including whether it can use the data to improve or train its product.

Relatedly, depending on the scope of the data shared with vendors, companies should consider adding data breach notification and defense/indemnity clauses if they are not already addressed in the contract or data processing agreement. It is not difficult to imagine that these AI products and services will be a new threat vector for hackers.

For outputs, the contract should address which contracting entity owns the outputs. For example, some AI vendors are now specifically acknowledging ownership issues regarding outputs in

contractual agreements and ancillary materials. Most notably, Microsoft recently updated its consumer Services Agreement to expand "the definition of 'Your Content' to include content that is generated by your use of our AI services." In other words, Microsoft recognizes that the user—and not Microsoft—owns the output. For many manufacturers using third-party technology to design products or production processes, output-specific provisions will require careful scrutiny in order to secure ownership of the relevant intellectual property.

---

[1] Also see "Key Considerations in AI-Related Contracts" by Erik Dullea, Shelby Dolen, Owen Davis, and David Stauss from Husch Blackwell's Byte Back blog.