Legal Considerations for IP in Smart Manufacturing: Data Ownership, Trade Secret Risks, and Patenting AI-Assisted Inventions

May 27, 2026

Key Takeaways

- Adopt a hybrid IP protection strategy: Combine patents for core technical innovations with trade secrets for evolving know-how (like datasets and AI optimization methods), supported by clear contracts that define ownership and usage rights in collaborations.
- Strengthen trade secret governance in AI environments: Mitigate risks from “shadow AI” and data leakage by limiting use to approved tools, enforcing access controls, embedding strong contractual protections, and training employees on safeguarding sensitive information.
- Clarify data ownership and document AI-assisted inventions: Explicitly define data rights in agreements to avoid disputes and ensure patent eligibility by documenting human contributions in AI-assisted innovations, since only natural persons qualify as inventors.

The rapid deployment of artificial intelligence (AI) -driven manufacturing technologies presents a dual challenge for in-house counsel and business leaders: how to capture competitive advantage through innovation while managing the attendant intellectual property (IP) risks. As manufacturers integrate AI-driven robotics, Internet of Things (IoT)-enabled digital twins, and agentic AI systems into their operations, they are generating significant intellectual property assets and exposures that demand proactive legal strategy.

Three questions should keep every manufacturing executive up at night. First: Are we adequately protecting the innovations our engineering and design teams are developing with AI assistance — or are we leaving valuable IP exposed? Second: We're generating massive volumes of operational data, but do we actually own it, and what can we legally do with it? Third: AI tools are proliferating across our workforce, often without oversight — how do we prevent a single employee prompt from exposing our most sensitive trade secrets?

This article, part of Foley's 2026 AI in Manufacturing & Supply Chain Series, distills practical legal frameworks at the intersection of AI innovation and IP protection, with strategies to secure IP rights, mitigate litigation risk, and navigate the contractual and regulatory complexities inherent in smart manufacturing.

1. Intellectual Property Protection Strategies for Smart Manufacturing Technologies

Effective IP management in smart manufacturing requires a layered strategy deploying patents, trade secrets, and contract rights in coordinated fashion. Consider automotive manufacturing: today's vehicles are software-defined platforms more akin to iPhones than to the cars of a generation ago, and automakers must increasingly think like technology companies rather than traditional manufacturers. This shift is emblematic of the broader smart manufacturing landscape, where patents are even more essential for protecting discrete technical innovations, such as novel AI integrations with industrial control systems, proprietary sensor-fusion algorithms, and advances in predictive maintenance. However, many competitive advantages in AI-driven manufacturing lie in iterative know-how and continuously evolving systems. In some cases, such competitive advantages may be better shielded as trade secrets.

Leading manufacturers increasingly employ a hybrid approach: leveraging patent protection to protect core inventions and create licensing opportunities, while leveraging trade secret protection measures to protect training methodologies, proprietary datasets, and optimization parameters. Copyright protection supplements this framework by covering software code and user interfaces, while trademarks safeguard branding around proprietary platforms. However, implementing such a hybrid approach must involve broad awareness of innovations across the company, as well as proper precautions in place to maintain the secrecy of innovations earmarked for trade secret protection.

In multi-party relationships, IP allocation should be addressed explicitly at the outset of any joint development. Governing agreements should clearly delineate background IP (pre-existing assets each party brings to the relationship), foreground IP (jointly developed innovations), and rights to improvements. Field-of-use restrictions, licensing terms, and sublicensing limitations should be negotiated with precision to avoid downstream disputes.

IP due diligence must precede the scaling of any AI tool in manufacturing. With patent filings in AI-for-manufacturing surging globally, manufacturers that rely solely on vendor representations without freedom-to-operate analysis risk costly infringement exposure.

2. Trade Secret Safeguards and Risks in AI-Driven Manufacturing Environments

The integration of AI into manufacturing operations has materially expanded the trade secret attack surface. Generative and agentic AI tools can rapidly codify tacit employee knowledge — process workarounds, optimization heuristics, institutional expertise — into digital form. The appeal of digitization is obvious: critical knowledge at your fingertips, instantly accessible across your organization. But every asset you can access instantly is an asset a threat actor can target. The more information you digitize, the larger your attack surface becomes. And the threat is not theoretical — breaches dominate every news cycle, with threat actors increasingly targeting IoT networks and AI training data.

"Shadow AI" has emerged as a particular concern: employees deploying unvetted generative AI tools that may transmit sensitive data to external servers or use proprietary inputs to train third-party models. The reality is that employees will use AI tools — the question is whether they use approved tools with appropriate safeguards or unsanctioned alternatives that expose the organization. Companies that fail to provide enterprise-approved AI solutions do not eliminate usage; they simply drive it underground, where the risks multiply. In manufacturing environments where production data is routinely shared across partners and platforms, the risk of inadvertent disclosure is acute.

Mitigating these risks requires a layered governance framework:

> **Approved Tools:** Restrict AI tool usage to enterprise-approved, internally hosted, or contractually controlled systems with appropriate confidentiality protections.
>
> **Access Controls:** Implement tiered access controls, data segmentation, and continuous monitoring of AI interactions to detect and limit unauthorized data flows.
>
> **Contractual Protections:** Require robust nondisclosure agreements with all vendors, employees, and contractors, coupled with exit protocols that mandate return or destruction of proprietary information.
>
> **Training and Audits:** Conduct regular trade secret audits and targeted employee training to ensure personnel understand what constitutes proprietary information — and the risks of disclosure through AI tools.
>
> **Need-to-Know Policies:** If information is not germane to the relationship, there is no reason to share it — regardless of the protections that may be available. The most effective trade secret programs are built on a principle of deliberate restraint: share only what is necessary, and no more.

Contracts with AI vendors should include confidentiality obligations, data-use restrictions, model training prohibitions, and audit rights. Where feasible, manufacturers should host models

internally or utilize private cloud instances. These safeguards reduce leakage risk and strengthen potential trade secret misappropriation claims under the Defend Trade Secrets Act by demonstrating reasonable measures to maintain secrecy.

3. Data Ownership and Contractual Risk Allocation in Smart Manufacturing

Data generated by smart manufacturing systems — sensor outputs, digital twin telemetry, AI inference logs — represents both a strategic asset and a persistent source of commercial dispute. In multi-party relationships, ambiguity over data rights can quickly escalate: Who owns sensor data from a shared production line? Can one party use another's data to train AI models? What restrictions govern data shared with cloud providers? Without clear contractual allocation, these questions invite costly litigation.

Agreements should address data ownership with specificity: classification of data as background (pre-existing) or foreground (generated during the relationship); allocation of rights to derivative works, including AI models trained on shared data; licensing scope and field-of-use restrictions; flow-down obligations for subcontractors; and indemnification for data-related IP or privacy claims.

Limitation-of-liability clauses should be calibrated to data-driven dispute risks, and dispute resolution provisions should reflect the parties' commercial relationship. Manufacturers should also secure audit rights over data usage and negotiate deletion or anonymization requirements upon contract termination.

4. Patenting AI-Assisted Inventions in Smart Manufacturing

The U.S. Patent and Trademark Office's November 2025 Revised Inventorship Guidance for AI-Assisted Inventions resolved considerable uncertainty for patent practitioners and innovators alike. Implementing the Trump Administration's Executive Order on American AI leadership, the USPTO reaffirmed the longstanding statutory requirement: only natural persons may be named as inventors. AI systems are instruments of invention, not inventors. The determinative inquiry remains conception: a natural person must form "a definite and permanent idea of the complete and operative invention."

For manufacturers deploying AI in process innovation, this guidance has immediate operational implications. Patent claims arising from AI-assisted work must be supported by clear evidence of human intellectual contribution, whether through prompt engineering, data curation, model validation, or the integration of AI outputs into a workable technical solution. Failure to document the human contribution invites rejection or exposes issued patents to invalidity challenges.

Manufacturers should implement protocols for contemporaneous documentation of AI-assisted invention: iteration logs, decision matrices reflecting human oversight, and records of modifications to AI outputs. This documentation supports patent prosecution and provides critical

evidence in enforcement actions. Additionally, practitioners should monitor foreign patent regimes, several of which are developing divergent AI-inventorship standards that may affect priority claims and filing strategy.

Conclusion: IP as Strategic Infrastructure

As AI-driven manufacturing technologies mature, intellectual property must be treated not as a compliance exercise but as core strategic infrastructure. Manufacturers that implement clear pipelines for tracking innovations, deploy layered protection strategies tailored to their business objectives, fortify trade secret programs, and negotiate precise IP ownership terms will be positioned to capture the value of their innovations while minimizing litigation exposure and regulatory risk.

Foley's Manufacturing, Technology, and Intellectual Property attorneys regularly advise manufacturers on IP strategy, contract structuring, and dispute resolution in AI-enabled operations. For more information, please contact the authors or your Foley relationship partner.

Author(s)

Vanessa L. Miller
vmiller@foley.com
Detroit
313.234.7130

Robert C. Okonowski
rokonowski@foley.com
Detroit
313.234.7191

Raymond J. McVeigh
rmcveigh@foley.com
Detroit
313.234.2734