

Adoption of Artificial Intelligence in Manufacturing Accelerating



FOLEY & LARDNER LLP

Article By

[John D. Lanza](#)

[Foley & Lardner LLP](#)

[Manufacturing Industry Advisor](#)

- [Communications, Media & Internet](#)
- [All Federal](#)

Wednesday, March 13, 2019

The rapid adoption of Industry 4.0 technologies leaves manufacturers with a choice: accelerate with the market or be left behind. According to a 2019 Global Market Insights, Inc. report, the market for artificial intelligence in manufacturing will grow to \$16 billion by 2025. Factors driving the adoption of Industry 4.0, the general name given to the deployment of cyber-physical systems, Internet-of-Things technologies and cognitive computing in the manufacturing environment, include:

- Reducing the cost of operations
- Enhancing operational efficiency
- Aligning operations with customer requirements
- Analyzing processes in real-time
- Scaling operations without intensive capital cost

Achieving these goals is supported by two main principles: interconnection and information transparency. Interconnection refers to the ability of machines, devices, sensors and people to connect and communicate with each other. Information transparency provides operators with large amounts of useful information needed to make appropriate decisions. The interconnected nature of machines and systems in an Industry 4.0 environment combined with information transparency allows manufacturers greater insight into the current operating conditions and operational efficiency of the factory. Comparison of operating conditions and health information between machines facilitates just-in-time

maintenance. Leveraging that information using big data analytics (perhaps using cloud-based services) will allow manufacturers to gain many advantages, including near-zero downtime. However, the promise of interconnection comes with its own challenges: (1) data security issues are exacerbated by the need to open previously non-existent lines of communication with vendors, partners and customers; and (2) manufacturers may find it harder to maintain the confidentiality of their processes.

Data security is a complicated area. All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have legislation requiring that entities notify individuals when security breaches of personally identifiable information occur. While most people will think of financial information when they think of “personally identifiable information,” the reality is that personally identifiable information is broader and may implicate the kinds of information maintained by manufacturers that can be inadvertently disclosed or intentionally targeted by bad actors. Manufacturers need to be aware whether their systems include “personally identifiable information” and where vulnerabilities may exist in their systems. For example, Internet-of-Things-enabled devices can allow outside attackers to compromise equipment. More prosaically, as highlighted in a recent data threat report by Honeywell, USB devices are a major threat to manufacturing and industrial facilities. In addition to being aware of the systems that have been deployed in the factory, manufacturers should also strongly consider having a response plan in place should a breach occur.

Information about machines and sensors, i.e., process line information, may be shared with vendors who process the information on the manufacturer’s behalf to surface actionable insights, partners who will use the information to optimize supply chain operations, or customers so that the manufacturer can provide personalized mass-market products, which can create risk for companies around protecting their trade secrets. When drafting and executing vendor, partnership and customer agreements, manufacturers need to consider carefully what information is being shared, how that information is being shared, and what happens to the information after the agreement expires or terminates. Thought also needs to be given to whether it is likely that either party will generate intellectual property apart from the data during the course of the relationship and how ownership of any such intellectual property will be determined.

Manufacturers who adopt principles of Industry 4.0 while keeping their eye on the legal issues presented by those principles will be well-positioned to succeed in the Fourth Industrial Revolution.

© 2019 Foley & Lardner LLP

Source URL: <https://www.natlawreview.com/article/adoption-artificial-intelligence-manufacturing-accelerating>