How to Protect Your Company’s Trade Secrets in the Industrial IoT

By Stephen Reynolds, Partner, Ice Miller LLP

While the rapid emergence of the Internet of Things has been well publicized in the area of consumer products, less attention has been given to one of the Internet of Things’ largest areas of growth—devices designed for businesses. These interconnected business devices, sometimes referred to as the “Industrial Internet of Things,” are revolutionizing the way businesses collect and use data. With all the promise of these new technologies come new risks to businesses—particularly in the area of protecting valuable trade secrets.

This article provides an overview of the Industrial Internet of Things, demonstrates how trade secrets can be put at risk by the Internet of Things, and provides practical guidance on how a business can protect trade secrets in this new industrial age of the Internet of Things.

What Is the Industrial Internet of Things?

Although consumer-facing devices—like wearable computers, personal health trackers, connected home security systems—have received the bulk of the Internet of Things hype, industry experts contend that “the vast majority of new uses of devices are by enterprises, not consumers.”[1] Indeed, in its 55-page Staff Report on the Internet of Things, the Federal Trade Commission devoted only a couple of sentences to the industrial use of the Internet of Things, recognizing that the Internet of Things “can include the type of Radio Frequency Identification (‘RFID’) tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels, and Internet-connected jet engines and drills on oil rigs.”[2]

As applied to business-to-business devices, the Internet of Things has been called “the next Industrial Revolution.”[3] The goal is for the interconnectivity of smart devices to enable businesses to improve efficiency and increase profitability. The future of the Industrial Internet of Things is bright. According to a recent report, companies including General Electric, Ford Motor Company, and Michelin are already finding opportunities through the Industrial Internet of Things.[4] For example, one leading software manufacturer offers an Industrial Internet of Things platform that provides industrial analytics to help businesses avoid equipment downtime, optimize profits, and manage risks.[5] Similarly, connected construction equipment is being used to reduce fleet operating costs and even reduce insurance premiums due to theft prevention.[6]

How Does the Internet of Things Put Trade Secrets At Risk?

In a recent study at the University of California, Irvine, researchers were able to reverse engineer a 3D printed object just by listening to the sounds emitted by the 3D printer.[7] While this does not necessarily implicate the Internet of Things, this anecdote illustrates that with new technologies come new ways to steal intellectual property. Among intellectual property theft, trade secret theft is a large concern. One study estimates that economic loss attributable to trade secret theft is between 1% to 3% of U.S. Gross Domestic Product, representing hundreds of billions of dollars.[8] Moreover, several of the
technologies most at risk for trade secret theft—information and communications technology, advanced materials and manufacturing, medical devices and pharmaceutical technology, and agricultural technology—are developed by the same companies leading the push into the Industrial Internet of Things. Reports of actual incidents of trade secret theft from U.S. companies have confirmed these fears.\[10\]

Inherent in the Internet of Things is the need to share information across connected devices, and such sharing of data between parties inevitably poses security challenges. For example, to meet certain regulatory requirements, the pharmaceutical, beverage, and construction industries will need to implement innovative methods for electronically transferring information to customers and suppliers, which naturally raises cybersecurity concerns.\[11\] Similarly, data is frequently collected by business vendors to help optimize companies’ manufacturing processes. This acutely puts the data being shared—which may constitute valuable trade secrets—at risk.

Significantly, recent lawsuits involving trade secrets demonstrate the dangers of sharing trade secrets between businesses. For example, in a recent federal court case, an industrial design firm entered into a partnership with a manufacturing company to evaluate a potential business relationship to develop metal cases for electronic tablets, such as iPads.\[12\] The companies did business together for a period of time but eventually the manufacturing company ended the relationship and developed its own metal cases. The industrial design firm sued the manufacturer for trade secret misappropriation, fraud, breach of fiduciary duty, and breach of contract. The district court dismissed all four claims and the Seventh Circuit affirmed, finding that under Illinois law it would only enforce the parties’ non-disclosure agreement if the plaintiff “took reasonable steps to keep its proprietary information confidential,” which it found lacking. Although ultimately unsuccessful, in another federal case, the defendant argued that a plaintiff could not pursue a claim for trade secret misappropriation because the plaintiff did not limit access to the proprietary data—specifically alleging as a basis that the plaintiff gave a third party root access to one of its servers.\[13\]

Another recent federal court case illustrates how the Internet of Things and its constant flow of data can undermine trade secret protection. In Allied Portables, LLC v. Youmans, No. 2:15-CV-294-FTM-38CM, 2015 WL 6813669, at *6 (M.D. Fla. Nov. 6, 2015), the district court found that information allegedly taken by the defendants—pricing information, customer lists, sales routes, and a business plan—constituted a trade secret. However, the court declined to issue a preliminary injunction, finding no irreparable harm because the alleged confidential information was over a year old and the nature of the plaintiff’s business changed over time. With the real-time collection of data utilized by the Internet of Things, it is not difficult to imagine a defendant arguing that the data it collected just months ago is now stale and not entitled to heightened protection as a trade secret.

**How to Protect Trade Secrets Flowing Through the Internet of Things?**

As illustrated by the cases referenced above, relying on contractual agreements between parties may not be enough to protect information a company considers as trade secrets. Rather, as with data security, the best approach is defense in depth, with multiple layers of protections for trade
secrets. Below are some practical steps companies can take to protect trade secrets in the new age of the Internet of Things.

**Contractual Obligations**

Imposing confidentiality obligations in contracts with parties who receive access to trade secrets is a good initial step. These contracts should be carefully drafted with the needs of the business and maintaining a balance between sharing information and the desire to keep the information protected in mind. Special attention should be paid to the applicable state law governing trade secrets and the manner in which information is designated as confidential.

**Data Classification**

Related to and perhaps necessary for imposing contractual obligations on others, companies would be prudent to have a comprehensive data classification system in place. For example, information could be classified as “highly confidential,” “protected,” or “public.” The obligations of third parties handling the information could vary depending on the classification of the data the third party obtains.

**Security Controls**

To obtain legal recognition of a trade secret under either the Uniform Trade Secrets Act[14] (adopted in most states) and the new Federal Defend Trade Secrets Act,[15] the owner must take reasonable steps to keep the information secret. This would include steps designed to prevent both outside threats and threats posed by company insiders. For example, businesses should consider the following:

- implementing “need-to-know,” role-based access controls;
- data classification and data location marking (e.g., “confidentiality” labels);
- employee handbook protections;
- non-disclosure agreements for contractors;
- monitoring and logging access to confidential information;
- proper data disposal;
- exit interviews to verify return/destruction of confidential information handled by employees; and
- legally pursuing parties responsible for misappropriation when trade secret theft occurs.

Although not meant as a comprehensive guide for businesses, the Federal Bureau of Investigation (FBI) has produced a Checklist for Reporting an Economic Espionage of Trade Secrets Offense, which has some specific questions that provide a good starting point for businesses to consider when evaluating security controls.[16] For example, the checklist asks questions about physical security precautions,
document controls, and computer-stored trade secrets, such as the following:

- **Does the company require sign in/out procedures for access to and return of trade secret materials?**
- **Are employees required to wear identification badges?**
- **How many employees have access to the trade secret?**
- **Was access to the trade secret limited to a “need to know” basis?**
- **Has the company established and distributed written confidentiality policies to all employees?**
- **Does the company have a written security policy?**
  - (a) How are employees advised of the security policy?
  - (b) Are employees required to sign a written acknowledgment of the security policy?
  - (c) Identify the person most knowledgeable about matters relating to the security policy, including title and contact information.
- **If the company stores the trade secret on a computer network, is the network protected by a firewall?**
- **Is remote access permitted into the computer network?**
- **Is the trade secret maintained on a separate computer server?**
- **Does the company prohibit employees from bringing outside computer programs or storage media to the premises?**
- **Does the company maintain electronic access records such as computer logs?**

**Conclusion**

The business-to-business application of the Internet of Things presents new and exciting opportunities to improve efficiencies and generate revenue across industries. As the use of these technologies expands, the need to legally protect trade secrets is an important consideration that should be taken into account when contracting with other parties, classifying data, and implementing security controls.

*This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader’s specific circumstances.*


[5] Id. at 12.


[12] nClosures Inc. v. Block & Co., 770 F.3d 598, 602 (7th Cir. 2014)

The Uniform Trade Secrets Act defines a “trade secret” as “information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” See Uniform Trade Secrets Act §1.4 (1985).

Under the Defend Trade Secrets Act, “trade secret” means “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information. See Defend Trade Secrets Act § 2(b)(1) (2016) (amending 18 U.S.C. § 1839(3)).