September 28, 2017

The Industrial Internet of Things (IIoT) and the Law

A Legal Perspective

Summary

The Industrial Internet of Things (IIoT) is an increasingly vital part of utility infrastructure.[1] While the IIoT has received substantial attention within the context of cybersecurity and grid reliability,[2] there has been little work done on the array of legal issues associated with the IIoT, many of which have little or nothing to do with cybersecurity. The interconnected and networked nature of the IIoT presents issues related to intellectual property, liability and risk sharing, and ownership interests. What will be the likely regulatory and legislative responses to an increasingly IIoT-dependent electricity grid? How can interconnected utilities share the costs of a largely digital control system that transcends the traditional generation, transmission and distribution systems?

There has been surprisingly little attention given by the legal community to the issues and implications associated with the IIoT, either generally or within the utility industry.[3] Discussion of the IIoT in the electric industry has been the province of operational and engineering experts. But IIoT operational and engineering challenges will inevitably present novel and difficult legal issues.

Background

Most people are now familiar with the Internet of Things (IoT), the network of physical objects, embedded sensors, connections and computers that permeates much of our everyday life. Encompassing the mundane (smart refrigerators and toasters), the vital (medical devices), the amusing (smart toilets) and the creepy (tracking and shopping monitors), the IoT has become both a buzzword and a way of life. We live among it.

The IoT continues to evolve within a largely consumer-driven digital ecosystem. As a result, IoT operating systems often have a shared heritage with the array of personal computing devices with which we are familiar. IoT devices, and the software that manages and maintains the communication networks between those devices, evolved alongside our phones, tablets and PCs. One can trace the IoT's lineage back to Gates, Jobs and Wozniak, and the IoT is part of the extended family whose patriarchs are Apple, Microsoft and IBM. Your smart fridge may have code deep inside it that traces back to a fabled Palo Alto garage.

The **Industrial** Internet of Things, on the other hand, while similar in name, is different in fundamental ways.[4]

First, to continue the familial taxonomic metaphor, if the IoT is made up of numerous first cousins, all related to your home computer and phone, the IIoT is made up of second and third cousins. The IIoT grew not out of the consumer electronics explosion, but alongside large-scale industrial control hardware. Much of the software behind the IIoT was custom-developed (often decades ago) as an adjunct to big, expensive pieces of industrial hardware: switches, valves, pumps and other heavy machinery. If those pieces of hardware are the bones and joints of industry, the IIoT is the quickly evolving nervous system

knitting them together. But that evolution has proceeded on a separate track from the IoT, and thus has different capabilities, structure and vulnerabilities.

Second, the IoT is focused on individuals; it is consumer-oriented and its end users are people ? families, small businesses and enterprises. The IIoT (as its name suggests) is directed to serve machines and industrial systems.

How important is the IIoT? It is now a fundamental part of the nation's critical infrastructure. It runs our oil fields, our gas pipelines, our water systems, our dams and heavy industry; it underpins the electricity grid, our train systems, our highways and our ports.

Why should lawyers care?

The first reason is the most dramatic. The IIoT is now understood to represent a key piece of critical infrastructure that is significantly vulnerable to cyberattacks.[5] Its vulnerabilities are different from the vulnerabilities of the IoT (in part, because of their different software heritage), and in some cases, more significant. Furthermore, the consequences that may flow from exploitation of those vulnerabilities is greater than are those from the IoT. If the IoT is exploited, cyberactors (state-sponsored, criminal, terrorist or other) are likely able to steal money, degrade data and engage in identify theft. They may even be able to shut off a smart fridge. But a successful IIoT attack can shut off or damage aspects of the day-to-day systems of society that are essential to individual life and well-being. An attack could shut down a hydroelectric plant, destroy a steel furnace or shut down the electric grid. The results have the potential to be catastrophic.

The second reason is less dramatic but perhaps more important, at least for lawyers. The IIoT forces fundamental changes in the organization of large-scale industrial businesses, and requires rethinking (and in some cases, revising) basic legal mechanisms for conducting business. It may change the concept of "ownership" of industrial components, and presents novel issues concerning intellectual property. It forces consideration of how best to contractually allocate risks (of both "ordinary" events and the types of catastrophic cyberattacks noted above) and how to price and obtain insurance. The IIoT requires reexamination of what a business thinks of as its "assets," and is likely to present emerging issues in financing, acquisitions and mergers.

Third, and final, just as the IoT and the Internet (driven largely by personal privacy concerns) have been subject to increasing regulations on the federal and state levels, so too is the IIoT likely to come to the attention of regulators.

IIoT and the law

When the IIoT and the law collide, cybersecurity immediately leads the conversation. Cyber vulnerabilities, of course, need to be acknowledged. Cybersecurity is the leading topic of any roundtable discussion or symposium and most of the articles about IIoT in the legal press. But our objective is to go beyond this discussion, into the legal waters that have yet to be charted.

A variety of legal disciplines have yet to be considered in depth in their relation to the IIoT, such as intellectual property, insurance and indemnification, commercial contracting, and antitrust/regulatory compliance. All these practices will, however, interplay with the IIoT in the future.

Take, for example, a power-generating station fed by multiple interstate natural gas pipelines, with a valve connecting the system and controlling the flow of gas into the generating station. The valve controls the flow of gas and may be considered to be part of the gas pipeline's system, but it is operated by the power-generating company. Previously, a comparable valve would have been a simple part of the system, and after purchasing the valve, the power-generating company would have manually controlled the flow of gas through the valve. Once in operation, the legal concerns would have been relatively minimal.

But today, this valve is connected and smart. This valve receives information from the power-generating company that controls and determines the gas mixture received, produced and transmitted to various interstate pipelines. The pipeline is "talking" to the valve, which is "talking" to the power-generating company, and vice versa. Initially, the immediate legal concern for this valve is cybersecurity. If it is controlled by internal software and operated by data rather than people, it is subject to technical failure and potential attack, with catastrophic consequences. However, there exist legal implications beyond this initial scare concern.

Initial contracts must establish the operational need for both the hardware and software of the valve, and these initial decisions can affect ongoing liability and tax concerns. This is not just a traditional buy/sell agreement between two parties for the purchase of a valve. There are now additional parties involved that provide the data to make this valve operate and maintain the software that communicates with the entire system. Did the company purchase this valve from a hardware manufacturer together with its software from a data company, or are they purchased separately? Is the data actually purchased, or is it leased? Who provides the maintenance for this data, and what if the data provider goes out of business? The power-generating company is a utility company, not Microsoft, and does not have the capacity to maintain software products with its own resources.

The data itself presents additional contractual issues. How does a third party monitor and maintain the rich data provided by the valve's operation? There is intellectual property embodied in this data with associated ownership, security and liability issues. Moreover, what if this third party goes bankrupt or dissolves? How will any initial contract address this possible turn of events?

The information generated from the operation of this single valve, such as weather reports, utilization records and maintenance needs, could be used for program efficiency or industry predictions. The humans who used to keep track of this information were subject to various regulations, such as those that bar manipulative trading techniques. Can smart machines be appropriately regulated? Is there a way to properly use and profit from this information?

Furthermore, all the separate pieces of the valve need to be insured: the hardware, the software, and the local and remote interconnected pieces. The effect that this valve has may cross state lines or be part of a variety of disasters. Are all these pieces going to be insured together or separately? How do the many interconnected companies in this scenario apportion the cost of insurance? How is risk mitigated, and how is it calculated on such a wide platform?

Ultimately, there is no denying that cybersecurity concerns are at the forefront of the IIoT discussion. However, failure to focus on this legal structure in the developing IIoT as it relates to the energy industry may in fact both deny opportunities for revenue and generate more risk than ever anticipated. For the energy industry, the need for energy and general corporate lawyers has morphed into a need for attorneys well-versed in the areas of software/hardware, intellectual property, tax, and insurance, among others.

---

[1] See "How the Industrial Internet of Things Is Changing the Electrical Industry,"; "How Utilities Can Prepare for the Industrial Internet of Things," and "The Internet of Things Is a Game-Changer for the Energy Industry." Of course, IIoT stretches across all industry, not only utilities. For instance, Massachusetts is considering adopting IIoT capabilities to its aging public transportation infrastructure, including the famous "T." This memorandum, however, focuses primarily on IIoT in the utility space.

[2] See North American Electric Reliability Corp., Critical Infrastructure Protection Standards.

[3] As of this writing, there is no reported case in Lexis in which a court uses the phrase "Industrial Internet of Things."

[4] The IIoT is well-defined as "a subset of the broader IoT, where...connections exist mainly to produce physical goods for the marketplace as well as to maintain the physical assets of production." LNS Research, "What Is the Industrial Internet of Things (IIoT) Platform?" (last visited June 20, 2017).

[5] For example, in December 2015, Russian hackers were able to use malware-laden phishing emails to gain control of Ukraine's electric grid caused blackouts across the country. *See* Tobby Simon, "Critical Infrastructure and the Internet of Things" (Jan. 2017).

Authors

David T. Doot

Of Counsel

Hartford, CT | (860) 275-0102

dtdoot@daypitney.com