DAY PITNEY LLP

NGA
NATIONAL GOVERNORS ASSOCIATION

Summary

Forum: The Industrial Internet of Things: A Legal View or "It's Not Just Cybersecurity"

Day Pitney LLP and the National Governors Association co-hosted a forum entitled "The Industrial Internet of Things and the Law: Not Just Cybersecurity." The Industrial Internet of Things (IIoT) is an increasingly vital part of our national infrastructure, and represents a likely path for dramatic change in our economy. While the IIoT has received substantial attention within the context of supply chain operations and cybersecurity, there are many legal issues associated with the IIoT that are tangential to cybersecurity that should be identified and worked through when IIoT is added to or used in our nation's infrastructure. By way of example, the interconnected and networked nature of the IIoT presents challenges related to intellectual property, liability and risk sharing, and ownership interests. Regulators and legislators have been increasingly focusing on IIoT and their actions in response must be taken into consideration.

The Forum was held to bring together lawyers, operators, regulators, and academics to identify legal issues presented by the IIoT. There were more than 40 participants. The keynote address was given by Michael Janke, a former Navy SEAL and cyber specialist. Janke co-founded Data Tribe, a commercial technology startup studio and venture capital firm focused on cybersecurity, big data and analytics. He has spoken around the world on privacy, cybersecurity and encryption, and recently received the "Visionary of the Year" award from the Center for Technology & Democracy. Janke's keynote focused on the growth of IIoT, its increasing relevance in a modern economy, the risks associated with its rapid adoption, and how the IIoT is related to, but distinct from, the Internet of Things (IoT).

Following the keynote, Day Pitney attorney Steven Cash spoke about objectives and terms of reference in preparation for the breakout roundtables, which included discussions on "Law, Policy & the IIoT" and "Cybersecurity & the IIoT." The breakout sessions were moderated by Day Pitney attorneys, but adopted a free flowing seminar/participant approach intended to facilitate open and candid discussion. Each of the two breakouts was charged with identifying specific legal issues related to the IIoT.

The Forum then reconvened in a "plenary" session, with a designated leader from each breakout group giving a short summary of their group's findings.

Outcomes

The Forum, in both breakout and plenary, generally concurred on a working definition of the IIoT: the system of networked devices (often associated with "hardware," such as switches, valves and other mechanics) that share data across the network to facilitate more efficient industrial processes. The IIoT covers functions all through the industrial supply chain, from raw material sourcing, through processing and/or manufacturing, and ultimate distribution to consumers. These functions are multilayered, and often "looped," in that the IIoT often facilitates systems involving multiple steps of processing and manufacturing. In fact, some participants noted that the IIoT's value lies in facilitating more efficient and complex networks of economic activity.

Building on Janke's keynote, the group also noted similarities to, and differences from, the similarly-named "Internet of Things," which the group defined as a wide range of consumer-facing connected devices. One phrase capturing this distinction is that the "IoT creates the 'Smart Home;' the IIoT creates the 'Smart Economy.'" While IIoT and IoT both use the internet, digital technology, and are data-reliant and data-intensive, they differ in scale, in scope, and in both the size of risk and opportunity. Further, the IIoT's risks and benefits tend to be spread both vertically and horizontally among institutions, while the IoT's risks and benefits are more limited to consumers and their data.

With general agreement on definitions, there were many observations of interest articulated by the group.

While attendees agreed that cybersecurity issues were only a part of the IIoT landscape and the legal issues which populate that landscape, it was clear in discussions that attention on IIoT often focuses initially or evolves into discussions of cybersecurity. There is little question that cybersecurity is the highest profile and most immediate challenge facing those who use IIoT, and the one that many existing systems and processes have already encountered. This, in turn, is heightened by the dramatic and existentially-threatening dimensions of the IIoT. Attention is naturally drawn to those areas issues that require immediate attention, such as cybersecurity, because of the existing reference framework and the newfound scale of IIoT cybersecurity threats.

Relatedly, both breakout groups expressed a need for STEM education and noted the existing lack of knowledge surrounding the IIoT. Lawyers, policy makers and executives must first work towards a common baseline of IIoT knowledge. Only then can parties assess risk and anticipate needs. Institutional knowledge cannot be siloed inside IT departments, and must be shared broadly.

In the plenary session, the group discussed the permeable membrane that both divides and connects the IIoT and the IoT. As the IIoT increases connectivity within supply chains, external points of connection with the IoT grow. Consumer-facing connected devices provide yet another point of access and communication with what used to be hidden and removed from daily life. These access points, which could be vulnerabilities, create an evolving standard of care. Internal decision makers and external policymakers must anticipate how the rapid adoption of the IIoT, and the increased communication with the IoT, affects that standard of care.

The breakout group that focused on law and policy led a discussion around the limitations of metaphors and existing legal paradigms. IIoT law may be the modern-day railroad law – requiring a new, multi-disciplinary approach – but can lawyers apply their existing disciplines to

new challenges presented by IIoT? On the other hand, perhaps none of this is new and lawyers and policymakers already have the tools to address these issues. Focusing on metaphors and seeking analogous bodies of law may cause one to be blind to the unique issues faced with the growth of IIoT. The IIoT diminishes the touchstone of physicality. Issues faced with IIoT are fundamentally new, and while existing bodies of law may inform IIoT law, lawyers expand beyond the bounds of traditional thinking to ensure thoughtful and comprehensive anticipation of and response to the challenges presented by IIoT.

Thus, existing paradigms provide imperfect templates. IIoT is rich with data, and intellectual property law may be ill-equipped to provide a framework sufficient to protect and capitalize on new types of data. Interconnected liability and risk increases with digitized supply chains and systems, and lawyers must consider how and when the existing bodies of tort and contract law must change to accommodate this new level of connectivity. The concept of privity of contract must be reworked in the context of IIoT systems, and new issues in bankruptcy and antirust will arise.

Both groups highlighted the role of the marketplace and explored how and whether regulatory bodies should step in to address potential market failures. In dealing with IIoT, where data and decisions instantly cross jurisdictions that will affect physical systems, regulators must first establish clear jurisdictional lines. With a diverse component supply chain, can the market and owners/operators address cyber risks, or should government play a role in setting minimum security standards (such as for component parts sourced from different countries)?

Next Steps: Since holding the Forum in Boston, we have had extensive informal discussion with participants. The feedback was positive, and we are planning a follow on event, perhaps late this Spring. We have also set up a LinkedIn private group , with membership currently involving only Forum participants (but intended to expand), in which documents and ideas can be shared.

---

[1] *Industrial Internet of Things (IIoT) and the Law*

* * *