FEBRUARY 2019

DEVOTED TO
LEADERS IN THE
INTELLECTUAL
PROPERTY AND
ENTERTAINMENT
COMMUNITY

VOLUME 39 • NUMBER 2

# THE Licensing Journal

*Edited by Gregory J. Battersby and Charles W. Grimes*

Wolters Kluwer

# *The Hype behind the Industrial Internet of Things*

## Jeremy Dunbar, Jonathon K. Hance, Joel Bagnal, Ashok Choudhury, Mark Soloman, and Mark Thirman

*Bracewell Partner Jonathon Hance is a litigator and an intellectual property lawyer who works to protect and monetize his clients' innovations and protect his clients' brands across a variety of sectors, including the energy, real estate, and technology industries. He also advises healthcare institutions regarding corporate governance issues and patient data privacy and protection under the Health Insurance Portability and Accountability Act (HIPAA).*

*Bracewell Associate Jeremy Dunbar handles complex commercial litigation related to energy, contract, and real estate matters. Jeremy draws from his experience as a former law clerk to the Honorable David Hittner of the United States District Court for the Southern District of Texas, where he assisted in thirty trials, including motions in limine, jury selections, evidentiary objections, jury charge conferences, and jury debriefings.*

*Joel Bagnal is the President and Chief Operations Officer of Vercilave, Inc., a cybersecurity company focused on offering customers a highly differentiated national security grade solution to prevent cyber threats from accessing networks. Joel is an experienced global security and risk management executive who develops and launches strategies that create enduring, customized security solutions across entire organizations. Joel implements customized risk management programs designed with effectiveness and growth as sustainable outcomes. A proven innovator, powerful influencer, and entrepreneurial leader, Joel rapidly builds high performing teams and develops leading edge solutions that achieve an organization's growth goals while also reducing enterprise risk and improving efficiency.*

*Dr. Ashok Choudhury is the Manager of Physical Sciences licensing at Vanderbilt University. He is the recipient of numerous technology transfer awards including a R&D 100 Award. Ashok is a metallurgist by training and stays involved in the technical community through teaching and advising activities. Ashok is the co-author of two books on failure analysis. He is a member of AUTM, LES, ASM International, Sigma Xi and Tau Beta Pi and holds CLP credentials.*

*Mark Solomon, Hamilton Brook Smith Reynolds, has dedicated his 20-year legal career to guiding universities, research institutions and companies of all sizes through the development, management, protection, and enforcement of intellectual property rights. He provides high value IP services for clients who value IP by drafting and prosecuting patent applications from licensing and strategic business and legal perspectives, as applicable. He also assists clients with intellectual property matters relating to licensing, patent litigation, written and oral opinions, trademark prosecution and oppositions, copyright law, trade secret law, domain name disputes, and sale of intellectual property assets, and provides associated strategic counseling.*

*Mark Thirman has over 30 years of experience in executive, business development, and sales roles gathered in a broad range of telephony, infrastructure, and networking companies. Currently, Mark is working on global loT strategy with J. D. Power, a global leader in consumer insights, advisory services, data, and analytics. Mark has also worked with Amazon Web Services (loT), Cloud Technology Partners, and TELUS. Mark currently chairs the Connected Things group at the MIT Enterprise Forum and serves on the board of directors. Mark is a frequent speaker on the topic of loT/Connected Things and often is a guest lecturer at MIT, Tufts, Boston University, and other universities.*

## Introduction

The term "Internet of Things" (IoT) was coined at the Massachusetts Institute of Technology Media Lab in 1966 by researcher Kevin Ashton as a last minute PowerPoint addition:

> I coined the term 'the Internet of Things' when I had to make a PowerPoint presentation in the

> 1990s to convince the senior management of the company I was working for, which was Proctor & Gamble, that we should put . . . a tiny microchip in everything Proctor & Gamble made.[1]

The phrase has since become confusing for many, but the best description of IoT is as a system of sensors, incorporated into consumer and industrial devices, which in turn are connected to a network (either the Internet or, in many cases, a private network[2]) to monitor, manage, locate, and collect real-time data. Device-generated data are important in many key industries, including medicine, automotive/transportation, HVAC/connected buildings, connected agriculture, and natural resources. Also, while consumer-facing IoT devices are just beginning to take a foothold, enterprise-focused IoT developments involving machine monitoring and control (previously referred to as "M2M" or "Machine-to-Machine," or in some cases by the acronym SCADA—"Supervisory Control and Data Acquisition") have quietly existed for over a decade.

Today, tens of millions of devices are part of a networked IoT system of one kind or another, with massive growth predicted for numbers of deployed connected devices and the data they emit.[3] Cellular phones, for example, are expected to have 3.5 billion IoT connections by 2023.[4] And at a recent Amazon Web Services conference, one presenter from the Formula 1 race car organization described their vehicles as containing "120 sensors on each car, generating 1.1 million telemetry data points per second."

Although sensors on race cars are exciting, perhaps IoT's most promising application is to industry—the so-called "Industrial Internet of Things" (IIoT).[5] IIoT generally refers to "the proliferation of industrial systems, machines, and devices capable of interacting with the physical environment, people, and other devices."[6] There is much hype behind IIoT technology. Popularly referred to as the "fourth industrial revolution,"[7] IIoT has been described as having the potential to "revolutionize the industrial sector in the United States and around the world."[8]

IIoT technology is already being adopted in several industrial markets.[9] For example, companies can remotely monitor industrial hardware and, using cloud-based analytics, predict the necessity for maintenance before it arises.[10] IIoT also has the potential to dramatically change industrial logistics; retail giant Amazon has begun to experiment with drone deliveries using IIoT technology.[11] Power management could also be improved when "specific sensors can detect environment and trigger to turn on/off control of lights, air-conditioners, humidity controls, [and] liquid control . . . ."[12]

For all of the hype, however, there are multiple unique challenges facing IIoT that need to be resolved before it can be fully and safely utilized. Chief among them are challenges involving intellectual property rights and data security. IIoT innovators will undoubtedly seek patent protection for their inventions. Difficulties in doing so may discourage further innovation. Likewise, as IIoT innovation evolves, device security and network vulnerability is inevitable, and the consequences of a potential data breach become catastrophic. This article discusses these challenges and explains why now is an opportune time to address them.

## Intellectual Property Challenges

Largely because of its inherent interconnectedness, IIoT presents multiple discrete and unique difficulties in obtaining and enforcing patent protection.

First, it may prove difficult to demonstrate patent eligibility for IIoT products. Furthermore, there is a jurisdictional aspect to this issue since the law regarding patent eligibility varies between the industrialized nations. In the United States, Section 101 of the Patent Act sets forth the requirements for patent protection eligibility: "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore . . . ."[13] Although software is generally patentable, abstract ideas are not.[14] Thus, "simply using software to implement abstract ideas is not patentable."[15] To determine eligibility, courts ask (1) whether the invention is "directed to an abstract idea"; and, if it is, (2) whether the invention "adds significantly more" to that idea.[16]

Courts have struggled to apply this standard to inventions involving computer technology,[17] and its application to IIoT will likely prove even more challenging.[18] In a physical sense, IIoT is not new. The "Things" in IIoT generally include hardware that have existed for years: a device being monitored, communications modules, connectivity equipment, and sensor technology. In that sense, one may find abstract the idea of, for example, connecting these devices in a way that allows for the collection and analysis of data to predict when manufacturing machinery will need maintenance. But is this application an abstract, patent-ineligible idea merely because it uses preexisting hardware? The answer will likely turn on step two, above. Thus, in drafting and submitting patent applications for IIoT technology, applicants would be wise to detail and exemplify how the IIoT invention adds significantly more to the preexisting technology it seeks to exploit.[19]

Second, the collaborative nature of IIoT will likely lead to difficulties in patent enforcement because of joint infringement. Joint infringement occurs when the infringing performance of a patented method is split between multiple parties.[20] Because IIoT technology usually requires the interaction of a diverse spectrum of devices, joint infringement is more likely to occur. Following the above example, an IIoT patent may prescribe a method of combining communications modules, connectivity equipment, sensor technology, and manufacturing machinery in a novel way that allows for prediction and enablement of maintenance that was otherwise unforeseen. An infringing method would likewise call for the interaction of these devices so that no single device independently performs the infringing activity.

Under current precedent, in such cases, a single defendant may be held liable only where the defendant exercises control or direction over the entire process such that every step is attributable to that party.[21] This may be easier to prove in the consumer context, where it is more likely that a service provider is directing or controlling the process,[22] but it is difficult to prove in the industrial context.[23] To avoid this difficulty, patent lawyers have sought to draft patent claims in a way that focuses on one device and thus requires only a single infringer.[24] Nevertheless, because of the propensity for joint infringement of IIoT patents, litigation seems inevitable.

Third, IIoT's inherent need for interoperability among a broad range of devices presents standardization and licensing challenges. More so than most previous technology, IIoT is dependent on the interoperability of many devices, and when a large number of separately manufactured devices must communicate, there develops a need for a standard language.[25] Patenting such standardized language creates a dilemma. On the one hand, patented IIoT standardization technology requires IIoT developers to choose between infringing and paying exorbitant licensing fees.[26] On the other hand, without patented standards, IIoT systems will likely develop independent codes and communications technologies, which will hinder overall compatibility.[27]

This dilemma has been addressed in the smartphone industry through the creation of so-called standard essential patents (SEPs).[28] Holders of SEPs must offer nonexclusive licenses on fair, reasonable, and nondiscriminatory (FRAND) terms.[29] The SEP model, however, may not prove as useful in the IIoT arena. IIoT requires interoperability among many more separately manufactured, unrelated devices than do smartphones.[30] Thus, the creation of standardization technology will be more difficult to coordinate.[31] For the same reasons, determining what standards are actually essential will be challenging.[32] Additionally, as was the case with smartphones, parties do not always agree on what constitutes a FRAND licensing fee.[33] Again, litigation seems inevitable.

Finally, because IIoT's success depends in significant part on new, innovative, and robust software, patent protection is not the only avenue for protecting IIoT innovation. Trade secret and copyright laws also play a part. Where disclosure of the software can be avoided and secrecy maintained (such as in an internal company implementation of an IIoT system), IIoT innovation could be protected by keeping the enabling software a well-guarded trade secret and by registering small portions of the code that do not reveal the trade secrets with the US Copyright Office under a "special relief request" from registration.

## Device Security and Network Vulnerability Challenges

IIoT also presents some of today's greatest device security and network vulnerability issues, many of which stem from the same qualities that make IIoT so promising.[34]

Since the risk of security breaches scales with both the number of connected devices and the complexity of the networks, it is obvious that the likelihood of IIoT breaches will only increase with time.[35] It has been hyped that IIoT will "grow close to 100 billion connected devices in the next five years and will likely outpace the consumer IoT due to the large-scale nature of the industrial products sector."[36] Although technological development and growth are good things, that amount of connected devices creates just as many vulnerable access points.[37]

Additionally, IIoT's interconnectedness broadens the potential scope of a security breach.[38] Because IIoT's utility is tied to its ability to connect many different devices, IIoT developers are incentivized to make that connectivity as seamless as possible. Again, this is presumably a good thing with regards to industrial development of IIoT technology. A vast network of seamlessly connected devices also, however, makes it easier for malware to spread to areas of a network that would otherwise be inaccessible.[39] Thus, the scope of a potential IIoT attack is broadened.

Finally, the context in which IIoT technology is applied increases the severity of a potential security attack. IIoT technology has been implemented in some of our nation's most foundational infrastructure systems, including our electricity, chemical, and manufacturing systems.[40] Successful attacks on IIoT networks within these sectors could have very dire consequences. Indeed, IIoT network breaches have already caused extensive damage internationally. In 2015, a German steel mill's network was breached, and the mill's blast furnace was prevented from shutting down, causing substantial damage.[41] In 2016, hackers gained remote access to the Ukranian power grid and disconnected power to approximately 225,000 people.[42]

To be sure, much effort is being made to address these concerns. Over $4.2 million were invested in device and platform security in the United States in 2017.[43] Most of this money was spent on software development; of the approximately 1500 companies in the United States focused on security, 95 percent of them are focused on software.[44] Software, such as firewall technology, intrusion detection, security information management, and security analytics, generally provides a response-based framework that identifies threats and provides a remedy.[45]

Importantly, however, while responsive protocols are valuable, experts have recently indicated that an often overlooked piece of the puzzle is the development of preventative hardware systems.[46] This is especially important in the IIoT context, where often times, much of the equipment being connected and monitored consists of legacy systems that have no hardware security apparatus.[47] Overall, cybersecurity should be a top priority for those industries adopting IIoT technology. And to ensure IIoT networks are as secure as possible, developers must take a holistic approach, building hardware-rooted security systems that use software encryption components to both prevent and respond to cybersecurity threats.

## The Hype Cycle

The challenges facing IIoT should not be discouraging. Developmentally, IIoT is in somewhat of a sweet spot with regard to addressing these issues.

Market research firm Gartner, Inc.'s Hype Cycle for Emerging Technologies tracks and predicts the development and ultimate success of emerging technologies.[48] The Hype Cycle consists of five chronological phases through which most successful developing technologies progress.[49] Essentially, the Hype Cycle begins with a technological trigger, after which expectations for the new technology tend to grow until they become unrealistic and then peak.[50] Expectations for the technology thereafter begin to wane, but as the hype catches up to reality, interest returns, and, if the technology ultimately proves successful, mainstream adoption sets in.[51]

The 2018 Hype Cycle places IoT just over the peak of inflated expectations, predicting that it will reach mainstream adoption in 5 to 10 years.[52] Most agree that the IIoT segment is developing at a faster pace compared to other IoT segments, so IIoT may reach mainstream commercial adoption even sooner.[53] Regardless, IIoT is currently near the height of its hype, which means expectations for IIoT may soon decline.[54] But therein lies the sweet spot. As the hype over IIoT wanes and reality sets in, an opportunity-window to address intellectual property and security concerns emerges so that when the hype catches back up to reality, IIoT is better poised for ready adoption.[55]

From an intellectual property standpoint, this period gives businesses an opportunity to develop strategic patenting plans so as to ensure eligibility and enforcement. It also provides time for case law to develop. Additionally, standardization and licensing protocols may be formulated so that compatibility issues do not hinder eventual mainstream adoption. With regard to device security and network vulnerabilities, this period gives developers a chance to create cohesive software and hardware systems that will bolster the vulnerabilities inherent in IIoT technology. It also gives regulatory bodies time to formulate regulations that address safety and privacy concerns.

IIoT technology has the promise of being more than hype. But as it develops and moves toward large-scale adoption, intellectual property and security difficulties will continue to emerge. For IIoT to truly reach its full potential, these issues need to be addressed. Luckily, now is the best time to do so.

[1] Allison DeNisco Rayome, *How the Internet of Things was Invented* (July 27, 2018), *https://www.techrepublic.com/article/how-the-term-internet-of-things-was-invented/*.

[2] Terminology is important: most enterprise-class IoT deployments are not on the Internet, despite the term IoT. It is fair to say that all internet connected devices are not IoT and all IoT devices are not always internet connected. Security plays an important role in choosing networks for devices to connect with—and many such devices are hidden away on private networks and may only be connected within the four walls of a factory on a hardwired connection.

[3] The global IoT market is forecasted to grow to $1,567 billion by 2025. *State of the IoT 2018: Number of IoT Devices at 7B – Market Accelerating*, IoT Analytics (Aug. 8, 2018), *https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/*.

[4] Chris Kelly, *Ericsson: 3.5 Billion Global IoT Connections by 2023*, Total Telecom (June 12, 2018), *https://www.totaltele.com/500283/Ericsson-35-billion-global-IoT-connections-by-2023*.

[5] Ashok Choudhury, Jonathon Hance, Mark Thirman, Mark Solomon & Joel Bagnal, Panel Discussion, IIoT: Enabling a Surge in Industrial Productivity (Oct. 15, 2018).

[6] Mauricio Paez & Kerianne Tobitsch, *The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues*, 62 N.Y.L. Sch. Rev. 217, 218 (2018).

[7] Raymond Millien & Christopher George, *Intellectual Property Lawyering in the Fourth Industrial Revolution (The Internet of Things* 1 (Oct. 2016), *https://www.researchgate.net/publication/313504500_Intellectual_Property_Lawyering_in_the_Fourth_Industrial_Revolution_the_IoT*.

[8] *Id.*

[9] Paez & Tobitsch, *supra* note 6, at 219; Robin Kester, *Demystifying the Internet of Things: Industry Impact, Standardization Problems, and Legal Considerations*, 8 Elon L. Rev. 205, 207–14 (2016).

[10] *Applications of the Industrial Internet of Things (IIoT)* (June 23, 2018), *https://www.rfpage.com/applications-of-industrial-internet-of-things/*.

[11] Ryan Mac, *Amazon Proposes Drone Highway as it Readies for Flying Package Delivery* (July 28, 2015), *https://www.forbes.com/sites/ryanmac/2015/07/28/amazon-proposes-drone-highway-as-it-readies-for-flying-package-delivery/#6d7e889a2fe8*.

[12] *Applications of the Industrial Internet of Things*, *supra* note 8.

[13] 35 U.S.C. § 101.

[14] W. Keith Robinson, *Patent Law Challenges for the Internet of Things*, 15 Wake Forest J. Bus. & Intell. Prop. L. 655, 666 (2015).

[15] *Id.*

[16] Alice Corp. Pty. Ltd. v. CLS Bank Intern., 134 S. Ct. 2347, 2355 (2014).

[17] Robinson, *supra* note 14, at 666.

[18] *See id.*

[19] Solomon, *supra* note 5.

[20] Robinson, *supra* note 14, at 668.

[21] Travel Sentry, Inc. v. Tropp, 877 F.3d 1370, 1378 (Fed. Cir. 2017).

[22] James Stein et al., *The Internet of Things: Divided Infringement*, Prosecution First Blog (Nov. 10, 2016), *https://www.finnegan.com/en/insights/blogs/prosecution-first/the-internet-of-things-divided-infringement.html*.

[23] James Stein & Kenie Ho, *3 Challenges for Internet-of-Things Patents*, Law 360 (June 10, 2016), *https://www.law360.com/articles/801969/3-challenges-for-internet-of-things-patents*.

[24] *Id.*; BMC Res., Inc. v. Paymentech, LP, 498 F.3d 1373, 1381 (Fed. Cir. 2007), *overruled by* Akamai Techs., Inc. v. Limelight Networks, Inc., 92 F.3d 1301 (Fed. Cir. 2012).

[25] Paez & Tobitsch, *supra* note 6, at 232.

[26] *Id.*

[27] *Id.*

[28] *Id.* at 232–33.

[29] *Id.* at 232.

[30] *Id.* at 233.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Bagnal, *supra* note 5.

[35] *Id.*

[36] Paez & Tobitsch, *supra* note 6, at 218. Indeed, it has been predicted that "worldwide technology spending on the internet of things will reach $1.2 trillion in 2022." *IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach $1.2 Trillion in 2022* (June 18, 2018), *https://www.idc.com/getdoc.jsp?containerId=prUS43994118*.

[37] *Id.* at 221.

[38] *Id.*

[39] *Id.*

[40] Bagnal, *supra* note 5.

[41] *Hack Attack Causes 'Massive Damage' at Steel Works*, BBC News (Dec. 22, 2014), *https://www.bbc.com/news/technology-30575104*.

[42] *Ukraine Power Cut 'Was Cyber-Attack'*, BBC News (Jan. 11, 2017), *https://www.bbc.com/news/technology-38573074*.

[43] Bagnal, *supra* note 5.

[44] *Id.*

[45] *Id.*

[46] *Id.*; *see also* Chris Grove, *IIOT and the Cyber Threat: A Perfect Storm of Risk*, *https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_JUN_17/IIOT_and_the_Cyber_Threat_S508C.pdf*.

[47] Bagnal, *supra* note 5.

[48] Gartner Hype Cycle, *https://www.gartner.com/en/research/methodologies/gartner-hype-cycle* (last visited Dec. 1, 2018).

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] Hype Cycle for the Internet of Things, 2018, *https://www.gartner.com/doc/3883066/hype-cycle-internet-things* (last visited Dec. 1, 2018).

[53] PricewaterhouseCoopers, *Industrial Internet of Things* 7 (2016), *https://www.pwc.com/gx/en/technology/pdf/industrial-internet-of-things.pdf*.

[54] *Id.*

[55] Hance, *supra* note 5; *see also* Scott Brinker, *One Thing Everyone Forgets About Gartner's Hype Cycle*, *https://thinkgrowth.org/one-thing-everybody-forgets-about-gartners-hype-cycle-ecfe7e9de8ff* (last visited Dec. 1, 2018).