New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
Litigation
WWW.NYLJ.COM
MONDAY, NOVEMBER 2, 2015

The Next Big Thing: 'Internet of Things' Litigation And Regulatory Risk

BY ROBERT S. BEREZIN

Most lawyers have heard of the "Internet of Things." Business leaders, after all, are busy making the Internet of Things (IoT) the next great wave of innovation to sweep across the global economy. Apple, AT&T, Cisco, General Electric, Google, Honeywell, Intel, Microsoft, Oracle, Panasonic, Samsung, and scores of others have been investing in the IoT for years. With current predictions of a $15 trillion IoT market in fewer than 10 years, it is easy to understand why so many industry giants have made the IoT a strategic priority.

How could the market grow that rapidly? For one thing, the core technology driving the IoT has long existed, and real-world examples of IoT systems abound.

As importantly, there are widespread efforts to create mass adoption. Leading standard-setting organizations are working with representatives across industries to define and standardize technical minutiae, while hundreds of members participate in various IoT industry and advocacy groups.

The challenge for lawyers assessing the litigation and regulatory risks posed by the IoT is significant due to its complexity and seemingly limitless applications across the consumer, commercial, and industrial economies.

Nonetheless, the basic technical and commercial structure of the IoT can be understood by lawyers, and, with that information, the risk assessment

ROBERT S. BEREZIN *is a partner at Weil, Gotshal & Manges, where he is a member of the complex commercial litigation and cybersecurity, data privacy and information management groups.*

challenge becomes manageable. Lawyers also should understand the IoT's structure because, as this article will explain, it inherently results in litigation and regulatory risks impacting a wide range of practice areas and subject matter disciplines.

A good first step to understanding the structure of an IoT system is to start with an "Internet of Things" definition. One such definition reads:

> The Internet of Things (IoT)[ ] is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.[1]

The following examples of IoT systems illustrate what the definition seeks to convey:

The Smart Home: The "smart home" is one in which security, HVAC, and entertainment systems, as well as doors, lights, and large appliances, form a home network. This network is in turn connected to a "cloud" computing platform via the Internet. Such smart home systems are monitored to trigger messages (often in the form of email or text messages to homeowners) and can be remotely controlled and programmed using, for example, smartphone applications. Some are self-learning so that, as the homeowner uses the system more, the system learns and implements preferences automatically. Smart homes incorporating at least some of these features are widely deployed today, and presumably will become even more commonplace in the coming years.

Smart Cars: The latest higher-end cars likewise offer IoT features, such as enabling drivers to use their smartphones or other Internet-enabled devices to remotely open car doors and start engines. In the near future, automobiles on a busy highway are expected to communicate in real time to avoid accidents. Taking a car-centric IoT system to its logical conclusion, Google has developed and is currently testing a self-driving car.

Health: Internet-enabled devices that monitor health-, fitness-, and wellness-related data (such as wearables) can provide early detection of complications, provide real time alerts to physicians or other caregivers, and track compliance with a treatment plan.

Industrial Applications: Within power plants, factories, warehouses, mines, docks, and other industrial settings, virtually everything related to production and the supply chain will be connected to a cloud computer platform, and thereby monitored, controlled, and automated (or semi-automated). These systems are also expected to mine huge data sets generated from machines to learn how to improve efficiency and performance over time. Ideally, industrial IoT systems will enhance quality control, health, and safety while reducing maintenance and other costs. GE has been actively deploying these types of "Industrial Internet" products and services for several years.

These and other IoT systems share a common structure, and are used or serviced by the same types of market participants.

To start, each IoT system must include "Things"—tangible products that exist in the real, non-digital world. Such "Things" consist of consumer or industrial devices or systems equipped with sensors, (possibly) controllers/actuators, and networking capabilities. A single manufacturer might make both the underlying device and the networked sensor attached to that device. A number of manufacturing giants have already committed to supplying IoT-enabled devices they hope will be compatible and interoperate with other key components of an IoT system.

Within the home, factory, or other setting, one will likely find a "hub" or local "gateway" connected via a local network to the "Things" found in and around that setting. The local gateway processes and passes data from the "Things" to the cloud computing platform; it likewise relays commands received from the cloud computing platform to the local "Things." Thus, the local gateway must be compatible and otherwise interoperate with both the networked "Things" and the cloud computing platform. A handful of the largest technology companies in the world have each developed an IoT local gateway. Many of the same companies are also developing or already deploying cloud service platforms, which interoperate with their own local gateway products and services.

The functions performed by the remote cloud computing platform are critically important to any IoT system. The computing platform obtains sensor-generated data from the "Things" via the local gateway and applies rules to determine how that data should be processed. It then stores the data in a potentially massive storage "warehouse" or "lake," communicates any alarms to the IoT system end customer, and sends remote control or other commands via the local gateway to the "Things."

It is believed that key cloud providers will serve, in the consumer context, millions of individual customers and thousands of industrial customers. The "Things" from all of a cloud provider's customers will send potentially massive amounts of data to that provider. The aggregated data obtained from these customers will then form a "Big Data" repository. In this sense, the IoT is a classic application of "Big Data." "Big Data" concerns how vast stores of unrelated and unstructured data can effectively be mined and analyzed to draw unique inferences and potentially make decisions, automatically or otherwise. Through Big Data analytics, industrial systems can be made more efficient. Health outcomes can be improved. Home energy use can be reduced. As a result, cloud providers or other authorized application developers are expected to develop and deploy analytic software, predictive machine-learning algorithms, and other applications capable of mining and analyzing massive repositories of structured and unstructured data.

In sum, the great promise of the IoT—including the trillions of dollars of economic impact it is expected to produce—lies largely in its use within the cloud computing platform of Big Data to improve service, safety, efficiency, and more.

The final primary participant in the IoT ecosystem is, of course, the end customer. The customer will purchase the "Things" likely from various manufacturers, and purchase the local gateway and IoT services either from a systems integrator (or other intermediary) or directly from the gateway and cloud platform provider(s).

Simply put, the fundamental IoT structure is a multi-participant, multi-supplier ecosystem. Intelligent, connected sensors within a home, industrial, or other setting generate data that is sent over the Internet to a service provider. That service provider then processes the data instantly to send messages, trigger remote control of the local devices, or take some other action. It also stores massive amounts of aggregated data from multiple customers for subsequent analyses to improve how local "Things" and systems work.

With that description, the regulatory and litigation risks inherent in this structure come into sharper focus. The following examples illustrate why this is so.

Cybersecurity. It is not news that today's traditional information systems are under attack from both state-sponsored and criminal hackers. The IoT combines traditional information systems, such as computer networks, servers, and data storage, with operational systems and other devices in the real world. This vastly expands the "target vector" for hackers. Worse, IoT system hackers could potentially access and attack home security systems, factories, and power plants connected to the grid. At the same time, the number of devices that must be secured, updated, and patched is staggering. Moreover, as explained above, the IoT involves the collection and storage of massive amounts of data generated by thousands, if not millions, of machines. Therefore, traditional IT systems already under attack will include even more massive repositories of potentially sensitive and valuable data.

Privacy. In the heavily-regulated consumer context, personally identifiable information, health information, payment information, and other sensitive consumer information must be protected from disclosure. Best practices in this space include disclosure and consent policies regarding storage and use, and minimizing the personally identifiable information that is collected and the purposes for which it will be used. Whether a satisfactory privacy regime in the IoT context has been implemented by the various participants identified above will be a key question; if the answer is unsatisfactory, the results will inevitably lead to significant regulatory and litigation risk.

Data Ownership. Given the potential of Big Data, machine-generated data within IoT systems are expected to be the essential ingredient to unlock the multi-trillion dollar potential of the IoT. Indeed, IoT data, amassed from a multitude of customers, is expected to create uniquely powerful data sets from which to derive valuable insights. The expression "information is power" clearly applies in an IoT future, and the potential value of the underlying data will not be lost on the various participants.

For example, within industrial IoT systems, customers are likely to consider data originating from their "Things" to be confidential and proprietary even though it will be stored on a third party provider's remote IoT cloud computing platform. It is therefore likely that certain data and material created from such data will be subject to contractual disclosure and use restrictions in favor of customers. Moreover, customers may seek other protections to limit dependence on specific IoT providers, costs associated with switching providers, and the use of data to benefit competitors. In contrast, every IoT provider has an incentive to create proprietary Big Data repositories and use its customers' data to benefit all of its customers, and to create customer "stickiness" using previously acquired data. IoT providers have a similar incentive to claim trade secret protection over data sets and material originally derived at least in part from their customers' "Things." Meanwhile, as data flows through an IoT system from

the customer's site to the cloud computer platform and back, different participants in the ecosystem will gain or lose control over potentially valuable data. Who owns or has other rights to raw or emergent data as it flows through the system, and what are the legal bases of the various participants' rights? The answers depend on the particular facts and the application of contract, trade secret, and/or intellectual property law. Once again, the inherent data-driven structure of the IoT gives rise to the risk of significant ownership disputes, particularly as the value of IoT systems grow.

Patent Litigation. As with any product or service based on technology, the expectation is that patent litigation will increase with the market value of IoT systems. This is particularly the case because the core technology underlying the Internet of Things is already the subject of numerous patents, and, as technology improves, many more will follow. In light of the IoT structure, litigation will presumably involve, for example, questions of whether the patent covers eligible subject matter and issues of divided infringement due to the many participants in an IoT system.

Competition/Antitrust. Although it is safe to assume that no single market participant currently has market (much less monopoly) power in a relevant IoT market, it would be unwise to neglect competition-related issues. For example, competitors are gathering in standard settings and other contexts to discuss the IoT. Participants need to know today what is and is not appropriate to discuss under the antitrust laws. In perhaps the not-too-distant future, certain participants could establish strategic positions within the IoT market and therefore gain significant market power—for instance, the gateway provider. The gateway will speak all of the potentially non-standard, non-open formats/languages of the "Things" and translate them into a standard format, which may or may not be industry standard.

Moreover, some gateway providers will also offer cloud computing platforms to customers. This will enable them to effectively control entry by application providers and other component suppliers into the IoT ecosystem. It could block competing cloud platform providers or their application providers. Cloud platform service providers will also amass Big Data sets spanning large numbers of customers. These data sets could easily become uniquely valuable and not easily duplicated by competitors. Switching costs for customers could become very significant based on interoperability, control of customer data and emergent data, and the value to the customer of insights derived from multi-customer Big Data sets. Also, given that the IoT system likely involves multiple participants cooperating to provide a service, subsequent acts by, for example, the gateway provider to exclude existing participants could result in antitrust or tortious interference claims.

Product Liability. The most obvious products that could pose product liability risk in an IoT system are the "Things." In IoT systems, products are connected to a network exposed to the Internet and therefore Internet hackers. These systems are expected to be deployed in a host of industrial, commercial, transportation, and urban contexts. In Germany, cybercriminals or vandals have already penetrated IoT systems in the industrial context to create a dangerous furnace explosion. "Smart" automobiles have been hacked to open doors and control engines, with videos on the Internet explaining how. The risk of bodily injury or property damage from an IoT system obviously cannot be ignored. Therefore, questions about which participant (or participants) in the relevant ecosystem are responsible and what legal standards should apply are sure to be important ones to many IoT participants.

Regulation and Regulatory Oversight. The sheer projected scale and economic importance of the IoT and the accompanying privacy and cybersecurity issues have already prompted multiple federal agencies to convene conferences and to issue reports. Congressional hearings have been held. Existing laws and regulations, such as those governing privacy, are likely to be supplemented and expanded. This, in turn, will surely increase the risks.

Although clients committed to the IoT market will eventually confront these and other litigation and regulatory risks, lawyers can help them identify, understand, and manage those risks. For the reasons discussed above, the first step in doing so is to understand the technical and commercial structure of the specific IoT systems the client is implementing now and in the future. This will not be a static exercise. Innovation and the inevitable change that follows, both commercially and technologically, will require lawyers to keep abreast of developments to effectively advise and advocate for clients.

.....●●.....

1. Internet of Things, Wikipedia, https://en.wikipedia.org/wiki/Internet_of_Things (as of Sept. 28, 2015).