The Internet of Things: What Is It and Why Do I Care?

Prepared by:
Matt C. Acosta
Jackson Walker LLP

Published on www.lorman.com - August 2018

The Internet of Things:
What Is It and Why Do I Care?

Written by Matt C. Acosta – 5/22/18

Even if you have never heard of the Internet of Things (IoT)
you're probably connected already.

In 2017, Gartner estimated that over 5.2 billion consumer IoT devices had already been installed and predicted that the number would grow to 12.8 billion by 2020.[1] For perspective, that is approaching *double* the world's population. The IoT is becoming ubiquitous in our daily lives. It is in our cars, our businesses, and our homes. We use it when we eat, sleep, relax, and exercise. More and more, like the internet itself, our entire way of life is changing in reliance on the IoT. Like with any technological change affecting the world on this scale, the law has been slow to react. The IoT has been developing for nearly 20 years, but only in the past few has our legal system begun to take note. As with the IoT itself, the emerging legal implications are sweeping and will affect both individuals as well as businesses of every size. This is the initial article in a multipart series that will offer a brief introduction to the concepts underlying the IoT and describe their emerging effects on our legal landscape.

What is the Internet of Things?

The truth is that the phrase "Internet of Things" has eluded precise definition. It has been roughly defined to include such jargon as “networked items connected to the internet,” “machine to machine communication,” and/or the set of technologies underlying and relying on “big data.” Regardless of the academic definition, to paraphrase Justice Potter, we know it when we see it.

Most of our daily interaction with the IoT involves a wide variety of consumer devices. There is the “smart” thermostat, like a Nest, that will automatically control the temperature of your house. There is the health tracker, like a Fitbit, that will monitor your calorie consumption and exercise habits. There are your car’s “smart” features, like adaptive cruise control, that will essentially drive you around automatically. All of these might fit into the IoT category. But part of the reason that the IoT is so hard to define is because it isn’t just one thing. It is a number of technologies that work together in a number of different ways. Some IoT devices use all of these technologies and some use only one. These foundational technologies can be summarized into four major categories[2]:

1. **Private Network Connectivity**. This means that a device can connect to a private network, like you’re household WiFi, rather than a public network like the internet. The “private” network can take a number of forms. It could be your home network managed by a typical wireless router. It could also be a network dedicated exclusively to a series of devices, such as smart speakers that communicate only with each other. The latter is sometimes called “mesh” networks. These technologies allow things to interact with other things without using the internet. Part of this is keeping the network, as well as the information flowing through it, “private.” That means encryption forms a critical part of this technology.

2. **Machine Learning**. If artificial intelligence is a scale between a desktop calculator and the Terminator[3], "machine learning" is somewhere in the middle. Machine learning is programming that enables a device to collect information and modify its own behavior in response to that information. This means collecting data, analyzing that data, determining trends in the data, and applying those trends to how the device will operate in the future. Take, for example, your Roomba. It will create for itself a map of your home so that it can vacuum more efficiently in the future.[4] Higher degrees of artificial intelligence (closer to Terminator) are being developed and included into IoT devices, but many consider the basic concept of "machine learning" as the baseline.

3. **Internet Connectivity**. For more than two decades, we have demanded access to the internet. Our daily access began with desktop computers, then moved to laptops, and then expanded to mobile devices. We used these devices to browse the vast and expanding internet, take advantage of internet-based applications (like Facebook), and communicate with others. But do devices need to do all or any of these things to take advantage of the internet? The IoT has proven that the answer is an emphatic "no." Over time, we have learned to take advantage of the internet's wide and varied applications, which can enhance[5] almost anything. As a result, internet connectivity alone can transform a toothbrush into an IoT toothbrush.

4. **Data Collection and Analysis**. This sounds simple but can get very complex, and it includes a vast array of technology. Here are a couple of examples. Let's say you have a smart

thermometer. It records the temperature in your house, it records when you change the temperature, what day of the year it is, what temperature you prefer in different rooms, and then eventually automatically adjusts those things to your previous preferences as time goes on. Awesome, but how does this raw data get us to the “smart” feature of automatic temperature control? Generally, we take a thermometer, a clock, a calendar, maybe a light sensor and over time assume you want similar temperatures under similar conditions (e.g. this time next year, you’ll want the temperature at 72 degrees).[6]

Now let’s go to a smart health monitor (like a Fitbit). Among other things, it collects gyroscopic data, oscillation data, heat and pulse data and determines when you’re sitting, walking, snoozing, or sleeping.[7] You didn’t tell it you were sleeping, it just knew. It also determines your position and elevation based on GPS data. You didn’t tell it you were going up a hill, it just knew. Over time, some devices can learn the difference between when you’re biking, running, treadmilling, lifting weights etc. all automatically. These are irregular activities, and to determine whether these activities are happening requires a combination of complex data and analysis.

In addition, both of these types of devices collect and save that data over serious periods of time. Days, months, years, etc. Let’s think about that. Collectively, (just these two devices) know where you went, what you were doing, what your heartrate was, when you were sleeping, on a daily basis pretty much every day. Here’s a question: Does any person that you know—or have ever known— have that kind information about you? Do they remember that information perfectly for months, or years? Moreover, many IoT devices do not save or analyze this data locally (i.e. within the actual device), but rather, send the data over the internet to a remote processing center, which does the heavy lifting and then sends the results back to the device. This brings us to our legal landscape.

Data Security:

Current events have put cybersecurity at the forefront of our minds. The broad umbrella of "cybersecurity" includes a number of legal issues for businesses and consumers. Data about people and their habits is valuable. Can companies protect a consumer's personal data while also relying on that data as part of its business model? They can. There are also compliance issues. For example, on May 25, 2018, the European Union will implement the General Data Protection Regulation (GDPR), which includes sweeping standards for data security applicable to business operating in Europe. In the United States, the Federal Trade Commission (FTC) has begun interpreting its long-standing consumer protection regulation authority to encompass companies' policies for preventing data security breaches. This has led to lawsuits and consent judgments imposing harsh penalties for companies without robust data-protection schemes. Let's avoid these.

Intellectual Property:

One of the natural limitations on the IoT framework is that these devices originate from a wide array of different companies and manufacturers that have their own proprietary technology and interfaces. They cannot share data among each other and are, therefore, much more inefficient than they could be. Every company wants to be the VHS tape and not the

Betamax. They want their own intellectual property to be the baseline for everything and everyone. This is a problem that has been addressed with other technologies, such as with cell phone data standards (i.e. 3G and LTE). Technology and consumer groups take up the charge by essentially analyzing hundreds of companies' proprietary (and usually patented) technologies and voting on those that will comprise a common standard. The technologies are then licensed on, so-called "Fair Reasonable and Non-discriminatory" rates (FRAND) to all of the companies using the standard. The definition of FRAND is less than clear and has been the subject of a plethora of patent litigation over the years. Companies entering the IoT space will need to be familiar with the FRAND licensing practice and its potential pitfalls. Also, who owns your data? When you set up facial recognition on your device, does the company now own that face data? Are you owed a license if the company sells the data? Can any license be granted by user agreement?

Products Liability and Consumer Protection:

Consumers can be injured by IoT devices, and as with any product, there are a variety of consumer protection statutes that might apply to any given situation. As many business have learned over the years, exposure from consumer lawsuits can be substantial. Companies must understand their potential liability for both defective and non-defective products. There are steps that can be taken to reduce potential exposure through company policies as well as user agreements. Consumers should also understand their rights and limitations when using IoT devices. In addition, the very act of collecting and using consumer data has been held under certain circumstances to warrant private causes of action. This has led to individual and class action lawsuits focusing on data collection and use policies. These private rights of action come from some unlikely places, such as—and I swear I’m not kidding—the federal Wiretap Act.

I’ll be exploring each of these, and other, topics in detail in the upcoming articles in this series. The IoT will only be expanding. It will soon play an essential role in all of our lives and businesses. These are revolutionary technologies that enhance our daily lives and have created new and rapidly expanding industries. As co-founder of the Global Business Network Stewart Brand once said, “Once a new technology rolls over you, if you’re not part of the steamroller, you’re part of the road.” I’d rather be the steamroller.

---

[1] https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

[2] No doubt others will take issue with this grouping. This summary is not meant to be definitive, but as a high-level introduction to general concepts for further discussion.

[3] For those with foil hats, most experts agree we are nowhere near to developing Terminator-like levels of AI, and some suspect that might not even be possible.

[4] http://www.latimes.com/business/technology/la-fi-tn-roomba-map-20170725-story.html

[5] Some would argue (such as fans of the HBO series Silicon Valley) that some applications, such as smart refrigerators that tell you when you are out of milk, solve a problem that doesn’t exist. I will leave the debate over whether this “enhances” an ordinary refrigerator to another time.

[6] https://nest.com/support/article/An-introduction-to-learning#nest-thermostat-learns-a-week

[7] https://help.fitbit.com/articles/en_US/Help_article/1141

The material appearing in this website is for informational purposes only and is not legal advice. Transmission of this information is not intended to create, and receipt does not constitute, an attorney-client relationship. The information provided herein is intended only as general information which may or may not reflect the most current developments. Although these materials may be prepared by professionals, they should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

The opinions or viewpoints expressed herein do not necessarily reflect those of Lorman Education Services. All materials and content were prepared by persons and/or entities other than Lorman Education Services, and said other persons and/or entities are solely responsible for their content.

Any links to other websites are not intended to be referrals or endorsements of these sites. The links provided are maintained by the respective organizations, and they are solely responsible for the content of their own sites.