



2016 CLM Annual Conference  
April 6-8, 2016  
Orlando, FL

**“The Internet of Things –  
Where the Cyber meets the Physical”**

**I. Understanding the Internet of Things (IoT)**

**A. What is The Internet of Things**

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.[1] The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure,[2] creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit;[3][4][5][6][7][8] when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.[9]

From Wikipedia, the free encyclopedia

The IoT is the latest development in the decades-old revolution in communications, networking, processing power, miniaturization, and application innovation and has radically altered communications, networks, and sensors. The IoT is a decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical world. However, the IoT differs from previous technological advances because it has surpassed the confines of computer networks and is connecting directly to the physical world. Just as modern communications have fundamentally altered national security and emergency preparedness (NS/EP), the IoT has had a similar transformative impact.

What's the buzz? The Internet of Things revolves around increased machine-to-machine communication; it's built on cloud computing and networks of data-gathering sensors; it's mobile, virtual, and instantaneous connection; and they say it's going to make everything in our lives from streetlights to seaports "smart."

Wired, "The Internet of Things Is Far Bigger Than Anyone Realizes"

IBM and its clients are ushering in a new cognitive era. IBM Watson IoT extends the power of cognitive computing to the billions of connected devices, sensors and systems that comprise the IoT. Why? Because IoT is testing the limits of programmable computing, and Cognitive IoT is how we will overcome those limits. It is how we will accomplish the transformational outcomes we know are both possible and necessary—from operational efficiency to customer experience to industry disruption.

How IBM sees the Internet of Things

As more and more devices connect to the Internet – everything from trains to air conditioning units to smoke alarms – the potential for the Internet of Things (IoT) to drive efficiencies, increase productivity and promote economic growth is becoming reality. In particular, the IoT is fueling innovation and creating opportunities in the development of clean technology, and helping redefine what a sustainable world will look like.

Chris Buddin, Global Head of the Clean Technology and Renewables Group and Internet of Things at Goldman Sachs, explores the possibilities at the intersection of the IoT and clean technology.

1. Things that are connected

The Breathometer	Fitbit bracelet
Withings cuff	iBGStar iPhone add-on
Adidas miCoach Smart Ball	UVEBand
Helmet by LifeBEAM	Mimo Baby Monitor "onesie" shirt
W/Me bracelet from Phytode	Melon or Muse headband
Nest Thermostat	SmartThings' home-automation system
Belkin's WeMo home electricity and water-usage tracker	GE's new connected appliances
Smart Phones	DropTag sensor and other sensors
Progressive Snapshot	Human Condition Safety Vests
Automatic Link driving and automobile monitor	
Cooltrax refrigerated asset tracking and temperature monitoring	

## 2. Data generated by things connected

steps you take in a day	calories burned
minutes asleep	heart rate
blood pressure	blood glucose levels
temperature	heart rate
hemoglobin levels	soccer performance
daily exposure to ultraviolet rays	blood flow
oxygen saturation	sleep habits
temperature	breathing patterns
changes in your autonomic nervous system	brain activity
ability to focus	home appliance and systems function
Electricity and water usage	driving habits

### **B. Fact Pattern for Understanding the Internet of Things**

a. ABC Co. contracted with DEF Co. to purchase poultry. The poultry was properly inspected at ABC Co. The poultry was transported from ABC Co. by Truck 1 to a Railway where it was transported to the city of destination. It was then transported by Truck 2 to DEF Co., where it arrived frozen. The poultry was then determined to be spoiled. Each party that came in contact with the poultry had documentation that it was at the proper temperature when it arrived and when it left their possession.

b. PWR Power Company recently installed for its regional customers, web enabled thermostats permitting them to control home temperatures during peak usage times. One hot summer evening, the company experienced an unusual spike in electricity usage which caused a blackout in that region. It was determined that someone had gained unauthorized access to the web enabled thermostats and set the thermostats on 30 degrees. It took the company 24 hours to gain control of the thermostats.

c. Mr. M. left his home one day at 8am as he normally does on his way to work. He typically walked three blocks to the train station and then took the train to work. A few weeks before, Mr. M. had an Implantable Cardioverter Defibrillator implanted for his slow heart beat. About 2 blocks from his home he felt faint, fell, broke his wrist, hit his head and lost consciousness. After getting out of the hospital he went back to the site of the accident. He observed a raised sidewalk flag and decided that was the cause of his fall. A lawsuit followed.

d. RDY Warehouse was a popular spot to store summer wear so that it would be conveniently located in time for the season. Over the winter clothing manufacturers had their goods shipped there. Over a long weekend the temperature unexpectedly began to drop in the warehouse. The temperature reached 30 degrees, causing the sprinkler pipes to freeze and water to flood the warehouse, damaging much of

the clothing. It was determined that XYZ insurance company had arranged to monitor the warehouse conditions, but it had lost connectivity to the warehouse just before the weekend.

## **II. The Internet of Things and legal responsibility and apportionment of fault**

A. Duty – Under Florida Law, a claimant must first demonstrate that the defendant owed a "duty, or obligation, recognized by the law, requiring the [defendant] to conform to a certain standard of conduct, for the protection of others against unreasonable risks." *American Optical Corp. v. Spiewak*, 73 So. 3d 120 (Fla. 2011), citing, *Clay Elec. Coop., Inc. v. Johnson*, 873 So.2d 1182, 1185 (Fla. 2003) (quoting *Prosser and Keeton on the Law of Torts* § 30, at 164 (W. Page Keeton et al. eds., 5th ed. 1984)).

B. Breach – Second, the claimant must establish that the defendant failed to conform to that duty. *Id.*

C. Proximate Cause - Third, there must be "[a] reasonably close causal connection between the [nonconforming] conduct and the resulting injury" to the claimant. *Id.*

D. Harm - Fourth, the claimant must demonstrate some actual harm. *Id.*

## **III. The Internet of Things and its application. - what do we want to know?**

A. Who are the potential defendants? In analyzing the various fact patterns, determine the potential defendants in the claim or lawsuit.

B. What do the claims person or defense counsel want to know? Analyze the fact patterns and determine what information is or may be available, keeping in mind the Internet of Things.

C. As an Underwriter, what would you want to know? What data, controls or sensors would you like to see which would enable you to better underwrite the risk.

D. As a Risk Manager, what would you want to know? What data, controls or sensors would you like to see which would enable you to better manage your risk.

## **IV. Legal Implications of the Internet of Things**

A. Discrimination – The Internet of Things, through data collection, provides the opportunity for discriminatory conduct by gathering information which one would otherwise be prohibited from gathering, such as lifestyle, health, race and geographic and other information.

B. Privacy – With the increasing interconnectivity of our lives and the devices we use, privacy continues to be attacked. Who maintains our data, who has access to that data and who owns that data is still being sorted out.

C. Security – The scope of cyber liability and data privacy issues involving the connected world as we now know it is growing almost every day. With the increase of connected devices and varying security protocol utilized by the many devices, the risk of data breaches will continue to expand.

D. Consent – The issue of consent and the utilization of IoT devices is challenging. No uniform requirements for requesting and receiving consent, advising users of the data gathered by the various devices and who is maintaining and storing that information and who has access to it has yet been developed.

E. Constitutional – The IoT is in its infancy and there are only 2 references to it in the reported cases. Both involving the ability to gather information surreptitiously and the rights of criminal defendants.